行政院所屬各機關因公出國人員出國報告書

（出國類別：其他）

參加 SEACEN 舉辦之「第 2 屆支付及清算系統監管」訓練課程出國報告

服務機關：中央銀行

姓名職稱：陳啟超，三等專員

派赴國家：越南

出國期間：104 年 3 月 21 日至 104 年 3 月 28 日

報告日期：104 年 6 月 25 日

目錄

壹、 前言 1
貳、 金融市場基礎設施準則及其評估方法 2
一、 金融市場基礎設施準則之發展沿革 2
二、 PFMI 資訊揭露架構及評估方法 4
三、 PFMI 評估案例—馬來西亞 10
四、 集中交易對手量化資訊公開揭露標準 13
參、 歐元體系金融市場基礎設施之監管 16
一、 制度架構 16
二、 法規環境及監管發展 17
三、 歐元體系之監管方法 22
肆、 香港零售支付系統監管之發展 24
一、 監管現況 24
二、 未來新的監管制度 24
伍、 金融市場基礎設施之網路防護 28
一、 國際現況 28
二、 2 小時復原時間目標 28
三、 網路攻擊的來源 29
四、 網路防護整合式方法 30
陸、 心得與建議 36
一、 心得 36
二、 建議事項 37
參考文獻 40

壹、前言

本次奉派參加東南亞國家中央銀行研訓中心(SEACEN)於本(2015)年3月22日至27日在越南河內舉辦之第2屆「支付及清算系統監管課程」，參加學員來自18個國家或地區，共計37人。本次課程邀請之講師分別來自「支付暨市場基礎設施委員會」[1](Committee on Payments and Market Infrastructures, CPMI)及泰國、馬來西亞、印度、菲律賓等國家之支付清算部門專家。

本次課程內容包括大額及零售支付系統之監管、國際間對於金融市場基礎設施(Financial Market Infrastructure, FMI)之監管標準及相關評估方法、各類 FMI 間之相互依存性、網路安全之防護。此外，本次課程亦安排個案討論，模擬某一新興經濟體如何根據「金融市場基礎設施準則」(Principles for financial market infrastructures, PFMI)，對於該經濟體之大額及零售支付系統進行評估，藉此讓參訓學員能對 PFMI 準則能有基本的概念，俾將其落實在自己國家之監管實務上，參訓學員亦可藉由個案討論之機會，分享彼此國家在監管支付及清算系統方面之經驗。

安全且有效率的 FMI 有助於維持及促進金融穩定與經濟成長。鑑於許多國家已採用 PFMI 準則監管支付及清算系統，本行及相關主管機關似宜跟進採用，俾在國際準則之適用與監管作業上，能與其他國家有一致性的標準；因此，本報告書於第貳章介紹 PFMI 準則之發展緣由，並說明該準則之評鑑方法及資訊揭露標準，再以馬來西亞為例，介紹國際貨幣基金(International Monetary Fund, IMF)及世界銀行(World Bank, WB)依據 PFMI 準則對該國 FMI 所作之評鑑結果。接著，為了解先進國家對於 FMI 及電子支付工具之監管方式，以供本行研擬相關政策之參考，本報告書分別於第參章及第肆章介紹歐元體系對於 FMI 之監管，以及香港對於零售支付工具之監管；第伍章則探討 FMI 在網路防護方面相關議題；最後提出個人參加此次訓練課程的心得與建議。

[1] 「支付暨清算系統委員會」(Committee on Payment and Settlement Systems, CPSS)自 2014 年 9 月 1 日起更名為「支付暨市場基礎設施委員會」。

貳、金融市場基礎設施準則及其評估方法

一、 金融市場基礎設施準則之發展沿革

金融市場基礎設施(Financial Market Infrastructure, FMI)係指參加機構間(包括系統營運者)之多邊系統，用以處理支付、證券、衍生性商品或其他金融交易之結算、清算或記錄作業。金融市場基礎設施有助於強化其所服務的市場，促進金融穩定；另一方面，卻可能因各項設施間之相互依存性而使風險集中化，若未適當管理，可能使金融體系遭受重大風險，最終演變成系統性風險，甚至會波及其他的金融市場。因此，CPMI 與國際證券管理組織(the International Organization of Securities Commission, IOSCO)自 2001 年起開始針對各類金融市場基礎設施，陸續發布「重要支付系統之核心準則」(Core Principles for Systemically Important Payment Systems)、「證券清算系統建議準則」(Recommendations for Securities Settlement Systems)及「集中交易對手建議準則」(Recommendations for Central Counterparties)等國際標準，該等準則亦可作為各國中央銀行、監理機關及相關主管機關在設計與評鑑金融市場基礎設施的主要依據。

為記取金融危機的教訓，以及呼應 G20 與金融穩定委員會(Financial Stability Board, FSB)希望檢討現行標準並擴大其適用範圍，以強化核心的金融市場基礎設施的目標，CPSS 及 IOSCO 爰於 2010 年 2 月開始全面檢討上述準則所制定的標準，在廣泛徵詢市場意見後，於 2012 年 4 月發布最終版的「金融市場基礎設施準則」(Principles for Financial Market Infrastructures, PFMI)報告書，計有 24 項準則，使金融市場基礎設施得以適應更大的不確定性及風險。至於各類型金融市場基礎設施所涉及的 PFMI 準則，詳如表 1。此外，PFMI 亦就中央銀行及相關主管機關制定以下 5 項職責，希望各國主管機關在法律制度許可範圍下，逐步將該報告書所提示的準則及職責納入法規與管理架構。

- 職責 A：金融市場基礎設施之管理監理及監管
- 職責 B：管理、監理及監管之權力與資源
- 職責 C：金融市場基礎設施相關政策之揭露
- 職責 D：金融市場基礎設施準則之適用
- 職責 E：與其他主管機關之合作

表 1　各類型金融市場基礎設施對於 PFMI 之一般適用性

準則	支付系統	證券集中保管機構	證券清算系統	集中交易對手	交易資料保管機構
準則 1：法規基礎	✓	✓	✓	✓	✓
準則 2：治理機制	✓	✓	✓	✓	✓
準則 3：全面性風險管理架構	✓	✓	✓	✓	✓
準則 4：信用風險	✓		✓	✓	
準則 5：擔保品	✓		✓	✓	
準則 6：保證金				✓	
準則 7：流動性風險	✓		✓	✓	
準則 8：清算最終性	✓		✓	✓	
準則 9：款項清算	✓		✓	✓	
準則 10：實體交割		✓	✓	✓	
準則 11：證券集中保管機構		✓			
準則 12：價值交換清算系統	✓		✓	✓	
準則 13：參加者違約之處理規約與作業程序	✓	✓	✓	✓	
準則 14：CCP 參加者客戶部位之區隔與可移轉性				✓	
準則 15：一般營業風險	✓	✓	✓	✓	✓
準則 16：保管與投資風險	✓	✓	✓	✓	
準則 17：作業風險	✓	✓	✓	✓	✓
準則 18：加入與參加標準	✓	✓	✓	✓	✓
準則 19：層級化參加機制	✓	✓	✓	✓	✓
準則 20：金融市場基礎設施之連結		✓	✓	✓	✓
準則 21：效率與效能	✓	✓	✓	✓	✓
準則 22：通訊作業程序與標準	✓	✓	✓	✓	✓
準則 23：規約、重要作業程序及市場資料之揭露	✓	✓	✓	✓	✓
準則 24：交易資料保管機構對市場資料之揭露					✓

資料來源：整理自 PFMI 報告書內容

二、 PFMI 資訊揭露架構及評估方法

(一)揭露架構

CPSS 及 IOSCO 為促進各會員國金融市場基礎設施及其主管機關遵循 PFMI 報告中所制定的準則及職責，於 2012 年 12 月公布「金融市場基礎設施準則：資訊揭露架構及評估方法」(Principles for financial market infrastructures: Disclosure framework and Assessment methodology)，此份報告屬於 PFMI 報告的補充報告，係將之前與 PFMI 報告同時公布的評估方法與資訊揭露架構兩份文件，加以整合。

「資訊揭露架構」規定 FMI 根據 PFMI 準則 23 所應公開揭露的形式及內容，以提升 FMI 相關資訊的透明度，使參加者、相關主管機關及社會大眾得以更清楚地了解 FMI 的公司治理、營業活動、風險概況及風險管理實務，進而支持 FMI 及其利害關係人所做的決策；其所揭露的各項資訊亦將成為評估方法的重要參考之一。標準化的資訊揭露架構也有利於對不同的 FMI 進行比較。FMI 應完成本報告所提供的資訊揭露範本，此範本包含以下 5 個部分：資訊揭露的重點；前次揭露以來的重大改變； FMI 的基本資料、營運表現、組織架構、法規架構及系統設計；適用準則的相關資訊；可對外提供的資源。此外，CPSS 及 IOSCO 已在研議特定型式的 FMI 應更常揭露的重要量化資訊。

(二)評估方法

為促進及監視各會員國對於 PFMI 報告所訂定各項準則的遵循情形，「評估方法」提供評估者有關如何進行 PFMI 評估作業的指引。「評估方法」之目標係判定 FMI（或主管機關）是否符合準則（職責）及符合之程度，並協助辨識可以改善之處。對於 FMI 而言，「評估方法」可做為決策時有用的工具，例如 FMI 在考慮引進新產品或服務時，或政策、規約、作業程序有重大改變時，均可引用「評估方法」，俾確保所規劃的改變不會破壞其對 PFMI 之有效遵循。此

外，FMI 亦可運用「評估方法」定期進行自我評估，以辨識有待改善之處及所需的資源。各國相關主管機關應定期依據「評估方法」對該國之 FMI 進行評估，目標放在辨識出潛在的風險及消除該等風險的建議行動，而此類評估作業對於那些因 FMI 涉及跨幣別或跨境交易而須與他國合作監理的主管機關而言，尤為重要。此外，IMF 及 WB 之「金融部門評鑑計畫」(Financial Sector Assessment Program, FSAP)，亦將使用「評估方法」進行外部評估，其目的在於辨識出影響全球金融穩定的風險及需要改善的領域，同時也進行跨國比較，以發掘最佳實務。「評估方法」包括以下 6 個步驟：

- 決定適當的評估範圍：評估者須謹慎衡酌要進行評估的 FMI、該 FMI 的作業與服務，及適用之 PFMI 準則為何? 並應事先就上開問題與被評估的 FMI 清楚地溝通。
- 蒐集每一關鍵考量的事實：評估者應蒐集足夠的事實，俾能針對 PFMI 每項準則做出結論，而評估方法在每項準則之關鍵考量(key considerations)下所列問題，有助於評估者蒐集相關事實，以決定是否遵循該項準則。
- 對每一項準則做出主要結論：主要結論(Key conclusions)係指評估者就受評金融基礎設施有關某項準則遵循程度所做之決定，而每一項適用之準則均應做出主要結論，並摘要方式描述主要結論。評估者必須找出與關鍵考量有關的缺失，並描述每一項缺失下的風險及其隱含之意義，最後做出結論。
- 對每項準則之遵循情況予以評等：評估方法論之評等架構針對評估者要如何評定每一項準則的遵守程度，提供指引。該評等架構根據評估者辨識出「關切議題」必須解決之重要性及急迫性，列出 5 種等級的判斷標準（如表 2），評估者應依評估當時的狀況賦予不同的等級。

表 2　PFMI 評等等級及其說明

等級	說明
符合 **(observed)**	該 FMI 符合本項準則。任何被辨識的落差或缺點不是「關切議題」，且非常小並可控制，該 FMI 在例行作業中即可考量予以解決。
大部分符合 **(broadly observed)**	該 FMI 大致符合本項準則。評估已辨識出一個或多個「關切議題」，該 FMI 應在明確時程內予以改善。
部分符合 **(partly observed)**	該 FMI 僅部分符合本項準則。評估已辨識出一個或多個嚴重的「關切議題」，如未及時處理，問題可能變嚴重。
不符合 **(non-observed)**	該 FMI 未符合本項準則。評估已辨識出一個或多個嚴重的「關切議題」，且必須立即採取行動，因此，該 FMI 應最優先處理該等議題。
不適用 **(not applicable)**	因為該 FMI 的特殊法規、功能、結構或其他特性，本項準則不適用於該 FMI 類型。

資料來源：整理自 CPSS-IOSCO(2012),"Principles for Financial Market Infrastructures : Disclosure framework and Assessment methodology," p.10

- 對每個關切問題提出適當的改善時程：

評估報告的結論，必須針對未能完全符合準則的事項，即所辨識出的「關切議題」，提供建議措施，且須訂定合理改善時程，俾使該 FMI 做出必要的改變。

CPMI 及 IOSCO 雖未列出各項準則的重要性，但評估者應基於該 FMI 最嚴重風險、最欠缺透明度或效率之所在，判斷問題嚴重性，據以排定處理的優先順序。辨識出優先順序後，評估者應決定每個領域必須採取的行動(actions)。若評估報告是由本國主管機關完成者，金融市場基礎設施通常需自行準備一份行動計畫供主管機關審查；若評估報告係由外部評估者完成者，該外部評估者通常會提供改善建議並與主管機關進行討論。

對於非屬「關切議題」之落差或缺點，評估者亦應提出改進建議方案；惟對這些建議之執行，並沒有硬性規定及特定改善時

程，FMI 可考慮將改進方案在例行作業中予以解決。

- 準備評估報告：評估者可根據 CPMI-IOSCO 發布的「金融市場基礎設施準則：資訊揭露架構及評估方法」報告附錄 B 之格式，撰寫遵循 PFMI 的「自我評估報告」。

(三)評估報告格式

1. 摘要：應強調評估報告的主要發現。

2. 前言：說明下列與評估有關的重要資訊

- 評估者：說明接受評估的 FMI 及進行評估的單位。
- 評估目標：說明評估的目標及內容。
- 評估範圍：說明受評的 FMI、受評 FMI 的營運與服務項目，以及所要評估的準則。
- 評估的方法：說明評估的程序。若非所有的準則均進行評估，應說明該等準則未進行評估之原因。
- 評估的資料來源：說明進行評估所使用資料的主要來源，包括公開及非公開的來源。這些來源可能包括書面文件（例如其他的評估報告、調查、問卷、研究報告、相關法規及產業指引）及與受評 FMI、主管機關或產業相關人士（例如參加者、其他 FMI、股票交易所、保管機構、證券自營商、終端用戶協會）之對話。

3. 受評機構辦理支付、結算及清算之概廓

本段應概括性描述受評 FMI 在支付、結算及清算的角色，以及其作業與服務內容，並提供簡要統計資料，俾有助於瞭解該 FMI 的業務範圍。上開描述及簡要統計資料應有助於與其他 FMI 比較。此外，本項亦應描述與受評 FMI 相關的法規、監理、監管架構及主管機關，並摘陳近年來已執行的重大變革或短期內規劃進行的重大變革。

4. 評估摘要

本段應總結詳細評估各項準則後的主要發現，並編製評估結果彙整表（如表 3）。對於每項準則，評估報告應：

- 強調 FMI 的關鍵實務及成就。
- 列出已辨識的關切問題。
- 對於未能完全符合的準則，應分別給予評論，並說明給予「大致符合」、「部分符合」、「不符合」等級的主要理由；指出造成未完全符合準則的風險因子，以及「關切議題」是否被處理，或持續改善後可達到的符合程度。

表 3　評等結果彙整表

評估等級	準則項目
符合	例如準則 1、3、6、8
大部分符合	
部分符合	
不符合	
不適用	

資料來源：同表 2， p.85。

5. 給予 FMI 之建議

評估者應列出 FMI 遵循 PFMI 準則時之關切議題、其他落差或缺失，以及任何建議改善措施及其行動時程（如表 4）。評估者應將建議改善措施按處理之優先順序排列。評估者亦應說明建議行動導致符合等級改善之方法，若 FMI 的改善計畫正在進行，或遭遇任何的阻礙，評估者均應加以註明。

表 4　建議改善措施的優先順序

準則	關切議題及其他落差或缺失	建議行動及評論	處理建議行動之時程

資料來源：同表 2， p.86。

6. 詳細評估報告

詳細評估報告（格式如表 5）應說明受評 FMI 適用的主要考量、主要結論及每項適用準則之評等等級。

表 5　遵循準則之詳細評估

對每一適用之準則而言	
準則 X 準則內容	
主要考量 N 主要考量內容	本章應提供與主要考量有關之 FMI 實務作業資訊。評估者應依每一主要考量所設定之問項指引，並依第 5 章所提供問項組合之標題排列資訊。只要選擇受評類型 FMI 所適用之主要考量。回答內容應反映 FMI 營運者及參加者的實際作業。
主要結論	本章應摘要敘述評估者為每一主要考量蒐集佐證事實而取得之主要資訊。摘要敘述應彙總 FMI 的作業與成效，描述任何考量議題的嚴重性，以及確認其他任何的落差或缺失。
評等結果	本章應敘明是「遵循」、「大致遵循」、「部分遵循」、「未遵循」或「不適用」準則，並說明評定為該等級之理由。
建議及評論	本章應為每一確認的考量議題及其他任何落差或缺失提供建議與評論。

資料來源：同表 2， p.86。

三、 PFMI 評估案例—馬來西亞

IMF 與 WB 之「金融部門評鑑計畫」(Financial Sector Assessment Program, FSAP)於 2012 年 7 月根據 CPMI 及 IOSCO 所發布的 PFMI 準則及其資訊揭露架構與評估方法，對於馬來西亞相關主管機關及重要金融基礎設施進行評估，並於 2013 年 2 月完成詳細評估報告，以下茲就該份報告之內容，概述如次：

(四)接受評估之金融市場基礎設施

1. 即時電子化資金及證券移轉系統(Real Time Electronic Transfer of Funds and Securities, RENTAS)：包括即時總額清算系統(Real Time Gross Settlement System, RTGS)、證券清算系統(Securities Settlement System, SSS)及證券集中保管機構(Central Securities Depository, CSD)等子系統。
2. 馬來西亞證券結算系統(Bursa Malaysia Securities Clearing, BMSC)
3. 馬來西亞衍生性商品結算系統(Bursa Malaysia Derivatives Clearing, BMDC)
4. 馬來西亞存託系統(Bursa Malaysia Depository, BM Depo)

(五)監管之法規架構

就支付清算系統而言，相關的法規架構分為兩類，一類是規範支付系統及政府債券的「馬來西亞中央銀行法(Central Bank of Malaysia Act 2009, CBA)」及「支付系統法(Payment System Act 2003, PSA)」，前者賦予馬來西亞央行擁有及營運支付清算系統的權力，後者則強化馬來西亞中央銀行監管支付清算系統的權力，明確賦予馬來西亞央行負責促進全國支付清算系統有效率、順暢運作的權限。

另外規範股權、債券及衍生性商品之結算與清算系統的法律包括「證券委員會法(Securities Commission Act, SCA)」、資本市場暨

服務法(Capital Markets and Services Act 2007, CMSA)、證券產業集中保管機構法(Securities Industry Central Depositories Act, SICDA)。其中 SCA 明訂馬來西亞證券委員會的職責及運作機制，CMSA 提供證券市場各類機構(例如證券交易所、結算機構及交易資料保管機構)運作的整體架構，並要求證券交易所及結算機構應將公眾利益、系統之安全與效率性，凌駕於本身商業目標之上，且應建立規約及作業程序，特別是與參加者違約之處理有關的部分。SICDA 則是提供有價證券存託及不移動化之法規架構。

(六)監管機制

馬來西亞的「支付系統法」及「中央銀行法」授權該國中央銀行擔任支付系統、證券清算系統及公債集中保管機構的監管者，該行依據支付系統法，可基於具系統重要性或公共利益等理由，指定應接受該行監管的支付系統，目前已指定 RENTAS 系統（包含 RTGS、證券清算及證券集中保管 3 個子系統）及 Espick 系統（票據結算系統）須接受監管。該等系統須符合國際標準，特別是 CPSS 及 IOSCO 所發布者，亦應定期提報詳細的業務資訊。此外，該等系統的規約及作業程序應經馬來西亞央行許可，央行會定期與系統營運者進行對話，以及有權進行稽核及要求提供所需資訊。

馬來西亞的「證券委員會法」及「資本市場服務法」授權證券委員會監管資本市場及所有與其相連結機構（包括 BMSC、BMDC、BM Depo）之順暢運作，其可要求該等機構定期報送資料、所有規約及作業程序須經證券委員會核准，以及符合 CPSS 與 IOSCO 發布之國際標準，亦可定期進行稽核。

(七)PFMI 準則之評估結果

本次國際貨幣基金(IMF)及世界銀行(World Bank)之「金融部門評估計畫」針對馬來西亞重要金融市場基礎設施所做評估結果彙整如表 6，以下說明評估人員對於 RENTAS 系統及主管機關職責所提出的建議行動：

1. RENTAS 系統（包括 RTGS、CSD 及 SSS）：定期測試違約管理作業程序、強化資訊揭露並測試移轉客戶部位的能力、強化日間融通機制及附買回交易合格擔保品之法律保障、採取債券定價機構的報價，以提升合格擔保品價格之可靠性[2]、嚴格驗證系統參加者的營運不中斷機制。

2. 主管機關：馬來西亞之央行及證券委員會應對社會大眾加強揭露其監管政策，以及持續擴大資訊交換的範圍，共同努力增強支付清算系統的安全、效率及可靠性；此外，雙方亦可利用新簽署的備忘錄強化合作監管。

表 6　馬來西亞 FMI 及主管機關職責之評鑑結果

評等 / 系統	符合	大部分符合	部分符合	不符合	不適用
RENTAS 之 RTGS	準則 1,2,3,4,5,7,8,9,12,13,15,16,17,18,20,21,22,23				準則 6,10,11,14,19,24
RENTAS 之 CSD 及 SSS	準則 1,2,3,4,5,7,8,9,11,12,13,15,16,17,18,20,21,22,23				準則 6,10,14,19,24
BMSC	準則 1,2,3,5,8,9,12,13,14,15,16,17,18,20,21,22,23	準則 7,17	準則 4	準則 6	準則 10,11,19,24
BMDC	準則 1,2,3,5,8,9,10,12,13,14,15,16,18,20,21,22,23	準則 4,6,7,17			準則 11,19,24
BM Depo	準則 1,2,3,11,11,13,15,16,18,21,22,23	準則 17			準則 4,5,6,7,8,9,10,12,14,19,20,24
主管機關之職責	職責 A、B、D	職責 C、E			

資料來源：IMF 及 WB

[2] 目前馬來西亞日間融通機制擔保品之評價是根據主要交易商的報價。

四、 集中交易對手量化資訊公開揭露標準

PFMI 準則 23 要求 FMI 至少應提供交易量及交易金額等「基本資料」予其參加者、相關主管機關及社會大眾，亦要求 FMI 應公開揭露本身的財務狀況、支持潛在損失的財務資源、清算時間表及其他營運表現統計資料等量化資料。CPMI 及 IOSCO 於 2015 年 2 月公布了集中交易對手(Central counter party, CCP)應遵循之「集中交易對手量化資訊公開揭露標準(Public quantitative disclosure standards for central counterparty)」，並鼓勵各會員國集中交易對手儘早（最遲於 2016 年 1 月前）公開揭露上述標準所規定的量化資料（表 7），嗣後並依上述標準所訂頻率更新資料。

(一)揭露目的

CPMI 及 IOSCO 要求 CCP 公開揭露量化資訊之目的係為使 CCP 的利害關係人（包括主管機關、直接或間接的參加者）及社會大眾可以進行下述作業：

1. 比較 CCP 之風險控制，包括 CCP 的財務狀況及抵擋潛在損失的財務資源。
2. 對於 CCP 涉及的風險有清楚、正確及充分的了解。
3. 了解並評估 CCP 的系統重要性，以及其對所服務的國家或地區、或所連結之基礎設施所造成的系統性風險。
4. 了解並評估直接及間接參加 CCP 的風險。

由於各家 CCP 進行交易的產品不同，CCP 在公開揭露量化資訊之同時，應輔以適當的註釋說明，俾使外界能正確理解其所揭露的資料。CPMI 及 IOSCO 在制定 CCP 量化資訊公開揭露標準時已徵詢各會員國 CCP 及其參加者的意見，試圖避免對 CCP 造成不合理或不成比例之額外負擔，因此，CCP 公開揭露的量化資訊係以其日常作業及風險管理所蒐集及維護的資訊為主，幾乎都是匿名且屬合計數，並制定資料的精細度(degree of granularity)，以避免洩漏 CCP 個別參加者之交易部位等敏感資訊。

(二)揭露頻率

為利對於 CCP 之評估及比較，「集中交易對手量化資訊公開揭露標準」要求 CCP 公開揭露量化資訊的頻率（多為每季或每年）較 PFMI 準則資訊揭露架構（至少 2 年更新 1 次）為高。CPMI 及 IOSCO 希望各會員國 CCP 使用相同的量化資訊揭露範本，以及提供時間序列資料，將每次公開揭露之資訊保留於網站上供外界使用，同時亦應確保資料之正確性。

表 7　CCP 公開揭露之量化資訊及頻率

PFMI 準則	應揭露量化資料	揭露頻率
準則 4 信用風險	因應違約事件的財務資源(例如自有資本、參加者提撥保證金、存放央行或商業銀行之現金、公債)總額	每季
準則 5 擔保品	充當原始保證金(initial margin)之合格資產及適用之折減率(haircut)	異動即更新
準則 6 保證金	1. 結算服務需要之原始保證金總額。 2. 個別合約設定之原始保證金比率。 3. 平均每日參加者支付之變動保證金總額。	1. 每季 2. 異動即更新 3. 每季
準則 7 流動性風險	1. 每項結算服務之合格流動資源(例如存放央行及具信譽商業銀行之現金、約定的信用額度、存放保管機構具高度變現性的擔保品)。 2. 在極端但可能的市場情況下，參加者及其聯屬機構發生違約，面臨最大的支付債務總額。	1. 每季 2. 每季
準則 12 價值交換清算系統	DvP、DvD 或 PvP 清算機制之清算比重（按金額及交易量）	每季
準則 13 參加者違約之處理規約與作業程序	1. 損失金額與原始保證金總額 2. 用以吸收損失的其他財務資源 3. 客戶部位結清(closed-out)之比率	事後
準則 14 區隔與可移轉性	所有客戶在以下帳戶之部位： 1. 個別獨立帳戶 2. 綜合性(omnibus)客戶帳戶 3. 法律區隔但作業合併(legally Segregated but operational Comingled)帳戶 4. CCP 與客戶合併(comingled)帳戶	每季
準則 15 一般營業與作業風險	1. 流動淨資產及 6 個月營業費用 2. 總收入、總費用、利潤、總資產及總負債 3. 手續費收入占總收入之比重	每年

PFMI 準則	應揭露量化資料	揭露頻率
準則 16 保管與投資風險	1. 來自參加者之現金 2. 存放上開現金各類形式（存款及投資有價證券）所占比重 3. 參加者非現金資產再質押的金額及到期日	每季
準則 17 作業風險	1. 核心系統在特定期間內（例如過去 12 個月內）之作業可用性目標及實際的作業可用性 2. 系統故障而影響結算服務之次數及時間 3. 復原時間目標（例如在 2 小時內）	每季
準則 18 加入與參加標準	1. 各項結算服務之結算會員人數 2. 結算會員在 10~25 位之結算服務： (1) 最大 5 家結算會員未平倉部位之比重 (2) 最大 5 家結算會員原始保證金之比重 (3) 最大 5 家結算會員出資違約保證金金額之比重 3. 結算會員超過 25 位之結算服務： (1) 最大 5 家及最大 10 家結算會員未平倉部位之比重 (2) 最大 5 家及最大 10 家結算會員原始保證金之比重 (3) 最大 5 家及最大 10 家結算會員出資違約保證金金額之比重	每季
準則 19 層級化參加機制	1. 客戶人數 2. 直接會員人數 3. 前 5 大及前 10 大結算會員客戶交易結算之比重	每季
準則 20 FMI 之連結	1. 為相連結 CPP 辦理結算之金額 2. 提供予相連結 CPP 之原始保證金與財務資源 3. 自相連結 CPP 收取之原始保證金與財務資源	每季
準則 23 規約、重要作業程序及市場資料之揭露	1. 每日平均結算交易量及名目金額（按交易工具、資產類別、幣別及集中市場與店頭市場區分） 2. 債務變更(novated)但尚未清算之證券交易之名目餘額及清算總額 3. 各履約機制或配對機構每日平均傳送之交易量及名目合約金額	每季

資料來源：作者整理自 CPMI 及 IOSCO 公布之「集中交易對手量化資訊公開揭露標準(Public quantitative disclosure standards for central counterparty)」。

參、歐元體系金融市場基礎設施之監管

一、 制度架構

(一)法規基礎

歐元體系監管功能之法律基礎明訂於「歐洲共同體成立條約(Treaty establishing the European Community)」及「歐元體系中央銀行條例議定書(Protocol on the Statute of the European System of Central Banks and of European Central Bank)」。根據「歐盟運作條約(Treaty on the Functioning of European Union)」第 127(2)條及歐元體系中央銀行條例第 3(1)條，促進支付系統之順暢運作係歐元體系內各中央銀行主要職責之一，中央銀行除了扮演監管角色外，亦扮演引領市場改變之協調者及支付清算系統營運者等角色。

歐元體系中央銀行條例第 22 條賦予歐洲中央銀行(European Central Bank, ECB)制定法規之權力，俾達到歐元體系的監管目標，確保結算及清算系統有效率且健全。ECB 於 2014 年 7 月 3 日利用其監管支付系統之權力簽署「具系統重要性支付系統規章(Systemically Important Payment Systems Regulation, SIPS Regulation)」，該規章涵蓋歐元區內所有由央行及民營企業營運之具系統重要性大額、零售支付系統。SIPS Regulation 落實 CPSS 及 IOSCO 於 2012 年 4 月發布的 PFMI，並賦予歐元區央行要求未遵循 PFMI 之系統營運者提出改善措施及裁罰的權力。

(二)監管功能之執行

為符合透明度原則，歐元體系發布幾份解釋其如何執行監管功能的文件，其中對於歐元體系監管角色有最詳盡說明之文件係 2011 年 7 月發布的「歐元體系監管政策框架(Eurosystem oversight policy framework)」。此一政策框架說明歐元體系進行監管的理由及方式、各國央行監管角色之分配（表 10）、相關

主管機關間之合作、及監管的範圍，而監管的範圍包括證券清算系統、交易資料保管機構、集中交易對手、支付系統/工具/機制、代理行及重要服務提供者等金融市場基礎設施。

表 10　歐元區央行監管角色分配表

金融市場基礎設施	歐洲中央銀行	歐元體系會員國央行
TARGET2 & EURO1	✓	
STEP2-T	✓	
CORE(FR)		✓
CLS	✓	
零售支付系統		✓
證券清算系統		✓
集中交易對手		✓
卡片支付機制		✓
Visa 歐洲	✓	
美國運通	✓	
萬事達卡		✓
SEPA Credit Transfer and Direct Debit	✓	
SWIFT		✓
SIA		✓

資料來源：Eurosystem oversight report 2014

二、 法規環境及監管發展

(一)PFMI

ECB 執委會於 2013 年 6 月採納 PFMI 作為監管各類 FMI 之標準。歐元體系認為為強化全球金融之穩定性及 FMI 管理各類風險之能力，並避免法規套利之風險，大型經濟體應即時且一致地執行 PFMI，進而確保公平的競爭環境，尤其是對全球具影響力之產業。

(二)具系統重要性支付系統之監管規定

歐洲於 2014 年 8 月 12 日開始實施的「具系統重要性支付系統規章(Systemically Important Payment Systems Regulation,

SIPS Regulation)」係規範歐元體系內由各國央行或民營機構營運，且具系統重要性的大額支付系統及零售支付系統，旨在確保支付系統妥適管理法規、信用、流動性、作業、一般業務、保管、投資等風險，以及健全公司治理。SIPS Regulation 之規定視支付系統所暴露之風險高低而所有差異，對於違反規定之系統營運者，亦訂有罰則及糾正措施。

根據 SIPS Regulation 之定義，所謂的具系統重要性支付系統係指可能引發系統性風險的支付系統。當前述支付系統本身無法保護自己免於所暴露的風險時，就會發生系統性風險。支付系統只要符合以下兩項條件，即應被視為具系統重要性支付系統或具系統重要性零售支付系統(Systemically Important Retail Payment Systems, SIRPS)：

1. 經歐元區會員國依據 98/26/EC 指令核准之系統，或營運者是在歐元區註冊之系統。
2. 一年內至少發生兩次以下情況：
   (1). 每日處理之歐元支付平均金額超過 100 億歐元。
   (2). 市占率至少符合以下一項標準：占歐元支付總交易量之 15%、或歐元跨境支付總交易量之 5%、或占單一歐元區會員國歐元支付總交易量之 75%。
   (3). 跨境活動（例如參加者與系統營運者所在國家不同，或與其他國家支付系統連結）涉及 5 個以上（含）國家，且至少處理 33%的歐元支付。
   (4). 提供其他 FMI 清算服務。

此外，歐元體系認為也可根據零售支付系統服務的地理範圍判定其是否具系統重要性。然而，這並不影響零售支付系統適用的監管規定，只影響歐元體系監管活動的組織。因此，歐元區零售支付系統依其跨境活動程度分為「歐洲具系統重要性零售支付系統(European systemically

important retail payment system, ESIRPS)」及「國內具系統重要性零售支付系統(national systemically important retail payment system, NSIRPS)」。具系統重要性之零售支付系統無法運作時，若會對歐元區造成負面影響者，即屬 ESIRPS，否則為 NSIRPS。

至於其他雖不具系統重要性，但對歐元區金融系統之安全與效率及大眾信心有其影響力的系統，各有不同的風險面向(risk profile)，歐元體系已將此類系統分為「顯著重要零售支付系統(prominently important retail payment system, PIRPS)」及其他零售支付系統，兩者差別只在於該系統在歐元區會員國國內之歐元支付市占率；若市占率達 25%以上（含）者，即屬 PIRPS；否則即屬其他零售支付系統。

2014 年 8 月 21 日，ECB 公布 4 個被視為具系統重要性的支付系統，包括由歐元體系營運之 TARGET2 系統、由歐洲銀行協會(European Banking Association，EBA)營運之 EURO1 系統與 STEP2-T 系統、及由 STET 公司營運之 CORE(FR)系統。該 4 系統至少符合以下條件中之 2 項：清算金額、市場佔有率、跨境相關性、提供服務予其他的 FMI。歐元體系每年會根據最新的統計資料，更新具系統重要性之支付系統名單。

(三)零售支付系統連結之監管期望(the Oversight expectation for links between retail payment systems, OELRPS)

零售支付系統係指處理大量、但金額相對較小之支付（例如支票、貸項撥轉及直接借記）的資金移轉系統。歐洲於 2002 年成立「單一歐元支付區(single euro payments area, SEPA)」，促使歐洲零售支付系統間連結程度提高，衍生之風險逐漸受到重視。鑑此，歐元體系認為應對零售支付系統之連結加以監管，以促使零售支付系統營運者妥適管理因連結而衍生的風險，故制訂一套零售支付系統應遵循的監管期望，即所謂的

OELRPS，計有以下 8 項期望：

1. 期望 1：與其他一個或多個零售支付系統建立連結之零售支付系統，應辨識、監視及管理連結所衍生之風險。
2. 期望 2：應具有完備、清楚及透明的法規基礎，使不同司法管轄區內的零售支付系統可相互連結，俾對相互連結之零售支付系統與其參加者提供適當的保障。
3. 期望 3：零售支付系統應謹慎評估連結衍生之作業風險，以確保資訊安全性，及 IT 設備與相關資源之可擴充性(scalability)及可靠性。
4. 期望 4：相連結之零售支付系統應密切監控且有效衡量、管理連結衍生的財務風險。
5. 期望 5：零售支付系統對於要求與其建立連結之零售支付系統，應制定客觀、公平的加入標準。
6. 期望 6：零售支付系統之連結應能滿足其參加者及市場的要求。
7. 期望 7：與連結之建立及運作相關的治理機制應清楚且透明，以提升連結之安全與效率，並兼顧相關公共利益及利害關係人之目標。
8. 期望 8：透過中介機構建立連結的零售支付系統應衡量、監視及管理因此所衍生的風險（包括法律、財務及作業等風險）。

(四)歐洲市場基礎設施監管規則(European Market Infrastructure Regulation, EMIR)

EMIR[3]於 2012 年 8 月開始生效，且是歐盟首次針對 CCP 及 TR 制定共同的監管架構。EMIR 除了落實 PFMI 外，在某些情況下甚至更為嚴格。歐洲證券市場管理局(European Securities and

[3] EMIR 之背景係源自 2009 年 G20 會議中，達成針對店頭市場衍生性商品須申報資訊之結論而制定。原訂自 2012 年 8 月 16 日生效，惟 2013 年 3 月 15 日有關補充 EMIR 內實際執行規定及監管措施之技術標準生效後，相關規範始正式施行。

Markets Authority, ESMA)以行政法規公布有關實際執行與監管作法之技術標準，於 2013 年 3 月 15 日起開始實施，用以補充 EMIR 規定，內含較詳細的要求規範。其內容主要涵蓋店頭衍生性商品交易之管理、集中結算以及交易資料保管機構三大部分。

(五)證券集中保管機構監管規則(Central Securities Depository Regulation, CSDR)

歐洲執行委員會於2012年3月公布一項改善歐盟證券清算及證券集中保管機構之安全與效率的法律提案。CSDR 自 2014 年 9 月 17 日起生效，針對歐盟 CSD 之許可及監理建立一套共同的架構，強化歐盟境內跨境清算的法律及作業條件，內容包含有價證券無實體化之義務、清算週期之協調、清算紀律措施及共同規約。

(六)支付服務指令修正案(PSD2)

歐盟執委會(European Commission)於 2013 年 7 月 24 日提出「支付服務指令修正案(Revised Directive on Payment Services)，簡稱 PSD2；PSD2 之目標包含提高歐盟支付市場的整合與效率、提昇支付服務提供者的營運範圍、確保強化支付使用者保護及資訊安全、鼓勵支付服務的減價、促進共通技術規範及互用性的形成。PSD2 的重點如下：

1. 因應科技發展及時代變遷，**擴大適用範圍**：提出第三方支付服務提供者[4](third party payment provider, TPP)之名詞定義並量身打造規範。透過手機或其他 IT 裝置進行的行動支付，若單筆支付金額超過50歐元或者是月支付金額超過200歐元也應適用 PSD2。
2. **強化資安要求**：歐盟將另提出支付服務提供者應遵循之「網路及資訊安全指令(Directive on Network and Information

[4] 第三方支付服務提供者係指基於存取其他支付服務提供者之支付帳戶（銀行帳戶或信用卡）所提供之相關服務，例如發動支付服務及帳戶資訊服務，但通常不持有客戶的資金。

Security, NIS Directive)」。歐洲銀行管理局(European Banking Authority, EBA)將與歐洲中央銀行(ECB)密切合作提出資訊安全指導原則，以輔導支付服務提供者符合資安事件處理要求。

3. **強化消費者保護**：相關規定包括涉及第三國及外幣之交易，只要有任一支付服務提供者是在歐盟境內，均應適用；只要支付未經授權，應立即退款予付款方；保障無條件退款權（惟商品或服務已完成消費者不在此限）；無需另外授權的交易額度由原本的 150 歐元下修為 50 歐元；對於客訴爭議，支付服務提供者應於 15 個工作日內以書面回覆。

三、 歐元體系之監管方法

(一)蒐集相關資訊：

歐元體系蒐集資訊的來源廣泛，包括與系統營運者間雙向聯繫、對於系統活動及文件之定期或臨時性申報。歐元體系央行除了利用法律賦予之權限蒐集資訊外，亦會利用道德勸說方法使系統營運者自願提供資訊。

(二)根據相關標準評估 FMI：

歐元體系會根據本身制定，或與其他央行及相關主管機關合作制定的標準及建議，評估 FMI。此外，歐元體系會定期監視、檢查 FMI，以及研究有關 FMI 的新發展。歐元體系對於各種支付系統及工具之監管優先順序，係根據其所衍生的風險大小及風險來源訂定。

(三)運用措施誘導改變：

當歐元體系發現支付、結算及清算基礎設施中的某一系統缺乏足夠的安全與效率時，將會根據上述評估得到的結果採取行動，以及誘導該系統營運者做出改變。歐元體系可採取的處置行動包括道德勸說、公開聲明、影響參加系統，及與其他主管機關合作。無論採取上述種監管方法，歐元體系認為最重要

的是與被監管機構維持良好的合作，此有助於確保有效監管並降低被監管者的負擔。

肆、香港零售支付系統監管之發展

一、 監管現況

零售支付系統處理大量但金額相對較小的交易，一般較不會引發系統性風險，因此，香港金融管理局(Hong Kong Monetary Authority, HKMA)認為零售支付系統不具足夠的系統重要性，係採非正式的監管原則，未指定此類系統應遵守「結算及清算系統條例(Clearing and Settlement Systems Ordinance, CSSO)」的規定。然而，HKMA 鼓勵零售支付產業以發布實務守則方式進行自我管理，俾促進系統的安全與效率。

上述實務守則包括 2005 年 8 月生效的「多用途儲值卡營運實務守則(the Code of Practice for Multi-purpose Stored Value Card Operation)」，及 2007 年 1 月生效的「支付卡機制營運機構實務守則(the Code of Practice for Payment Card Scheme Operators)」，前者係制定有關作業可靠性、資料安全性，及香港境內多用途儲值卡(multipurpose stored-value card, MPC)發行者、系統營運者、收單行之效率與透明度等方面的原則，後者則是制定有關作業可靠性、資料與網路安全性，以及香港境內信用卡與借記卡營運者之作業效率與透明度等方面的原則。

此外，「銀行業條例(Banking Ordinance)」授權 HKMA 管理香港境內 MPC 之發行，以確保 MPC 機制及其發行者之健全運作。依據「銀行業條例」，持牌銀行被視為有助於 MPC 之發行，免經核准即可發行 MPC；但其他計畫發行 MPC 的機構則須先申請許可成為「吸收存款公司(deposit-taking company, DTC)」。

二、 未來新的監管制度

全球零售支付市場快速成長，科技創新及民眾對新科技接受度逐漸提高，催生新形式的支付工具與服務，例如儲值支付卡片、線上儲值支付工具及網路或行動支付服務。鑒於目前「銀行業條例」

對於儲值卡的監理體制僅適用於裝置式多用途儲值產品，而「結算及清算系統條例」係賦予 HKMA 指定及監管大額結算及清算系統的權力，該二法規未涵蓋非實體形式的儲值支付產品及重要的零售支付系統，前述非實體形式的儲值支付產品通常非銀行業者所發行，資金主要儲存在網路式帳戶、行動帳戶或電腦伺服器上。

為確保零售支付系統的安全與健全，HKMA 已提出「2015 年結算及清算系統條例修正草案」，將非實體形式的儲值支付產品及重要的零售支付系統納入該條例之規範。以下介紹香港儲值支付產品(stored value facilities, SVF)及零售支付系統新的監理制度：

(一)儲值支付產品之監管制度

為確保儲值支付產品發行者具備適當能力管理消費者儲值的資金，以保障消費者權益，HKMA 將建立儲值支付產品執照核發制度，規定如未取得 HKMA 核發之執照，任何人不得在香港發行或協助發行多用途儲值支付產品。

1. 適用範圍：包含以裝置為基礎及非以裝置為基礎的多用途儲值支付產品。單一用途、使用範圍有限及累計儲值金額低於 100 萬元港幣之儲值支付產品尚不列為監管對象。

2. 核發執照條件：

(1)**在香港境內有實體據點**：依香港法律登記之公司法人且在香港境內設有辦公處所。此項規定將使 HKMA 可有效監管執照申請人，即使其系統及作業設置在香港境外，或是透過網際網路提供服務。

(2)**主要營業項目**：執照申請人的主要營業項目必須是儲值支付產品之發行，以確保申請人的主要資源只用在儲值支付產品業務上。

(3)**財務健全**：執照申請人必須符合最低資本要求，亦即實收資本額不得低於 2,500 萬元港幣。

(4)**儲值金額之管理**：執照申請人必須具備可適當保護消費

者儲值金額的防護機制，且儲值金額與自有資金須加以區隔。此外，執照申請人亦須具備適當的儲值金額風險管理政策及程序，以確保有足夠資金因應消費者贖回儲值金額。

(5) **股東及經理人之適格性及審慎的風險管理規定**：執照申請人的財務長、董事及經理人必須具適格性，負責管理儲值支付產品業務的人員具備適當的專業知識及經驗。執照申請人須具備合適的風險管理政策及程序，並與其支付產品之規模、風險及複雜度相稱。

(二)零售支付系統之監管制度

現行的「結算及清算系統條例」僅規範大額的結算與清算系統，惟鑑於被廣泛使用的零售支付系統能否安全且有效率地運作，攸關香港日常的經濟活動，該項條例之修正草案爰擴大將零售支付系統納入規範。在香港境內營運或處理港幣或外幣零售支付交易的零售支付系統若符合指定條件，即須接受 HKMA 之監管。

1. 指定條件：根據「2015 年結算與清算系統條例修正草案」，若零售支付系統本身失序會造成以下任何一種情況時，HKMA 將有權指定該零售支付系統接受監管：

   (1) 對於貨幣或金融穩定、香港作為國際金融中心之功能產生負面的影響。

   (2) 損害社會大眾對於支付系統或金融體系之信心。

   (3) 對香港日常商業活動產生實質、負面的影響。

2. 其他考量因素：

   (1) 透過該零售支付系統辦理轉帳、結算或清算之交易總額。

   (2) 透過該零售支付系統辦理轉帳、結算或清算之交易平均金額。

   (3) 透過該零售支付系統辦理轉帳、結算或清算之交易筆數。

(4) 該零售支付系統參加者數量。

(5) 直接或間接連結大額支付系統。

3. 審慎監管規定

(1) 營業規章須有適當的違約機制。

(2) 符合安全性規定：包括與系統運作相關的風險管理及控制程序；系統所持資料的安全及完整性；系統的穩健性，包括財務健全。

(3) 符合效率規定：包括參加成本及參加條件之合理性。

(三)HKMA 的監理權力

「2015 年結算及清算系統條例修正草案」賦予 HKMA 下述監理之權力：

1. 監管：包括現場審查、非現場審查、蒐集資料、行政指導、實施作業規約、訂定法令、發布指引等。

2. 調查：當 HKMA 有合理原因相信儲值支付產品發行者或零售支付系統營運者違反規定時，依法有權進行調查。

3. 制裁：HKMA 有權視違規行為之特性及嚴重性，施以不同程度之行政裁罰（例如警誡、警告、譴責、命令提出改善措施、撤銷及暫時吊銷執照）或罰款（1,000 萬元港幣，或因違規而獲取之利潤或避免之損失的 3 倍，以金額較大者為準）。

伍、 金融市場基礎設施之網路防護

一、 國際現況

金融體系遭受網路攻擊[5]的次數愈來愈頻繁，受影響的層面也愈廣，網路攻擊本身的複雜度也提高。鑑於 FMI 在促進金融體系穩定性上扮演關鍵的角色，CPMI 已試圖了解 FMI 目前所面對的網路風險，及 FMI 能否有效處理最糟的狀況。

CPMI 已成立工作小組分析在 PFMI 架構下，FMI 及其監管者所面對各種網路安全議題之相關性。該小組成員以與各會員國 FMI 及其參加者、相關利害關係人訪談之方式，進行普查，更加理解各會員國 FMI 在網路防護領域的能力與觀點。從上述訪談中，工作小組發現 4 種現象：

(一)網路防護逐漸成為 FMI 的首要課題。

(二)FMI 正在處理系統遭受網路威脅對於金融穩定造成的風險。

(三)FMI 試圖達成在極端網路事件後在 2 小時內復原的目標，此或許需要花費數年的時間達成。

(四)FMI 應提供法規方面之支援，促進各方之溝通與協調，以尋求有效的解決方案。

此外，雖然 FMI 的高階管理人員多已考慮將網路防護列為首要工作，惟在金融部門日漸遭受網路威脅之情況下，業者需更加努力使產業能達成設施更快復原的目標。

二、 2 小時復原時間目標

由於 FMI 攸關國內及國際之金融穩定，PFMI 明確要求 FMI 應有營運不中斷計畫，以處理會導致重大作業失序風險的事件，包括可能造成大規模或重大失序的事件；然而，上述事件不侷限於硬體設施遭受之威脅破壞，亦包含網路攻擊事件。根據 PFMI 準則 17

[5] 網路攻擊係指試圖滲透某個環境或事件對其網路安全性造成負面影響之行為。

之主要考量 6，FMI 的營運不中斷計畫應包含備援中心的使用，且其設計應能確保重要資訊系統能在失序事件發生後 2 小時內回復運作，此即所謂的 2 小時復原時間目標(two hours recovery time objective, 2h-RTO)。FMI 即使在極端的市場情況下，仍應能於失序事件當日營業結束前完成清算。雖然 FMI 發現在極端的網路情況下要達到 2h-RTO ，極具挑戰性，但 FMI 高階管理人員仍支持此一目標。

三、 網路攻擊的來源

大多數的民眾所熟悉金融機構所提供的網頁式(web-based)服務，只是大型金融機構所使用的一小部分技術。因此，金融機構多將心力放在阻止侵入者將其網頁作為進入該機構內部網路、系統及取得資料之入口，以免影響其營運。以 FMI 為例，通常會將內部系統與網頁式應用服務區隔開來，使潛在的侵入者較難將其列為目標。然而，FMI 仍須努力減緩網路行動者(cyber actor)愈趨複雜及多變之戰術帶來的衝擊。網路行動者是一種多樣化的群體，視其動機及能力代表不同等級的威脅（如表 8）。雖然網路攻擊的衝擊大不相同，但試圖中斷金融機構業務運作或破壞 FMI 重要功能的網路攻擊，即可能會造成系統性風險。

金融機構及 FMI 的業務運作也可能遭遇頻繁的低度網路攻擊，這類攻擊通常是由信念駭客所發動的，藉由製造網路塞車或轉址等方法使金融機構或 FMI 的網路癱瘓或線上服務中斷，雖不致連累內部系統，但可能造成商譽風險(reputational risk)。

表 8 網路行動者之種類及攻擊力

種類	定義
組織型犯罪 (organized crime)	主要是受到利益激勵的駭客團體，其具備較先進的技術，試圖攻擊低度防禦的目標。
信念駭客 (hacktivist)	與組織型犯罪的能力相當，差別在於其攻擊係受到本身意識型態信仰所激發。
對手 (adversaries)	具備進行長期攻擊所需財務資源及專業技術的駭客團體，其動機涵蓋經濟、財務及政治等。
內鬼 (insiders)	違反公司信任的內部員工利用其進入系統之權限，發動網路攻擊。
第三者 (third parties)	試圖取得機密資訊或在黑市向其他網路行動者兜售系統弱點資訊之競爭者或第三者。
個人駭客 (skilled individual hackers)	試圖挖掘目標缺陷以獲取個人名聲或報酬之個人。

資料來源：Harold Gallagher, Wade McMahon and Ron Morrow2014 年 12 月「網路安全性：保障加拿大金融系統之防護(Cyber Security: Protecting the Resilience of Canada's Financial System)」

四、 網路防護整合式方法

網路防護整合式方法是要確保即使是服務品質下降，FMI 能持續運作。為了對付網路攻擊的手法並恢復服務，FMI 通常會採用整合式方法，此方法係根據內部所研擬的網路防護框架(framework)所制定，或會隨更一般化的(generic)框架進行調整，例如美國商務部(Department of Commerce)國家標準技術研究院(National Institute of Standards and Technology, NIST)於 2014 年 2 月發布的網路防護框架、世界經濟論壇於 2014 年 1 月所發布的網路防護方法、MITRE 公司[6]於 2013 年發布的網路防護框架。基本上，網路防護整合式方法包含以下三個面向：

(一)範圍(Scope)：FMI 的網路防護框架係處理網路攻擊可能造成表

[6] MITRE 公司係一間美國的非營利公司，主要任務是針對美國政府在國防情報、航太科技、民政系統、國土安全、司法、健保及網路安全等領域所遭遇的挑戰，提供創新且實際的解決方案。

9 所列 3 種情境。

表 9 網路攻擊影響分析

情境一	情境二	情境三
機密性缺口	可用性缺口	完整性缺口
1. 機密資料被網路攻擊竊取 2. 提供服務之能力未必受損 3. 網路攻擊或許只是後續更複雜攻擊的開端 4. 不易及時認出並減輕衝擊 5. 損害 FMI 的聲譽	1. 無法取得服務 2. 影響 FMI 與參加者間的通信、影響 FMI 對其參加者的支援、影響 FMI 更新服務內容、影響 FMI 與交易對手的資訊交換 3. 使參加者及金融市場無法運作時間延長	1. FMI 的核心資料及系統因網路攻擊而毀損 2. FMI 資訊或系統之完整性不再被信賴 3. 備援系統可能也毀損 4. 系統初期似乎正常運作 5. 為使系統恢復至可信賴狀態，應決定是否停止服務 6. 可能需要相當多的時間偵測及分析問題 7. 完全恢復服務的時間可能很久 8. 參加者在 FMI 的部位可能被鎖住且不再被信賴而導致系統性風險 9. 所有權及金融部位的爭議可能導致對金融市場失去信心 10. 可能對其他的 FMI、參加者與其客戶及市場造成連鎖反應，包括流動性及信用效應。

資料來源：整理自 BIS(2014),“Cyber resilience in financial market infrastructures ,” p.6

(二)網路治理(Cyber governance)：網路治理框架不僅包含 FMI 的 IT 基礎設施，也涵蓋人員、技術、程序及溝通等層面。

1. 人員：FMI 所有的人員（包括作業人員、管理階層及董事會）均與網路防護的兩大要素（安全性及作業復原）有關，

均須對網路風險有高度的認知，內部稽核單位在確保網路風險倡議與政策上扮演重要的角色。有效的網路防護要求網路風險應在 FMI 風險管理框架內被周延處理。

2. 技術：強化系統之安全性，提升對於網路攻擊的防護能力，採取多層式的網路防護措施，例如控管使用權限。

3. 程序：從作業風險的觀點，董事會決策過程中應妥適評估網路防護之意涵。網路防護屬於作業風險的一環，有賴 FMI 不同層級人員（例如作業單位、內部稽核、資訊安全主管及董事會）對於網路防護及營運不中斷之投入與分析。

4. 溝通：由於 FMI 與參加者、其他的 FMI、服務提供者等相互連結，故建立彼此間能有效溝通的管道十分重要。然而，FMI 的資訊安全團隊與其交易對手須能維持充分的信賴，方有利於彼此分享敏感資訊。當 FMI 遭受網路攻擊時，相關利害關係人間（包括主管機關）之及時溝通，有助於 FMI 恢復運作並防止網路攻擊擴散。

(三)防護措施：FMI 應運用各種控管措施，有效防範網路攻擊之發生、偵測進行中的或已完成的網路攻擊、能在網路攻擊後恢復原訂的服務水平。

1. 防範網路攻擊之措施

(1). 辨識：FMI 正在改善其對業務背景、支援關鍵功能的資源及相關網路風險的了解，因此首重在使風險管理策略與業務需求一致。

(2). 認知：提升組織內各階級人員對網路之認知的方法包括員工訓練及網路威脅分析。

(3). 深度防禦：亦即將系統與系統元件層級化並建立防火牆的過程，因此若其中一個元件受到波及，不會讓另一個元件再受攻擊。面對網際網路之應用程式（例如電子郵

件軟體）被視為最大的風險，因此應優先將其與核心系統元件隔離。

(4). 阻止惡意活動：使用防毒軟體，以及分析網頁服務與基礎設施（包括監視與檢查可疑的網路電子郵件及病毒碼入侵），找出攻擊者可能會用來輸入病毒碼的弱點，或許可以阻止網路上的惡意活動。

(5). 減少被攻擊的機會：亦即減少攻擊者可以進入 FMI 網路的點，作法包括限制網際網路閘道的數量、列出可使用之軟體清單、將重要的網路隔離。

(6). 測試及應用程式管理：安全性稽核及滲透測試配合使用先進的分析與模擬攻擊，以確保符合安全標準，並找出現行安全機制的弱點。FMI 應定期進行滲透測試，包括內部自行辦理及與外部顧問合作。應用程式管理則包括列出可使用的應用程式清單，降低攻擊者在作業環境植入病毒碼的風險及定期更新應用程式與作業系統，以修補系統的弱點。

(7). 存取控制：存取控制措施可防止未經授權人員進入系統取得資料，而特殊權限使用者僅限於那些真正需要擁有資料的人員。當有人試圖特許存取資料時，高階主管應收到警示。存取控制措施之目標放在控制組織內部人士攻擊的風險及外部攻擊者進入系統的機會。偵測措施會使用存取紀錄及警報等工具來監視特許進入行為，以及辨識異常活動。

(8). 基礎設施之控制及開發：IT 基礎設施之設計對於資訊安全管理有重大的意涵。IT 基礎設施可採取預防性的及主動的措施嚴加控管。虛擬機器(virtual machines, VMs)及虛擬桌面影像(virtual desktop image, VDI)等技術使員工可以遠端存取主機，並使用安全性程式控管使用者權

限，將主機與資料集中管理。

虛擬機器可用來創造網站、伺服器及工作站的非持續性，將系統重新設定至所謂的黃金狀態(golden state)，以有效移除網路攻擊者安裝的惡意軟體，使其不易持續存在於 FMI 的網路上，且因環境不斷改變使攻擊者不易透過網路進行偵查或傳播，此一程序也有助於復原。

密碼防禦措施（例如敏感資料之加密）之佈署亦被視為良好的防禦實務，因為其可保護敏感資料在不安全環境下傳遞時，不會被未經授權者修改或存取。

2. 偵測

FMI 能否快速偵測及評估網路攻擊範圍攸關其縮短復原空窗期。大多數的 FMI 實施多項控管措施，例如多方蒐集並分析資料相關性，俾能及時偵測異常的活動。此外，大多數的 FMI 也會維護及測試其偵測程序與步驟，以驗證防護措施的有效性。

(1). 監視：監視措施須能使利害關係人偵測到客戶間的異常交易（例如金額、交易對手或時間異常），彼此間之合作有助於防範網路攻擊擴散。此外，技術人員須了解 FMI 系統處理一般及關鍵業務的情況。

(2). 檢查點(checkpoint)：FMI 密集使用檢查點及確認技術，可能會對參加者造成作業負擔，但可減少診斷及分辨異常情況所需的時間，在系統內安裝此類相互強化之設計可改善其防護及偵測效果，亦有助於加快 FMI 復原速度。

3. 復原

系統可持續運作的設計係指即使系統提供服務的水準下降，例如僅限處理優先交易，仍應確保系統具有持續運作

的能力，網路防護係欲吸收網路攻擊造成的衝擊，使系統不致完全停擺。因此，所謂的復原係指系統能在一定時間內恢復至相當水準或是完全復原狀態。

FMI 應建立即時擷取交易及其他重要資料的作業程序，並將該等資料儲存在異地的系統。透過兩地資料之頻繁核對，將有助於偵測到被破壞或變造的交易，及使系統資料回復正確。此外，為避免重要資料遺失，FMI 應建立異地備援系統，並定期測試，確保可載入已被備份的資料。

陸、心得與建議

一、 心得

(一)國際組織正就金融市場基礎設施之監管，研議應公開揭露之量化資訊，以利跨國比較

根據 PFMI 準則，各國金融市場基礎設施除應遵循現行的資訊揭露架構外，應另外公布重要的量化資訊，如相關法規確定性及信用風險曝險程度等，俾使包括社會大眾在內的利害關係人能對該基礎設施進行評估，並作跨國間之比較。有鑒於此，CPMI 及 IOSCO 已先就 CCP 制定應公開揭露之量化資訊及其揭露之頻率，嗣後可能再擴及其他金融市場基礎設施。

(二)香港金管局修法將非實體支付工具及新興零售支付系統納入監管，以強化前述系統之監管法源依據

現行香港支付系統之監管權責，係歸屬 HKMA，該局依據「結算及清算系統條例」，負責監管大額結算及清算系統，另根據「銀行業條例」，負責監管實體形式的多用途儲值支付產品；惟對於非實體形式之儲值支付工具與新興零售支付系統，則缺乏完善的監管制度，主要因該類系統之營運者多為非銀行業者。為確保該等工具與系統運作順暢及安全，香港金管局近期修訂「2015 年結算及清算系統條例修正草案」，將該局的監管範圍擴及於非實體支付工具與新興零售支付系統（不涉單一用途的儲值支付工具），並賦予監管權限如核發上述工具與系統營運者執照、收集資料、發布指引、訂定規約、進行調查及裁罰等，以強化該局對於零售支付系統之監管法源依據。

(三)金融市場基礎設施應持續投入資源強化網路防護，以確保系統遭受外力中斷後能於 2 小時內恢復運作

由於 FMI 負責辦理各類金融商品交易之結算及清算，加上

FMI 彼此往往相互連結，因此，其能否順暢運作攸關整體金融體系之安全與效率。在網路攻擊之威脅逐漸升高的環境下，FMI 現有的網路防護機制將勢將面臨新的挑戰，似宜持續投入人力及相關資源於網路防護機制之強化，俾使 FMI 能降低網路攻擊造成之衝擊，達到 PFMI 準則所訂標準，亦即 FMI 之重要資訊系統能在失序事件發生後 2 小時內回復運作。

二、 建議事項

(一)蒐集各國 PFMI 遵循進度及相關評估報告，以作為國內進行系統自我評估之參考

為呼應 G20 及金融穩定理事會(FSB)的期望，CPMI 及 IOSCO 自 2013 年 8 月起公布各會員國各類金融市場基礎設施第一階段[7]遵循情形之報告，並依各國進度持續更新報告內容；2015 年 2 月再公布歐盟、美國及日本等國家或地區之集中交易對手與交易資料保管機構在第二階段[8]遵循情形之報告，澳洲、香港及新加坡則預計於 2015 年年中開始進行第二階段之評估。

2015 年初本行已完成 PFMI 之中文譯本，目前正針對同資系統及與其相連結之結算系統，辦理 PFMI 自我評估作業之前端預備工作。為利該等作業進行順利，且與國際標準趨於一致，似可蒐集上述 CPMI 及 IOSCO 公布之報告資料，以掌握國際間對於 PFMI 之遵循情形，並參考各國自我評估作業之細項標準，作為本行辦理 PFMI 評估作業之參考。

(二)採分離原則執行支付及清算系統之營運及監管功能

支付清算系統營運者與監管者兩種角色不同，加上系統監管涉及資訊、風險管理、財務會計等多種專業，部分國家央行

[7]第一階段：會員國司法管轄區內金融市場基礎設施及相關主管機關是否已完成必要的修法或立法程序，以反映 PFMI 準則與職責之新規定。

[8]第二階段：已採行的改革措施是否獲得落實，並與 PFMI 準則與職責之規定相符。

乃將 RTGS 系統之營運與支付清算系統之監管兩種功能分離，例如由不同部門負責(例如香港)，或將 RTGS 系統委外營運(例如馬來西亞)，主要目的在使央行專責監管，避免因身兼多重身分造成角色混淆，並減輕人力負擔。

反觀我國，上述兩項工作均由本局支付清算科負責，未來似可研議將營運者與監管者兩種功能於本局內分由不同業務科別負責執行。

(三)加強主管機關間對電子支付工具之監管合作

本次課程有關網路安全防護的議題，強調隨著網路科技快速發展，網路支付業務型態亦將隨之改變，因此，主管機關應適時修訂相關法規（如香港「2015 年結算及清算系統條例修正草案」)，或於法令尚未完備時，採取其他因應措施，並於必要時，與其他主管機關共同合作，加強對相關機構之監管，以避免因網路安全之漏洞，導致消費者權益受損，甚至進而影響金融穩定。

我國對於零售支付工具之監管原僅規範於「電子票證管理條例」，惟該條例係規範實體型式之儲值支付工具，並未涵蓋電子支付工具之發行機構，例如支付連、歐付寶等所謂的第三方支付服務公司。為因應新型態的網路經濟消費蓬勃發展，促進電子支付工具發行機構之健全經營及發展，以提供民眾安全便利之資金移轉服務，立法院於 2015 年 1 月三讀通過「電子支付機構管理條例」，並於同年 5 月 3 日開始實施，開放電子支付機構可辦理「網路帳戶儲值（含台外幣）」、「線下交易（即實體交易）」和無實質交易的「匯款」三大業務。自此，我國對於零售支付工具之監管體制堪稱完備。

該條例雖已明訂金管會為主管機關，負責電子支付機構之申請、許可、監督及管理等業務，其中有關業務許可及部分管

理規則之訂定，須洽商本行意見。惟因電子支付機構的資本規模及監理強度不如銀行，為確保電子支付工具之安全與效率，金管會宜強化與本行或其他相關主管機關(涉及洗錢防制業務為法務部、涉及電子商務業務為經濟部)間之監管合作，例如建立監理資訊分享機制及協調溝通管道。此外，亦可運用其他非法定的監管工具，例如道德勸說或直接參與電子支付產業相關議題會議，促使業者落實作業風險之管理。本行基於確保支付系統運作安全及效率之權責，亦宜密切關注該等機構業務之發展，俾協助主管機關維持電子支付業務之健全發展。

參考文獻

1. 本次訓練課程主辦單位提供與會學員講義資料(2015)。
2. 黃昱程(2014) ,「金融市場基礎設施準則(PFMI)執行實務」,公務人員出國報告。
3. 張國興(2014),「遵循金融市場基礎設施準則以增進金融穩定與有效監管：評鑑方法及交易資訊揭露」,公務人員出國報告。
4. 陳娟娟、蔡依琳(2013) ,「2013 年度 SEACEN 研究計畫評估系統性金融市場基礎設施之分析架構」,公務人員出國報告。
5. 龔玲雅(2013) ,「金融市場基礎設施準則暨中央銀行監管職責之探討」,公務人員出國報告。
6. BIS(2014), “Cyber resilience in financial market infrastructures.”
7. CPSS-IOSCO (2012), “Principles for financial market infrastructures: Disclosure framework and Assessment methodology.”
8. ECB(2014), “Revised oversight framework for retail payment systems.”
9. ECB(2014), “Eurosystem oversight report 2014.”
10. ECB(2014), “Oversight expectations for links between retailed payment systems.”
11. IMF(2013), Country Report No.13/58. “Malaysia: Publication of Financial Sector Assessment Program Documentation-Detailed Assessment of Observance of the CPSS-IOSCO Principles for Financial Market Infrastructures.”