出國報告（出國類別：其他）

參加「APEC 金融監理人員訓練倡議－科技風險監理研討會」會議重點與心得報告

服務機關：金融監督管理委員會檢查局

姓名職稱：李智婷　研究員

派赴國家：韓國

出國期間：2016 年 5 月 8 日至 13 日

報告日期：2016 年 5 月 31 日

摘要

「亞太經合會金融監理人員訓練倡議」(Asia-Pacific Economic Cooperation Financial Regulators Training Initiative, APEC FRTI)機制係自 1998 年 5 月為藉由提升銀行業與證券業監理人員之分析與技術能力以強化亞太區域金融業之監理工作而建立，並於亞洲開發銀行(Asian Development Bank, ADB)總行設置秘書單位綜理訓練倡議相關事務；今(2016)年預訂舉辦 11 場研討會，其中專屬銀行業監理人員共 5 場、證券業監理人員共 4 場。

為增進亞太國家金融監理及檢查人員對科技風險監理之瞭解，亞洲開發銀行與韓國金融監督院(Financial Supervisory Service, FSS)在 APEC FRTI 機制下，於 2016 年 5 月 9 日至 13 日於韓國首爾共同主辦「科技風險監理研討會」，並邀請美國聯邦準備銀行(Federal Reserve Bank, FED)指派資深檢查人員擔任講師，指導與會人員對銀行業在網路、電腦作業系統以及對新興資訊科技(IT)領域之基礎概念，藉此強化監理與檢查人員之風險辨識、評估和監督之能力並瞭解檢查關注重點。

本次共有孟加拉、柬埔寨、中國大陸、印度、印尼、馬來西亞、尼泊爾、巴基斯坦、巴布亞紐幾內亞、菲律賓、索羅門群島、斯里蘭卡、泰國及我國等 14 個國家 36 位金融監理檢查人員參與研討會，上課方式主要係由講師說明資訊風險管理、網路與防火牆、虛擬化作業、資料安全及新興科技等議題對銀行業之衝擊與風險，以及檢查人員應關注之重點，各國金融監理檢查人員並於研討會過程中分享各國檢查實務經驗或提問討論。

本次奉派出席本研討會，除期望藉由課程瞭解美國聯邦準備銀行現行對銀行業資訊科技之監理檢查作業，並能加強與 APEC 各出席會員國之監理檢查人員互動交流相關議題之監理檢查經驗外，面對未來金融業數位金融之發展，將就如何逐步調整並強化本局對金融業資訊科技之檢查關注重點及監理措施提出具體建議。

目次

壹、 前言

「APEC FRTI 科技風險監理研討會」係由亞洲開發銀行 ADB 與韓國金融監督院 FSS 在「亞太經合會金融監理人員訓練倡議」機制下共同主辦四天半之中階課程，參訓對象主要為亞太區域會員國家之金融機構資訊科技檢查人員，以及查核項目涉及資訊相關議題且對 IT 概念、監理及風險有基本瞭解之其他檢查人員。

本篇報告第一部分為「研討會目的」，說明主辦單位舉辦研討會之目的及本會派員出席擬達成之成效。第二部分為「研討會過程」，簡述授課講師、參加學員、授課內容與方式。第三部分為「研討主題」，彙整本次研討會主要講述與討論內容。第四部分為「心得與建議」，說明參加本次研討會之心得與建議。

貳、 研討會目的

本次「科技風險監理研討會」主要由美國聯邦準備銀行之資訊科技檢查人員擔任講師，課程設計以網路及作業系統之基本概念為主軸，並涵蓋資訊系統控制與管理、資料管理及新興科技所涉風險，目標在指導參加學員完訓後具備下列能力：

一、 瞭解銀行資訊科技與架構更進階之概念。

二、 辨識與金融機構資訊環境相關之營運及監督風險。

三、 研提對機構營運風險衝擊之因應措施。

四、 討論對金融機構之檢查結果及關注事項。

五、 分析與處理包括：虛擬化、網路、資訊安全及軌跡(log)管理、「攜帶自有裝置 (Bring Your Own Device, BYOD)」、雲端運算(cloud computing)、服務供應廠商管理、行動裝置、社群媒體等新興科技所暴露之風險與衝擊。

六、 應用於未來工作範圍：

(一)在資深資訊科技檢查人員之協助下，評估與辨識非複雜型金融機構之主要風險。

(二)研提或協助研提有關金融機構科技風險之檢查缺失。

(三)主導或參與銀行涉及資訊科技檢查缺失與關注事項之討論。

參、 研討會過程

一、講師與出席人員

本次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，該講師 Colin K. Gavin 係屬芝加哥聯邦準備銀行(Federal Reserve Bank of Chicago)監督與管理部門風險管理處(Department of Supervision and Regulation)之技術架構師(Technology Architect)，主要職務包括在 STREAM (Supervision Technology Risks Educate, Analyze and Manage) 實驗室對聯邦準備體系、聯邦存款保險機構(FDIC)、美國財政部金融管理局(OCC)及州會員銀行等機構提供資訊科技例行教育訓練，並參與銀行資訊科技專案檢查，本身尚具備多項資訊科技相關證照，原訂另一位講師 Joe Krencicki 因事無法授課。

參與本次研討會之國家包括來自孟加拉、柬埔寨、中國大陸、印度、印尼、馬來西亞、尼泊爾、巴基斯坦、巴布亞紐幾內亞、菲律賓、索羅門群島、斯里蘭卡、泰國及我國等 14 個國家 36 位金融監理檢查人員。

二、課程進行流程

(一)5 月 9 日：上午各國參加研討會學員辦理報到(接續之每日上、下午均應辦理簽到)，首先由主辦單位韓國金融監督院 FSS、亞洲開發銀行 ADB 及美國聯邦準備銀行進行開訓致詞，並由各參訓學員自我介紹，隨即開始研討課程，由講師說明當日主題包括：資訊風險管理架構及風險衡量、資訊治理、資訊科技之稽核與監理檢查作業、網路基本概念、網路安全及設計、網路架構、防火牆及其他控管機制。

(二)5 月 10 日：講述主題包括：Microsoft 及 Mac 為基準之作業系統介紹、伺服器與客戶端作業架構及目錄、虛擬化技術之應用及探討「攜帶自有裝置 BYOD」之相關風險。

(三)5 月 11 日：講述主題以資訊安全管理為主，包括辨識威脅來源、漏洞管理、滲透測試、修補程序管理、變更管理、資料完整性及機密資訊與事

件管理等。

(四)5 月 12 日：講述主題以新興科技為主，包括雲端運算、對服務供應商之管理、業務持續營運計畫(Business Continuity Planning, BCP)、災害復原、行動裝置(Mobile)概念、行動銀行及支付認證等相關風險。

(五)5 月 13 日：講述最後一項主題為社群媒體與相關風險，並由 FSS、ADB 及 FED 進行結訓致詞後即頒發本次研討會結業證書。

肆、 研討主題

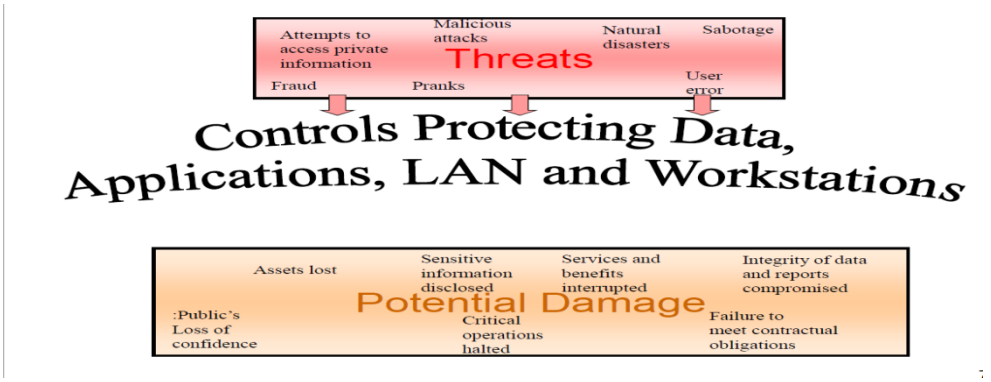
一、 風險管理與資訊治理

(一)風險管理

1.「風險」係指因意外或故意觸發資訊系統安全弱點而產生威脅之可能性，進而對組織產生衝擊影響，依定義所涵蓋之三項要素為弱點、威脅、可能性，其交互結果對組織產生之損失影響即成為風險。

2.組織之風險管理應關注日常作業模式之變更情形，並持續評估其可能形成之潛在威脅，依據組織應受保護資產之價值，透過辨識、控制及減輕資訊系統相關風險之過程，以抵禦各式內、外在威脅及潛在可能損失(如下圖)，惟風險管理旨在由合理之人員進行合理性之控制，仍不免存在「殘餘風險」是應有的認知。

圖 1：風險管理介面[12]



3.風險管理架構

常見之風險管理架構有美國電腦稽核與控制協會 ISACA 所提出之 COBIT5、COSO 內部控制金字塔、NIST、ISO/IEC 27001 及 Microsoft 之風險管理模組等，主要就金融機構常引用之 NIST 及 COBIT5 提出解說，。

(1).NIST

---

1. Federal Reserve System, STREAM
2. STREAM 全名為科技風險監理實驗室(Supervision Technology Risks Educate, Analyze and Manage)，係為美國聯邦準備銀行設立於芝加哥洲負責辦理金融監理檢查人員之資訊科技教育訓練。

美國國家標準與技術研究所(National Institute of Standards and Technology, NIST)為美國聯邦之非監管機構，負責制定與推廣度量衡學(measurement)、標準(standards)和技術(technology)，針對風險管理提出風險評估 10 項步驟、風險抵減 7 種方法、風險管理評估 3 項重點，其中包括聯邦機構至少每 3 年辦理一次風險管理評估。

(2).COBIT5

COBIT(Control Objectives for Information and related Technology) 係由美國資訊系統稽核與控制協會(Information Systems Audit and Control Association, ISACA)及 IT 治理組織(IT Governance Institute, ITGI)共同建立之國際公認準則，作為企業建立資訊系統與科技安全控管政策與程序之參考控制架構。COBIT5 於 2012 年提出，包括 5 項治理原則及 4 種管理課責領域，以 RACI 圖表現各個流程之風險角色與責任。

4.風險評估

資訊系統之風險評估旨在運用適當之風險測量方法或工具，對組織資訊安全管理範圍內之每一資訊資產因遭受洩露、修改、不可用和破壞所帶來的任何影響做出一個風險測量列表，以便識別風險控制優先等級並選擇適當且正確之安全控制方式，將風險控制於機構可接受之範圍內。提出風險評估包括盤點系統與資料、辨認資產弱點及選擇控制方式、決定殘餘風險、彙整報告並每年定期檢視評估結果等四大項、13 小項之基本步驟。

5.檢查人員對風險管理架構應關注之重點

(1).瞭解有那些持續進行之風險識別程序

(2).瞭解風險管理架構所運用之管理邏輯

(3).上開管理邏輯對組織是否合理

(4).瞭解不同風險管理方法(如 NIST 及 COBIT)之差異，至於金融機構應採用哪一種風管架構，取決於銀行對自身條件與環境之評估，並

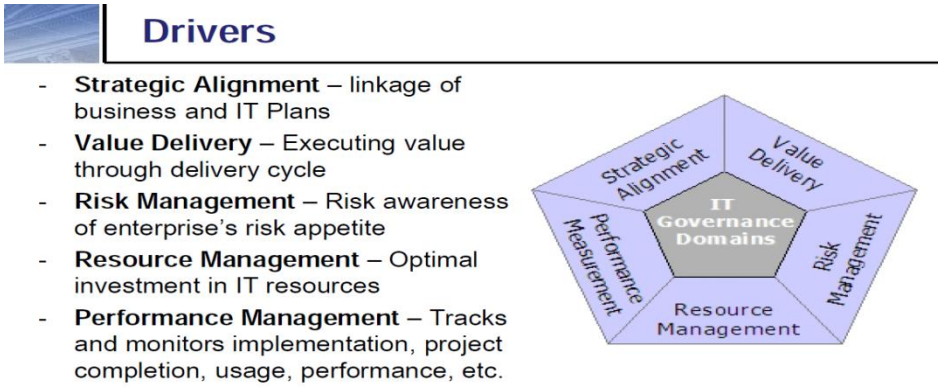
無最佳選擇之建議

(5). 熟悉機構所採用之風險管理邏輯或風險管理架構，以瞭解其內部處理程序之運用

(二)資訊治理(IT Governance)

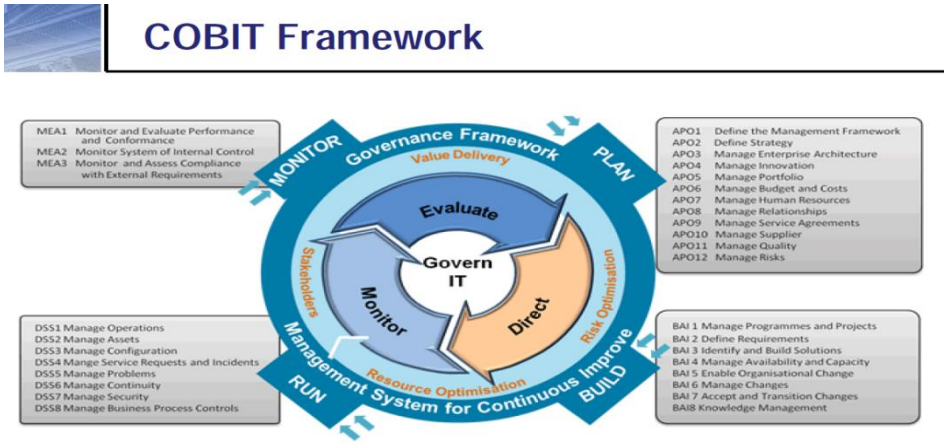
資訊治理旨在引導和控制機構各種營業活動和流程之架構，以確保資訊科技與業務目標一致，推展業務發展，促使收益最大化，涉及領域包括策略聯盟、價值傳遞、風險、資源與績效管理五項。

圖 2：資訊治理領域[3]



國際上較成熟之資訊治理架構及實務有 COBIT、英國 ITIL 服務管理實務(ITIL Service Management Practice)、ISO 27002/9000 等，以 COBIT 架構為例，包含 31 個資訊治理控制流程，並運用平衡計分卡分別自日常運作及公司角度評估 IT 治理情形。

圖 3：COBIT 架構[4]



3. Federal Reserve System, STREAM
4. Federal Reserve System, STREAM

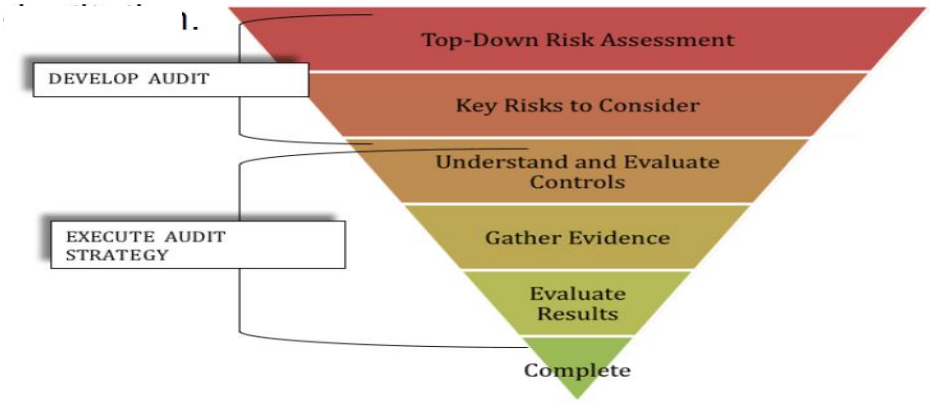
(三)資訊稽核(IT Audit)

主要講述資訊稽核之目標、董事會及內、外部稽核相關職責與獨立性角色等傳統知識，並提出有效之風險導向稽核、資訊稽核委外、對金融機構資訊稽核之評價重點等。

1.風險導向稽核

有效之風險導向稽核應能涵蓋機構之主要業務活動，由上而下進行風險衡量，並就關鍵風險衡量結果決定查核頻率與深度，查核計劃須符合機構之規模與業務複雜度，風險導向稽核運用於資訊科技查核則係透過關注營業活動與程序，瞭解機構重要營運部門與產品之整體相對風險與運用資訊科技之控制情形。

圖 4：風險導向稽核程序[5]



2.資訊稽核委外及對金融機構資訊稽核之評價重點

(1).機構應對資訊稽核委外廠商辦理實地查核，並確保監督委外作業

(2).對資訊稽核之評價包括：稽核部門隸屬之單位、獨立性、風險評估執行情形、稽核計畫與範圍、稽核工作底稿(稽核報告時效及品質、工作底稿完整性及品質)、缺失改善方案及追蹤管理情形、資訊稽核人員之適格性(含學經歷、教育訓練、國際專業認證資格如 CISA、CRISC、CISSP、CIA 等)、是否切實向董事會及其他利害關係人報告

5. Federal Reserve System, STREAM

3.檢查人員對內部資訊稽核應關注之重點

(1).稽核報告單獨提報高階管理層/董事會

(2).組織結構、委員會成員和陳報關係

(3).潛在問題之陳報程序與處置

(4).對外部稽核委任之範圍與管理

(5).內部稽核章程和作業規章之董事會核准程序

(6).稽核計畫之責任歸屬與施行現況

(7).出具報告頻率及具體內容

(8).董事會對稽核計畫及查核日期修訂之認知和參與程度

(9).管理層對查核意見之回應意見及預訂完成日期

(10).明確指出重複出現之缺失

(11).對審計委員會及董事會之陳報情形

(12).對未結案查核報告之追蹤管理情形

(13).涉及資訊安全、業務持續營運及供應商管理等重大風險

(14).配合內部稽核或風險評估之查核期程/週期

(15).資安事件管理報告

(16).稽核部門之獨立性和作業準則

(17).內部稽核報告、工作底稿是否依循已核准之政策與流程

(18).對工作底稿之存取及所有權之妥適性

(19).稽核報告覆核程序之妥適性

(20).查核發現之根本原因

(21).稽核主管評核過程之獨立性

(22).陳報之查核報告與工作底稿查核發現之一致性

(23).內部稽核人員與主管之專業知識與在職訓練情形

(24).增進各董事瞭解查核程序與發現之訓練情形

(25).對稽核人員獲取相關專業證照及培訓情形

(26).委外辦理內部稽核與顧問之評選機制

(27).依稽核計畫執行期程配置適當內稽人員

二、 網路安全與防火牆

(一)網路管理與安全性

1.網路基礎概念

主要講述網路之類別包括常見之區域網路、廣域網路、都會區域網路(Metropolitan Area Network, MAN)、儲存區域網路(Storage Area Network, SAN)、個人區域網路（Personal Area Network，PAN）以及無線網路，其中儲存區域網路係採用光纖通道技術、磁碟陣列、磁帶櫃、光碟櫃等技術，連接伺服器和儲存裝置。

網路基本裝置包括交換器(Switch)、路由器(Router)、防火牆(Firewall)，以及其他如中繼器(Repeater)、數據機((Modem)、入侵偵測防禦系統(IDS/IPS)、虛擬專線網路集中器(Virtual Private Network concentrator)等。網路標準架構有國際標準化組織（ISO）提出之七層開放式系統互聯模型(OSI)及四層之 TCP/IP 模型最為廣見。

2.通訊協定

目前網路通訊協定之 IP 位址係採 32 位元(4 位元組)之 IPv4，惟已遭遇位址使用短缺之窘境，新一代 IPv6 計劃建立未來網際網路擴充的基礎，目標是取代 IPv4，但同樣也必須面臨早期路由器、防火牆等相關應用程式皆須改寫之問題。

3.VPN

虛擬專用網路(Virtual Private Network, VPN）是一種提供予被授權者在兩個網路設備間傳遞已加密訊息之私人通訊方式，常用於中、大型企業或團體與團體間，針對此議題亦與講師討論並確認美國監理檢

查人員在外部係採 VPN 方式連線至內部，惟必須特別注意授權與必要性。

4.檢查人員對網路安全管理應關注之重點

(1).一般及風險衡量政策制定情形

①金融機構是否訂有密碼、加密、稽核、風險評估、變更管理規則等？

②金融機構是否訂有網路安全政策？是否包括存取管理、網路過濾及路由規則?

③金融機構是否訂有遠端存取/VPN 政策？

④是否已建立妥適之監測和日誌紀錄管理規定？

(2).風險衡量

①是否檢視資料安全性與系統配置相關之現有政策和作業程序？

②是否評估各個網路之系統硬體、操作系統、應用程序和資料之重要性？

③是否探討每個內外部系統之潛在風險？

④是否探討在正式系統執行測試程序之風險及風險抵減方法？

⑤是否評估安全配置要求之妥適性?

⑥是否包含對金融機構網路結構之描述？

(3).安全架構

①是否能及時修補及更新所有系統安全漏洞？

②所有系統和軟體配置是否均經銀行資訊安全部門核准?

③所有不需要之軟體和服務是否已停用或解除安裝？網路安全設備之預設帳號密碼是否已移除?

④內部稽核是否已查核系統並驗證系統漏洞修補和強化作業規範之落實情形？

⑤資訊單位是否透過存取權限清單(ACLs)和代理伺服器管制網路服務？

⑥資訊單位是否建置監控機制，以確保所有網路安全設備透過安全管道進行遠程管理？

⑦金融機構是否將所有系統納入監控範圍？

⑧日誌記錄格式是否標準化？是否集中處理?

⑨金融機構對網路相關設備已建立妥適之安全管理程序？

(4).網路安全性

①內部稽核範圍及查核項目之完整性

②對測試廠商之合約、測試人員背景及執行作業之實地查核

③測試報告是否詳載範圍、重要假設、風險排序及評估結果、後續修正建議等內涵?

(二)防火牆設計

主要簡介防火牆、入侵偵測系統(Intrusion Detection System, IDS)、入侵防禦系統(Intrusion Protection System, IPS)等網路安全技術。

1.防火牆

防火牆之基本功能在於隔離網路中不同信任程度之區域設備與系統，通常網際網路等外部系統屬非信任區域，機構內部網路則屬受信任區域，運用防火牆軟體或伺服器主機設備，透過客製化之設定以檢測、過濾並產生所隔絕網路區域之流量報告。型態包括網路邊界防火牆(Network perimeter firewall)、主機型防火牆(Host-based firewall)、虛擬型防火牆(Virtual firewall)三類。講師說明硬體防火牆較軟體防火牆佳，並建議良好之防火牆應具備邊界及內部防火牆二層，且分別採用不同規格之廠商產品。

2.IDS/IPS 入侵偵測/防禦系統

入侵偵測/防禦系統為補充防火牆功能之網路安全設備，用以偵測內部不當使用或外部惡意攻擊，並具有漏洞補強機制、提供警告、阻斷與隔離功能，IDS 種類有主機型(Host-based IDS)、網路型(Network-based IDS)及合併運用前揭兩種之系統。IPS 種類有網路型(NIPS)、無線型(WIPS)、主機型(HIPS) 及網路行為分析(NBA)。講師說明下一代防火牆趨勢係將網路型 IDS 併入傳統防火牆功能。

3.檢查人員對 IDS/IPS 應關注之重點

(1).機構對 IDS/IPS 之認知

①管理階層是否清楚瞭解 IDS 之重要性?

②是否辨識機構面對之威脅，並執行相關控制措施?

③是否辨認機構之機敏資訊，並瞭解其所放置之伺服務及所在網路區域安全性?

(2).日常運作

①IDS/IPS功能是否委外處理? 委外廠商存取機構資料之權限為何?

②機構是否檢視應用程式或作業系統日誌，以監視並確保 IDS/IPS 之運作正常性

③檢視 IDS 日誌之頻率與負責人員為何? 日誌發現有入侵可能性時之處理程序?

④如何管理日誌? 日誌儲存空間不足之處理方式?

(3).警示處理

①IDS 偵測可疑入侵之示警程序? 是否通知管理者或安全人員?

②IDS 偵測可疑入侵時之反應程序? 是否自動重新恢復設定?

③IDS 誤測如何處理? 誤測機率為何?

(4).檢查程序得參閱美國聯邦金融機構檢查委員會(Federal Financial Institutions Examination Council, FFIEC)IT 檢查手冊。

三、 作業系統及虛擬化設備

(一)作業系統

1.作業系統類別

講師介紹有關電腦作業系統(Operating System, OS)之基礎概念，包括 Microsoft Windows 家族：Windows7、Windows8、8.1、8RT、Windows 2008 及 2008R2、Windows XP 等各版本及其問題，以及 UNIX 與 Linux 系統，另亦說明行動裝置普遍使用之 iOS 及 Android 市占率為 85%，其他尚有 Samsung(44%)、BlackBerry(4.8%)、Symbian(4.4%)、Windows

Mobbile3.5%。

2.安全性

UNIX 及 Linux 之安全性可列為作業系統之健全實務(Sound Practices)[6]，其作法包括：

(1).關閉未使用之服務

(2).限制使用者以「根」(Root)最高權限登入

(3).在不影響可用性下安裝 IP 過濾器或防火牆規則

(4).安裝供應商所提供之最新修補程式

(5).限制遠端存取

(6).限制提高身份權限以「系統管理者」(super user)登入

3.檢查人員對作業系統應關注之重點

(1).參酌健全實務之作法檢視

(2).是否使用強密碼規則或其他授權登入使用機制，如權仗(token)?

(3).是否建立及監控稽核軌跡?

(4).遇金融機構合併案例，應檢視雙方資訊環境及系統之差異性

圖 5：購併銀行應就作業系統進行差異比對[7]

- Operating systems in place at Oak Tree Bank
  - Mobile OS
    - Corporate Blackberry Server running Blackberry OS 7 on the client devices
    - Apple and Android devices are not allowed
  - Server OS
    - Windows 2008R2
  - Client OS
    - Windows 7 only. No XP clients are present

- Operating systems in place at Checkers Bank
  - Mobile OS
    - BYOD – no one really knows……no one really cares……
  - Server OS
    - Windows 2000 Server
      - Legacy server – No Internet connection.
    - Windows 2003 Server Domain Controllers
  - Client OS
    - Ubuntu 12.04
    - Windows XP, Window 7, Windows 8

(二)虛擬化(Virtualization)設備

1.虛擬化技術

6.講師說明實務執行並無所謂最佳實務(Best Practices)，建議稱健全實務(Sound Practices)以表示其功能、制度或執行面優良之作法。

7. Federal Reserve System, STREAM

虛擬化方法論自 1960 年即由 IBM 提出，主要概念係運用硬體或軟體分隔、分時共享、機器模擬等技術，將電腦硬體資源區隔為登入系統、電子郵件系統、網際網路、資料庫等多項功能環境，以達資源使用優化並較實體基礎設施成本低，以及易於管理和提高正常運行時間等效益，至部分市場認為虛擬化亦能提高安全性，講師係抱持存疑之態度。

許多機構已導入虛擬化環境，運用硬體輔助建立虛擬化設備以分隔不同功能之作業環境，常見型態有儲存設備虛擬化(NAS, SAN)、網路設備虛擬化(VPN, VLAN)、記憶體虛擬化(Virtual Memory)、伺服器/工作站虛擬化等模擬實體電腦之虛擬機器(Virtual Machine, VM)。

2.虛擬化特性

將實體設備模擬分割後，各虛擬化設備形成虛擬化架構，運用虛擬硬體設備之軟體 VMWare 進行環境運作如日誌紀錄、警示提醒及因應、運作成效等之監督工作，整體虛擬化設備具有動態資源調配之特性，並能提高資源使用率、具容錯能力、備份支援等。

3.BYOD

(1).行動裝置之演進與風險

資訊科技之進步為大眾帶來生活便利與效率，自從 Apple 於 2007 年發表 iOS 行動裝置改變了個人使用電腦之眾多習性，機構因而面臨員工「攜帶自有裝置」(Bring Your Own Device, BYOD)如智慧型手機、平板電腦等到工作場所可能之風險，較開放之環境甚至能連接公司內部網路存取資料、處理公務。

圖 6：行動裝置之演進[8]

BYOD 之風險來自行動裝置，其中 Apps 之設計顯少能符合資訊科技相關政策，另外運用行動裝置將存取之資料複製於雲端，亦對機構形成潛在風險，雖然減少採購硬體成本，提升員工工作之便利性與效率，惟行動裝置之效率與安全性本來即為對立，允許 BYOD 之機構及其員工使用者必須在兩者間權衡取捨。

(2). 行動裝置之安全性政策

機構應針對 BYOD 之開放程度訂定相關管理政策，包括資料儲存與分享、設備連結與授權、照相、影音及資料連結等功能控制、允許使用之應用程式等，此外，金融機構亦得參酌資安期刊[9]針對 BYOD 行動資料保護、行動裝置管理、網路存取控制提出之建議制定相關政策。

4. 檢查人員對對虛擬化設備應關注之重點

(1). 虛擬化架構

①機構對機敏資訊及資料之分類情形

②日誌紀錄之監視情形

③整體網路架構之妥適性

8. Federal Reserve System, STREAM

9.微軟全球資安觀察，「7 個小技巧建立成功的 BYOD 政策」

(2).虛擬化設備之管理程序

①是否進行風險評估?

②是否有委外項目?

③實際運作情形及管理階層對運作之監督

④配置與變更管理

⑤內部稽核查核情形

(3).虛擬化設備之完整性、可用性及安全性

(4).機構對 BYOD 之檢查重點

①機構允許 BYOD 之實際執行情形

②是否評估行動裝置平台相關風險?

③是否制定工作場所使用行動裝置之相關政策?

四、 資訊安全

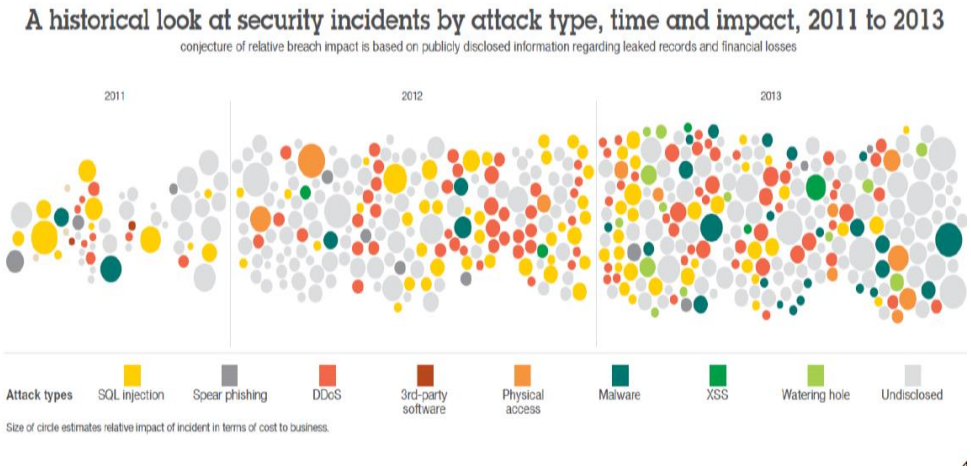
(一)威脅(Threat)型態

資訊安全所遭受之威脅或攻擊型態,依 2011 至 2013 年發生之資安事件分析資料顯示，主要包括隱碼攻擊(SQL injection)、魚叉式網絡釣魚(Spear phishing)、分散式阻斷服務攻擊(DDos)、協力廠商惡意軟體(3rd-party software)、惡意軟體攻擊(Malware)、水坑攻擊(Watering hole)、其他未知攻擊手法等，其中以 SQL injection、DDos 及未知的攻擊手法對機構衝擊較大，至發動惡意軟體攻擊之國家以美國占 42.3%最高、中國大陸占 5.9%、其他區域占 24.2%。

講師並提醒 Adobe PDF/ Reader/ Flash 經常遭到駭客攻擊，凸顯其防禦力較弱，建議機構宜獨立使用並以不連結機構內部網路為原則；另有關近期肆虐之勒索軟體(Ransomware)，經詢問講師表示，目前尚無任何預防措施建議，如電腦系統不慎遭其攻擊，僅能逕行依指示付款或立即中斷後重新設定格式化電腦，其內部某部門確有依指示付款之經

驗，最佳預防係依資料重要程度採定期或即時備份。

圖 7：2011 至 2013 年之威脅型態[10]



(二)漏洞(Vulnerability)管理

機構之軟、硬體及應用程序、內部自行開發或委外資訊系統，均可能潛藏弱點或因配置造成暇疵，而漏洞管理目標在保護機敏資訊，特別是客戶資料，以確保對重要資訊 CIA(保密性、完整性與可用性)之要求，講師建議機構應組成至少 2 人之漏洞管理小組，並進行持續性之追蹤、發現與處理工作，依 2013 年統計有 47.6%聚焦在攻擊支付服務產業之漏洞、金融產業 27.32%、政府部門則占 2.46%，在金融機構推動行動支付之潮流下，其漏洞管理(或稱弱點掃描)已成重點項目。

完美之「零漏洞」是不實際的，重點在採行持續且適當之漏洞偵測及修補措施，目前市場上有許多付費或免費之漏洞偵測工具如 Superscan、Nessusl、Nmap 等，講師建議機構得採用至少 2 種之免費工具負責發現與分析。

(三)滲透測試(Penetration Testing)

滲透測試係指藉由被授權之測試者(Pen Tester)模擬駭客(Hacker)之各種攻擊手段或其他工具，對機構電腦系統或網路進行安全性評估，評估結果依高、中、低程度進行後續之修補。

測試工具從事前偵測、弱點掃描、入侵偵測、系統修補、證據蒐集等程序，講師均提供相關工具之建議。另學員詢及備援裝置是否應

10. Federal Reserve System, STREAM

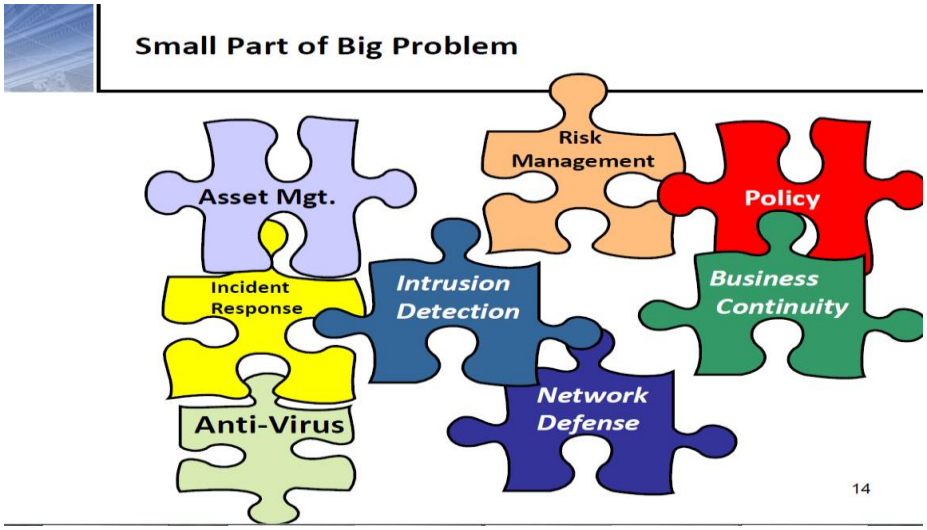
進行滲透測試，原則上至少一年辦理一次為佳，至於對委外或協力廠商基於其握有資訊之重要性程度，亦得於合約中要求定期交付滲透測試報告。

(四)修補程序與變更管理

1.修補程序管理

修補作業係資訊人員感到最痛苦繁雜的工作之一，機構資訊系統之修補需求可能來自於外部軟體供應商或協力廠商網站、通知，以及內部弱點掃描結果，透過人工及系統(如 Microsoft 更新服務)自動處理，其重要性由下圖可見，看似微不足道又頻繁之修補作業如未落實執行，累積即成大問題。

圖 8：大問題之形成[11]



2.變更管理

機構因應客戶需求或內部業務改造程序之調整而對資訊系統進行之變更稱之，變更請求(Request For Change, RFC)來自於系統問題報告、使用者提出之系統強化需求、採行新系統架構或標準如使用新作業系統、高階管理者之要求、其他危急狀況之變更，其中針對危急狀況之變更如占整體變更之 10~20%即屬過高。講師針對變更管理亦提出不良實

11. Federal Reserve System, STREAM

務(Bad Practices)作法如使用者未對所有變更進行測試、使用者於開發環境測試、未通過使用者測試即變更等。

五、 新興科技與議題

(一)雲端運算(Cloud Computing)

1.依據美國聯邦金融機構檢查委員會(Federal Financial Institutions Examination Council, FFIEC)對雲端運算之定義，係指一項從直接持有硬體或軟體資源到分享資源之演進過程，客戶端使用者得透過協力廠商所提供之網際網路「雲端」軟硬體設備，依需求取得資訊科技之服務。

2.美國國家標準與技術研究所 NIST 對雲端運算有清楚之說明，其必備特性包括：

(1).允許從不同客戶端存取網路服務(Broad network access)

(2).透過虛擬架構中之資源動態配置等方式快速且彈性共享網路、儲存及運算資源(Rapid elasticity)

(3).各式服務均能適當監控管理(Measured services)

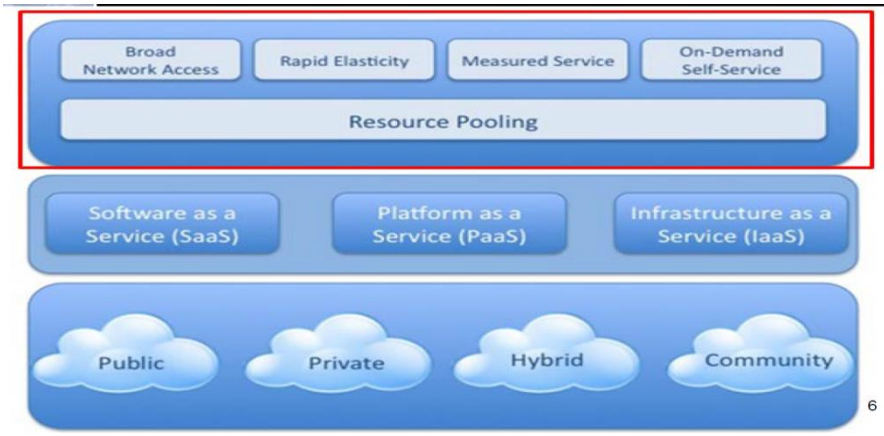
(4).機構依使用需求調整運算資源配置(On-demand self-service)

(5).資源動態配置與分享(Resource pooling)

常見之雲端運算服務模式有軟體即服務(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。

雲端運算之部署模式包括：公用雲(Public Cloud)、私有雲(Private Cloud)、社區雲(Community Cloud)、混合雲(Hybrid Cloud)，其中混合雲係結合公用雲及私有雲。

圖 9：NIST 雲端運算架構[12]



3.雲端運算之安全性

(1).資安等相關風險

雲端服務之彈性資源運用確實為機構節省不少固定成本與處理技術，相關付出之代價於機構將資訊或服務委外處理時顯現，機構面臨之問題與風險包含：資產逐漸公開與分散、客戶資訊無預警遭洩漏、變動或刪除、未能確保服務不中斷等。

(2).委外供應商問題

針對金融機構與雲端委外服務供應商之合約，講師強調依目前雲端服務供應商如 IBM、Microsoft、Amazon，均採用制式化契約，幾乎無金融機構得以客製化條款之前例，金融機構應於委外服務之評估階段，透過實地訪查(Due diligence)瞭解委外服務供應商之技術能力與雲端設備之環境外，建議應確認該等供應商是否清楚並能遵循金融機構相關法規，就雙方談妥之客戶服務層級協議(Service Level Agreement, SLA)逐條檢視委外合約，以避免可能違反資料保護相關規範或有與監理規範衝突之情形。

4.檢查人員對雲端運算應關注的重點

(1).金融機構對雲端服務之策略與治理

①檢視雲端服務決策與機構長短期策略有無衝突？

12. Federal Reserve System, STREAM

②是否訂有雲端服務供應商之遴選及持續監督之政策與程序？

③檢視主要雲端服務商之績效及相關風險考量是否陳報高階管理者

④檢視機構對委外廠商實地查核程序是否符合機構需求、服務品質及監理要求

(2).對雲端服務供應商合約及委外作業管理

①評估雲端服務供應商之遴選及持續監督作業程序

②檢視服務層級協議 SLA 有關資料所有權、儲存位置及格式、儲存所在地區或國家之相關規範、爭議處理

③檢視合約是否明訂與其他雲端客戶之資料區隔？

④檢視合約是否清楚訂有雙方職責？是否將退出及禁轉換條款納入考量，以防止被供應商套牢(vender lock-in)？是否考量供應商中途退出或與其他供應商合併？

⑤檢視合約是否揭露雲端服務供應商之分包商？

⑥委外廠商合約管理應著重細節，非模糊簡單化

(3).雲端服務供應商回復能力

①金融機構業務持續營運計畫(Business Continuity Planning, BCP)/災難復原計畫(Disaster Recovery, DR)演練是否涵蓋雲端服務提供商，機構是否評估雲端服務提供商之 BCP/DR？

②雲端服務供應商如何確保正常地提供客戶服務，以及在意外發生時之處理方式

③瞭解雲端服務供應商是否有進行中之變更管理程序，並要求機構及供應商均應在處理現場

(4).資訊安全性

①金融機構是否明確規範雲端服務供應商應具有完備之資訊安全管理機制，如資料安全保護策略、安全認證、交易安全設計、實體安全、備援及稽核等。

②瞭解雲端服務供應商對資訊安全、舞弊調查及資安事件通報之最大責任範圍

(5).金融機構及雲端服務供應商是否均有獨立風險評估單位(內外部稽

核、測試協力廠商)？

(二)業務持續營運計畫(BCP)/ 災難復原計畫(DR)/ 業務影響評估(Business Impact Assessment, BIA)

1.有無計畫

金融機構面臨全球資訊安全事件層出不窮以及未能預知知天災人禍，對於金融業務持續營運均已列為各國監理機關要求重點，所謂「沒有計畫等同計劃失敗」(Failure to plan is planning to fail)。

2.演練測試

資訊系統必須依重要性區分等級如 Tier0 為服務區域網路及光纖、核心轉換器等、Tier1 為使用活絡之目錄、電子郵件及電話、Tier2 為電子銀行及電子商務、Tier3 為檔案伺服器、Tier4 為測試伺服器，據以評估災難發生對機構之影響，並依據復原時間目標(Recovery Time Objectives, RTO)及復原點目標(Recovery Point Objectives, RPO)進行演練測試，講師亦說明進行「實地演練」(Real test)遠比「桌上演練」(Table top test)為佳。

3.檢查人員對 BCP/ DR 計畫應關注之重點

(1).業務持續營運計畫是否符合機構實際業務模式？

(2).是否由管理階層主導業務持續營運計畫？

(3).是否定期演練 BCP/ DR 計畫(包括情境演練、復原測試、測試異地復原、測試供應商之設施與服務等)？

(4).業務持續營運計畫是否已涵蓋所有新資訊系統？

(5).是否定期檢視並配合現況修訂計畫？

(三)行動理財服務

1.行動理財商品

伴隨行動裝置之便利與普及，行動理財服務包含行動行銷、行動

支付、行動銀行、行動轉帳等帶來商機，但也帶來挑戰與問題。

圖 10：行動理財服務範圍[13]

2.行動裝置所伴隨之風險

開放 Web 軟體安全計畫(Open Web Application Security Project, OWASP)為一個開放社群、非營利性組織，主要目標係研議協助解決 Web 軟體安全之標準、工具與技術文件，美國聯邦貿易委員會(FTC)並強烈建議所有企業需遵循 OWASP 所發佈的十大 Web 弱點防護守則，並已將其列為最佳實務。2014 年針對行動裝置所發表更新之 10 大風險及其相對之防護守則如下：

M1	**脆弱之伺服器端控制(Weak Server Side Controls)** 防護守則：開發伺服器端應用程式應避免產生 Cloud Top 10 risk 及 OWASP Top 10 2013 所列相關風險。
M2	**不安全之資料儲存(Insecure Data Storage)** 防護守則：不將敏感資料存放於開放式之儲存媒體如：SD 卡，僅儲存必要資訊並採用檔案加密應用程式介面，設定檔案讀寫權限。
M3	**傳輸層保護不足(Insufficient Transport Layer Protection)** 防護守則：確認所有敏感性資料均採用 SSL/TLS 加密方式傳輸，

13. Federal Reserve System, STREAM

	傳輸媒介包含網路連線、Wi-Fi 連線、近場通訊(Near Field Communication, NFC)等。
M4	**非故意資料洩漏(Unintended Data Leakage)** 防護守則：瞭解行動裝置所使用之作業系統、輸入及交易平台、其他資料儲存等開發架構，再據以採用相對之控制方式如：依部分應用程式會儲存帳號、密碼等敏感性資訊，得手動解除自動儲存功能。
M5	**身分或交易授權與認證不嚴謹(Poor Authorization and Authentication)** 防護守則：APP 程式開發應自伺服器端強化認證工作，並使用嚴謹之身分驗證與授權如：雙因子認證。
M6	**加密失效(Broken Cryptography)** 防護守則：APP 程式開發者應避免使用過時或金鑰長度不足之加密演算法，所選用之強健加密演算法並經不斷反覆測試。
M7	**使用者端注入(Client Side Injection)** 防護守則：APP 程式開發者應注意透過客戶端可能之攻擊如：SQL 執行語法(SQL injection)、特殊字元等，充份過濾不受信任之內容。
M8	**安全決策透過不受信任之輸入(Security Decisions Via Untrusted Inputs)** 防護守則：APP 程式開發者應注意經由惡意攻擊者以略過應用程式權限檢核或安全控制之可能性。
M9	**不適當之連線處理(Improper Session Handling)** 防護守則：避免使用行動裝置之硬體識別碼為連線值，並將連線值過期時間設定於可接受範圍內，以兼顧預防攻擊者輕易猜到帳號、密碼等機敏連線內容，以及使用者無須常常因離線而重新驗證。
M10	**原始程式碼缺乏保護(Lack of Binary Protections)** 防護守則:程式開發者應遵循APP程式碼撰寫最佳實務如Android或iOS specific best practices。

圖 11：OWASP 發表行動裝置前十大風險[14]

3.檢查人員對行動理財產品應關注之重點

(1).機構是否能掌控行動理財產品之發展，包括瞭解複雜行動支付系統之互通性

(2).機構是否能掌控包括非銀行業協力廠商、網路設備、服務供應商等之 RFP 及 SLAs

(3).瞭解行動理財服務之交易授權模式及處理作業

(四)授權認證機制

1.身分認證與授權模式通常包括：

(1).「知道什麼？」如 PIN 碼、密碼、帳號、使用者 ID

(2).「有什麼？」如憑證(token)、智慧卡

(3).「是什麼？」如生物辨識

(4).單因子或多因子認證

2.行動銀行之認證與授權

傳統電子銀行之網頁授權與認證係指透過表單(forms-based)或 HTTP 進行驗證，自使用者端於網頁輸入使用者名稱、帳號等方式與伺服器來回傳遞及認證，行動銀行較為普及後，相關技術與安全性易漸受

14.開放 Web 軟體安全計畫(Open Web Application Security Project, OWASP)網站，https://www.owasp.org/index.php/File:Mobile_Top_10_2014.png

重視，認證程序為設備認證、應用程式認證、安全交易。與會學員詢及，對於使用者而言，於傳統網頁得透過網址確認其真實性，惟行動銀行係來自 APP store 或 Android play store 等 APP 商店所安裝提供，至該 APP 是否為金融機構官方而非偽造之網址，講師亦說明目前尚無法確認 APP 真實之 URL。

3. 檢查人員對認證與授權機制應關注之重點

(1). 網路銀行均應具備多層身分認證機制

(2). 所有系統均應遵循密碼規則

(3). 持續評估新風險並適時更新認證及授權機制

(五)社群媒體與相關風險

1. 社群媒體係指透過網際網路應用程式及廣播功能用以分享意見、資訊之平台，相對因用戶於社交網路建立及交換資訊內容亦形成潛在風險，金融機構之社群媒體使用型態包含：僅有少數例外之完全封閉式、僅供內部使用、僅可使用部分受允許之社群網路、開放所有社群媒體之使用。

圖 12：社群媒體平台[15]

15. 開放 Web 軟體安全計畫(Open Web Application Security Project, OWASP)網站，https://www.owasp.org/index.php/File:Mobile_Top_10_2014.png

2.社群媒體風險

(1).資訊外洩

員工及/或客戶無意或故意洩露資訊，可能損害機構聲譽或違反其員工或客戶之隱私權。

(2).貶損性或假資訊

不滿之客戶、員工、競爭對手或其他惡意行為者利用社交網站傳播虛假、誤導或負面資訊，致損害機構聲譽。

(3).遭惡意軟體攻擊、社交工程及其他安全性威脅

因進行社交工程演練而使用社群網路，可能暴露大量之個人及企業資料，社群媒體執行之小應用程序、廣告軟體、驅動下載軟體，以及其他可執行之功能，均可能傳遞惡意軟體予用戶。

3.檢查人員對社群媒體應關注之重點

(1).社群媒體政策與治理

①金融機構是否使用社群媒體? 允許及禁用之社群媒體為何?

②是否訂定管理政策? 並瞭解參與訂定政策人員,機構風險管理架構是否涵蓋社群媒體相關風險?

③檢視政策是否考量其他國家或地區之法規遵循情形?

④是否在訂約前實地查核社群媒體之協力廠商?

(2).社群媒體內部控制制度之建立情形。

(3).社群媒體對資安事件之回應機制

①回應機制使用之工具為何?

②意外事件是否影響營運、機構聲譽?

③內部訓練是否包含社群媒體之風險與威脅

伍、 心得與建議

一、建立金融科技跨領域工作小組，納入金融各業別、資安、法務人員

金融科技(FinTech) 並非單純將既有金融產品與服務加上資訊科技，而是以消費者需求與市場機會為主並融合金融與資訊科技領域，所發展出以科技提供創新之金融服務，其中涉及財務會計、法務、電子商務、數位科技及資訊安全等專業領域，目前大陸銀監會係於 2012 年設立銀行業信息科技監管部，專責銀行業資訊科技監管督導和專項排查(專案檢查)，另美國 FED 在監理銀行業之雲端委外服務，已規定監理及檢查人員於業者委託前，即須參與審閱相關合約內容，顯示監理機關因應金融科技之發展，相關監督與檢查已不僅止於針對金融各業別與資訊安全領域，所涉委外契約或金融專利等相關金融法務亦是必要之一環。監理機關針對 FinTech 趨勢及金融業發展數位金融現況，建議也能納入法務人員之參與。

二、勇於嘗試新風險管理或監理與檢查方法、工具

本次研討會主題之關鍵字為：「科技」、「風險」、「監理」，面對科技不斷創新，監理與風險管理往往僅能在後端追逐把關，如何使監理和風管不致與科技前進之步伐落差過大，建議金融機構之風險管理機制宜居於新興科技業務推展之前，充份國際化，勇於嘗試國際新型風險管理方法或內部稽核工具，如雲端運算或儲存委外前，是否已確實掌握可能之技術、政策及法律風險，是否密切關注國際資安組織動態如國際雲端安全聯盟(Cloud Security Alliance, CSA)對雲端運算之機敏區域安全規則。

監理與檢查機關除密切關注國際金融科技趨勢外，對於大數據、行動金融等服務，亦宜多方瞭解與運用新興稽核工具，另美國 FED 等監理機關係運用各式免費之工具進行金融機構之網路或資訊系統安全檢測，如 Nmap 掃描網路連結以蒐集目標主機連線資訊，進行漏洞掃描、Metasploit 協助進行滲透測試及入侵檢測、Maltego 用以蒐集 Email, Twitter, Facebook 及主機系統之網路架構等，如基於檢查人員尚不宜直接進入業者之資訊系統，建議得透

過檢視機構產出之相關報告，藉以瞭解金融機構之網路環境是否存有潛在威脅關係。

三、建立金融科技簡易知識庫，強化監理檢查人員之專業持續進修

金融服務因科技導入而有日新月異之進步，金管會監理與檢查人員對於金融科技相關知識除自我摸索，以及透過金融研訓院、中華民國電腦稽核協會等外部教育訓練強化外，建議初期監理機關得於內部網路建置金融科技相關之小型知識庫，透過專責人員定期搜尋瞭解國內外相關資訊如：國內、外金融科技監理法規、檢查指引或手冊、創新金融或電子商務服務與問題等，篩選具學習或參考價值之新知，建置於內部網路供監理與檢查人員隨時瀏覽，未來亦得於金管會檢查局外部網路比照「稽核專區」之概念，設立「金融科技專區」。

四、賡續因應金融服務科技化發展及先進國家作法，調整監理與檢查重點

金管會檢查局目前對資訊作業之查核重點包括網路金融業務之管理如：網路金融業務(含線上金融服務、行動支付、兼營電子支付機構業務)之系統安控、交易安全設計及網路安全措施(如：防火牆、入侵偵測防禦及弱點掃描等資安防禦措施、異常事件預警監測機制、電子郵件社交工程演練及資安教育訓練)，因應金融科技發展，亦已調整資訊安全查核重點，如增列電子銀行、手機信用卡安控基準之查核、行動應用 APP 安全管理等。然而舉凡大數據、智慧網路、移動裝置、雲端運算、社群媒體、物聯網、生物辨識及機器人等均屬運用科技之創新金融內涵，監理機關面對金融服務科技化之趨勢，大部分傳統之資訊風險評估方法未必能逕行適用於新興科技，建議得關注先進國家之作法，如美國聯邦金融機構檢查委員會(Federal Financial Institutions Examination Council, FFIEC)已制定電子商務應建立之強健認證機制與詐欺偵測機制之指導方針、雲端運算委外服務廠商之安全性等，強化我國現行金融科技之查核重點。

五、因應金融業跨境業務，建立國際監理機關聯繫機制與窗口

金管會為延伸台灣金融業之服務觸角，掌握亞洲市場發展契機，分散風險，正積極推動金融業亞洲布局，而金融機構跟隨政策開放之腳步，亦持續積極拓展跨境金融業務與市場版圖，如跨境、跨產業、跨虛實整合之電子商務，金融機構在進行任何跨境業務活動前，均應熟稔當地法律規定及監理規範之適用與遵循情形，而監理機關亦應透過官方網站、金融監理合作瞭解備忘錄(MoU)機制等管道，瞭解各跨境金融業者之法令遵循情形，然基於業務細節繁複或其他考量因素，如未能透過正式管道取得資訊，建議將經由受訓或參訪等方式所結識之人員，建立為非官方之國際監理機關聯繫窗口，以作為日常監理或檢查之諮詢來源之一。

六、鼓勵金融業者提供健全實務或最佳範例

中國大陸對新創事業通常給予較大發展空間，待市場逐步成熟再思考監管之問題，在放任創新且無監管規範之情況下，往往形成難以控制之市場，然而考量監理規範未必能領先或預知市場之創新機制或產品，無法走在市場最前端，如果過度嚴格或保守，亦將限制產業之創新與發展，在過猶不及之權衡下，建議監理機關得透過誘因鼓勵金融業者將新創服務之構思與相應之風控制度提出健全實務或最佳範例(sound practices, best practices)，除能讓業者引領市場並作為其他業者之參考範本外，亦使監理機關能兼顧業者之新創服務與風控。