出國報告（出國類別：實習）

參加 SEACEN 支付系統營運課程

服務機關：中央銀行
姓名職稱：吳黃蘋　業務局四等專員
　　屠敬傑　資訊處四等專員
派赴國家：馬來西亞
出國期間：2019 年 4 月 21 日至 4 月 27 日
報告日期：2019 年 7 月 24 日

目　　次

壹、前言

本次奉派參加由 SEACEN(The South East Asian Central Banks)研訓中心於馬來西亞吉隆坡所舉辦之「支付系統營運課程」，講師來自印尼及馬來西亞等央行資深官員，以及 SEACEN 研訓中心、SWIFT 及 VISA 等機構資深人員，共有 14 國派員參加，包含我國、孟加拉、汶萊、柬埔寨、香港、印尼、寮國、馬來西亞、蒙古、尼泊爾、巴布亞紐幾內亞、菲律賓、斯里蘭卡及泰國等國，總計 38 名學員。

授課內容包括：(1)大額與零售系統之運作與發展、(2)支付清算系統之風險管理、(3)金融市場基礎設施準則及(4)持續運作管理等。來自馬來西亞央行及印尼央行的資深官員於課程中介紹馬來西亞支付系統潛在的風險來源、各式風險管理工具，以及支付系統之監管方式及央行扮演之角色，另針對近期興起的零售支付之詐欺風險，闡述應對策略。

本次與會各國央行之大額支付系統，多已採行即時總額清算機制(Real-Time Gross Settlement, RTGS) (除柬埔寨及尼泊爾)並有改造計畫，例如，本次與會的印尼央行與馬來西亞央行計劃大額支付系統改採 ISO 20022 訊息標準，而斯里蘭卡央行則計劃採混合清算機制並降低交易手續費。我國應持續關注主要國家央行對大額支付清算系統之改革成效，以作為強化同資系統之參考。另外，隨著支付系統對資訊科技的依賴提升及資訊科技的發展日新月異，支付系統面臨各種由科技發展所帶來的議題，也使業務持續運作及資訊安全相關議題愈形複雜。監管機關應持續關注並改善相關管理措施，確保金融市場基礎設施在任意形式的攻擊下具有足夠的韌性，以維持金融體系穩定。

本報告內容主要分為五章，除第壹章前言外，第貳章說明支付清算系統風險管理；第參章概述業務持續運作管理；第肆章說明資訊安全相關管

理原則與措施；第伍章為心得與建議。

貳、支付清算系統風險管理

一、支付系統攸關一國金融穩定

ECB 前理事 Gertrude Tumpel-Gugerell 指出，維持金融穩定與貨幣穩定(monetary stability)成為央行職責的部份原因在於央行於支付系統所扮演的角色。央行作為銀行的銀行，必須維持安全而有效率的支付及清算系統，以處理伴隨經濟交易活動而產生的各項收支及債權債務的清算業務。

(一)主要國家大額支付清算系統處理的年交易值達 GDP 之數十倍

維護金融穩定係各國央行之共同目標，亦是我國中央銀行法定經營目標之一。根據我國「中央銀行法」，中央銀行政策目標有四項：促進金融穩定、健全銀行業務及維持對內及對外幣值的穩定，以及在上述目標範圍內，協助經濟發展[1]。

金融穩定與貨幣穩定實係相輔相成之兩股力量，穩定的物價有助於金融穩定，而只有在金融穩定下，貨幣政策工具之操作才能發揮預期效果。自 1990 年代以來，國際間陸續發生多起重大金融危機事件，不僅造成國際金融市場動盪不安，更使總體經濟付出相當代價。為避免金融不穩定對國家經濟造成重大損害，近年來國際金融組織及各國央行均積極發展維護金融穩定之架構，期透過系統性之分析及監控，適時採行適當政策或措施，以達到金融穩定之目標。

以支付系統來說，一個安全且有效率的支付系統有助於金融穩定，若支付系統管理不佳，總體金融環境將滋生多種風險，例如信用風險及流動

[1]「中央銀行法」第 2 條規定，中央銀行經營之目標為促進金融穩定、健全銀行業務、維護對內及對外幣值之穩定，以及於上列目標範圍內，協助經濟之發展。

性風險等。以大額支付系統(large-value payment system)為例，主要國家大額支付系統處理的一年交易值占 GDP 高達 20~58 倍，如表 1。

表 1 大額支付系統－交易量及交易值			
大額支付系統	**年交易值**	**年交易值/GDP**	**年交易量(筆)**
美國 CHIPS	417.9 兆美元	20.4	114.8 百萬
美國 Fedwire	716 兆美元	34.9	158 百萬
英國 CHAPS	83.5 兆英鎊	39.6	48.5 百萬
日本 BOJ-NET	32,318 兆日圓	58.8	15.2 百萬
歐元區 TARGET2	432 兆歐元	28.6	89 百萬

註：除歐元區 TARGET2 為 2017 年資料，其他皆為 2018 年資料。

資料來源：BOE、Fed、TCH、BOJ、BOE 網站。

如果支付系統其中一位參與者到期違約無法履行債務，可能會造成骨牌效應引起系統風險，並快速散播至整體金融體系。正如美國聯準會前主席 Alan Greenspan 在其回憶錄上所說：「如果任何人想要摧毀美國經濟，可先破壞支付系統；銀行將被迫回到實體貨幣之資金移轉，企業交易則回到以物易物或借據。全國經濟活動將像落石般向下滾動。」

(二)支付系統之即時總額清算(RTGS)等機制有效降低系統風險，有助於金融穩定

為降低系統風險，1990 年代之後，廣受各國採用作為大額支付系統的清算機制是即時總額清算，RTGS 對系統接受的各筆支付指令，在參加清算

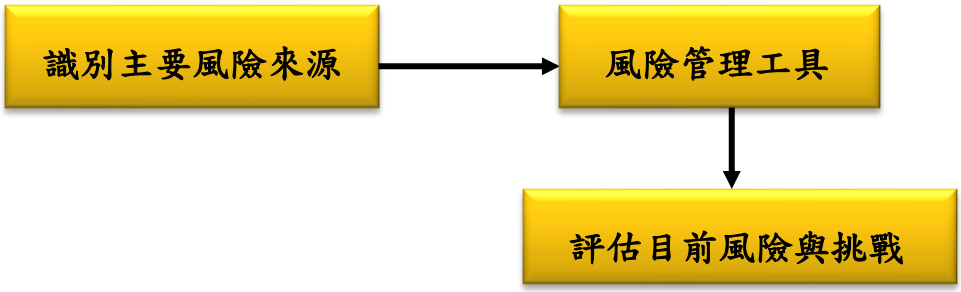
各方若帳戶有足夠餘額(或可用的融通額度)的情況下即執行總額清算，清算完成的交易立即生效，不可撤銷，具有最終清算效力。

RTGS 可有效降低參加清算各方在過程中可能面臨的清算風險，且央行通常會配合提供流動性(日間透支)，以促進支付系統的順暢運作，有效降低系統風險，有助於金融穩定。

二、支付系統風險管理工具

支付及清算系統運作既與央行維持金融穩定有關，央行等系統營運者應對支付及清算系統進行風險管理、定義、評估並衡量風險後，利用適當的風險管理工具控制風險，並適時檢視控制方法。

圖 1　風險管理流程



資料來源：SEACEN 課程講義。

(一)大額支付系統風險管理工具

大額支付及清算系統面臨之主要風險，為信用風險、流動性風險、系統性風險、作業風險及清算風險，支付及清算系統營運者可利用各式風險管理工具(表 2)，以因應來自系統營運者、參與者及其他相關機構與整體金融體系的風險，說明如次：

表 2　大額支付系統主要風險管理工具

風險	風險管理工具
信用風險	擔保品
	折價率
	淨應付金額上限
流動性風險	日間透支
	佇列等候機制
	資金互卡解決機制
	隔夜資金自動擔保機制
清算風險	PvP、DvP
	RTGS
	防止無法被清算的機制
作業風險	強化維運支付系統資訊基礎設施
	建置(並落實)備援機制與營運不中斷計畫

資料來源：SEACEN 上課講義。

1. 因應信用風險，風險管理工具如次：

(1) 擔保品：為降低央行信用風險，當參加單位使用日間透支時，須提供央行所規定的合格擔保品，例如中央政府公債、國庫券及央行定期存單等。

(2) 折價率(haircut)：央行得設定擔保品之折價率，即參加單位提供之擔保品市值須按某一比率折價，目的在於減輕擔保品因市場價格劇烈波動所受的影響，以確保央行的債權。

(3) 淨應付金額上限(net debit cap exposure)：央行得設定個別參加單位營業日之未清算支付指令的淨應付金額上限，如高於該限額，便不得再發送支付指令，以控管央行信用暴險。

2. 因應流動性風險，風險管理工具如次：

(1) 日間透支：為避免因金融機構流動性不足，產生資金互卡現象，影響支付系統運作，參加單位得以央行認可之擔保品設質給央行後，於營業時間在央行核可額度內，由央行墊付日間透支之金額，參加單位則需於日間透支償還截止時點前將當日透支金額還清。

(2) 佇列等候機制(Queuing Mechanism)：將各項因帳戶餘額不足扣付之交易區分為不同優先等級，俟資金到位後依序執行完同一優先等級之所有指令後，再處理次一優先等級之指令。此機制有助於參加單位將其資金依重要性配置，降低流動性不足時可能引起的風險。

(3) 資金互卡解決機制(gridlock resolution)：若參加單位無法完成交易，出現資金互卡的情況，則由系統計算出可行的解決方案(例如多邊淨額互抵等方法)，盡量降低對其他參加單位影響之機制。

(4) 隔夜自動資金擔保機制：為避免參加單位於夜間清算時流動性不足，參加單位得以央行認可之擔保品設質給央行後，由央行墊付透支金額，參加單位則需於隔日將透支金額還清。

3. 因應清算風險，風險管理工具如次：

(1) 款券同步交割(Delivery versus Payment, DvP) 、**款對款同步收付機制**(Payment versus Payment, PvP)：DvP 為符合國際標準之清算機制，可確保交付券項(或款項)的一方確實收到款項(或券項)，有效防範違約交割風險；PvP 係指兩種幣別間之款對款同步收付，為國際間控管外匯交割風險之機制。以美元及新臺幣換匯交易為例， PvP 機制可確保支付美元(或新臺幣)的一方會收到新臺幣(或美元)，不會發生違約交割風險。

(2) 即時總額清算(RTGS)：RTGS 對系統接受的各筆支付指令進行逐筆總額清算，參加清算各方若帳戶有足夠餘額，則每筆支付指令於進入系統後即執行清算，清算完成的交易立即生效，具有最終清算效力，有效降低參加清算各方在過程中可能面臨的清算風險。

(3) 防止無法被清算的機制(failure to settlement arrangement)：為降低清算風險，系統營運商其他可採用的機制包括損失分擔機制[2](loss sharing)等。

4. 因應作業風險，風險管理工具如次：

(1) 強化維運支付系統資訊基礎設施：定期維護及更新系統軟硬體，強化資訊系統基礎設施，以維護支付系統安全。

(2) 建置(並落實)備援機制與營運不中斷計畫(Business Continuity Planning, BCP)：支付系統營運者為避免天災人禍影響系統運作，必須事先模擬情境，擬定營運不中斷計畫，確保在遭遇衝擊時，仍能夠提供正常服務，計畫應包括建立支付系統備援機制，迅速接續重要支付清算業務運作，例如可採用自動即時備援機制(automated real-time backup systems)，將主中心系統程式及交易資料同步保存在同地與異地備援系統，或是採用不同於現行系統之技術(non-similar facility, NSF)，預先複製重要金融基礎設施核心業務功能，俾重要系統遭遇網路攻擊而無法運作時，尚能透過 NSF 維持重要業務之運作。

(二)零售支付系統風險管理工具

---

[2] 損失分擔機制係指系統參加單位簽署損失分擔合約，相關違約交割損失將由違約擔保基金負擔，以完成清算。

就零售支付而言，美國零售業聯合會(National Retail Federation)表示[3]，支付卡[4](payment card)詐欺仍然為大型零售商最關心的問題，因此該會倡導更安全的支付卡，有效的零售交易風險管理工具包括：

1. **晶片支付卡**：支付卡中的晶片相較傳統磁條而言，較難被犯罪集團偽造，因此晶片支付卡安全性更高，可有效降低支付卡之詐欺交易。

2. **PIN 碼**：晶片支付卡雖然很難偽造，但亦非常難證明持有卡片的人為合法持有人，因此如持卡人進行交易時輸入 PIN 碼，以取代簽名的步驟，能減少支付卡盜刷問題。

3. **3D 驗證機制**：若要阻止信用卡的網路詐欺交易，可採取的方式為 3D 驗證機制，該機制係由 VISA、MasterCard 及 JCB 合作建立，讓持卡人能在更安全的網路環境下交易。持卡人透過需要在網路交易時輸入一次性的手機短訊 3D 驗證密碼或是預先設定的驗證碼後才能完成交易，讓網路交易增加多一重保障。

(三)我國同資系統風險管理工具

我國支付及清算系統係以中央銀行同業資金調撥清算作業系統(簡稱同資系統)為總樞紐，舉凡銀行間大額資金移轉、同業拆款交割、外匯買賣新台幣交割及債、票券交易之款項交割，均透過該系統處理，並連結國內證券、票券、債券及零售支付等結算系統，辦理銀行間資金最終清算作業，構成一個完整之支付及清算體系。同資系統係我國重要的金融基礎設施，本行採取若干風險管理工具來控管同資系統風險，說明如次：

---

[3] NRF (2018), “Fraud Still Retailers' Top Payment Issue Despite EMV,” Nov.

[4] 支付卡包括信用卡及轉帳卡等。

1. 信用風險工具－擔保品等

為保護本行債權，本行要求參加單位辦理日間透支應提供擔保品。依「中央銀行辦理日間透支作業規範」之規定，參加單位向本行申請日間透支，應提供合格擔保品，以十足擔保設質為之；前述合格擔保品包括本行可轉讓定期存單、本行定期存單、登錄中央政府公債、登錄國庫券及其他經本行同意之無實體證券等[5]。

2. 流動性風險工具－日間透支及佇列等候機制等

(1) 日間透支：為利即時總額清算機制運作順暢，降低流動性風險，當參加單位資金短缺，致交易無法順利進行時，本行得依其提供設質擔保品總額，核給日間透支額度，而日間透支利息費用係依擔保品的種類，按本行當時公告擔保放款融通利率之 1~1.5 倍計算[6]。

(2) 佇列等候機制：同資系統採取佇列等候機制，如前節所述。

3. 清算風險工具－DvP、PvP 及 RTGS 等

(1) DvP 、PvP：2004 年 4 月同資系統將票券的交割款納入清算，採款券同步交割機制，且於 2008 年 4 月將中央登錄公債的交割款項納入同資系統清算，亦採款券同步交割機制，以降低清算風險。另外，2014 年 2 月同資系統與外幣結算平台連結，以辦理美元與新臺幣換匯交易款對款同步收付機制。

(2) RTGS：同資系統於 2002 年 9 月全面採行即時總額清算機制，控管大額清算風險，當參加單位的帳戶餘額足夠時，系統才會清算其所發送的支付指令。

---

[5] 詳見「中央銀行辦理日間透支作業規範」第 7 點。

[6] 詳見「中央銀行辦理日間透支作業規範」第 18 點。

4. 作業風險：延時管理、建置備援機制及營運不中斷計畫等

(1) 建立延時管理機制：為有效督促參加單位善盡參加系統職責，本行已於 2012 年 10 月建立明確的延時事件管理制度，訂定「中央銀行同業資金調撥清算作業系統連線機構申請延時作業程序」，明文規範參加單位均應遵循同資系統清算作業時程，並以「延時時間」作為事件管理因子，分「輕度(20 分鐘以內)」、「中度(20 分鐘~日終 18 時)」、「嚴重(逾日終 18 時)」共 3 等級管理，督促參加單位應加強管理其同業資金調撥作業，如發生延時情形，應切實檢討改善事件原因，以維護同資系統順暢運作。

(2) 建置備援機制：為確保大規模失序狀況發生時，同資系統仍能維持營運不中斷，本行已建置備援中心，隨時接替主中心作業，並定期辦理演練作業，以驗證備援中心之作業可靠性。

(3) 營運不中斷計畫：因任一參加單位若無法順利連線執行同資系統作業，均可能對其他參加者造成影響，爰同資系統營運不中斷計畫規劃將參加單位因應異常狀況之業務持續運作能力納入，本行已於 2019 年 3 月函知參加單位，每年至少辦理 1 次媒體備援作業演練。

三、馬來西亞支付清算系統概況及近年風險管理改善措施

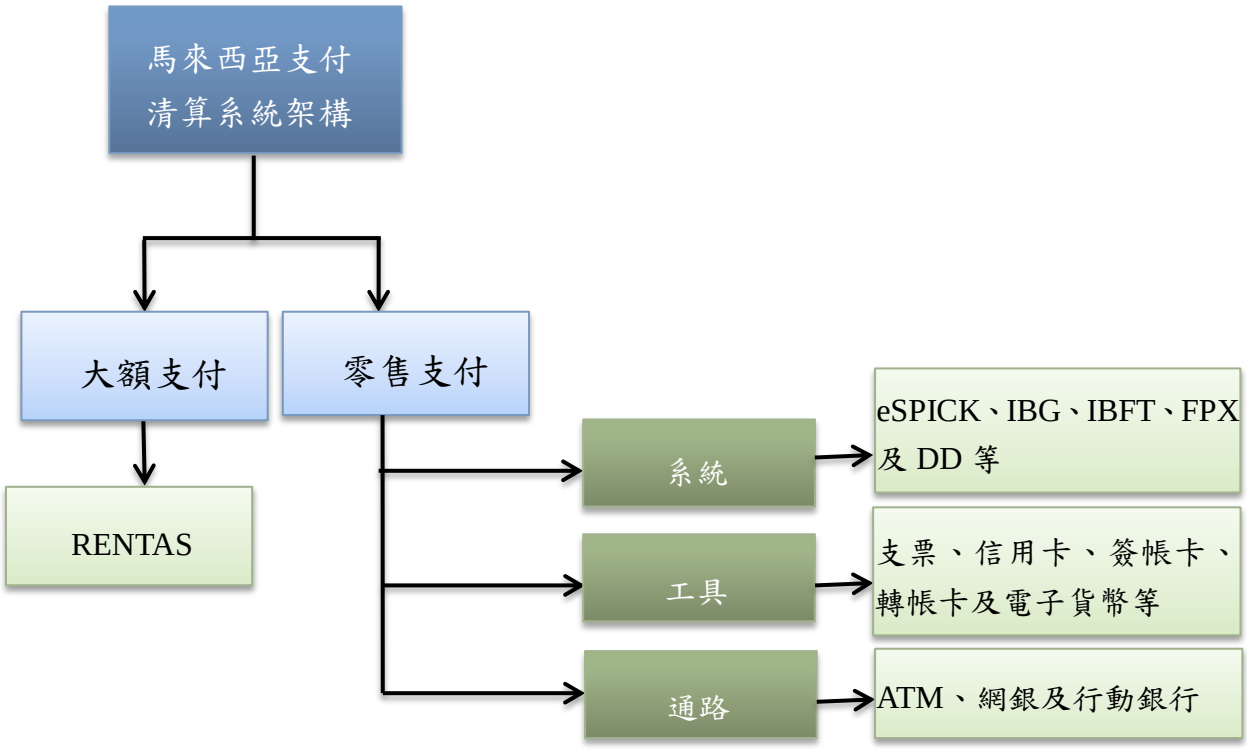
馬來西亞央行(Bank Negara Malaysia, BNM)為馬國銀行業及保險業之主管機關[7]，負責監理馬來西亞之支付清算體系，降低支付系統整體風險，並確保主要支付系統之運作順暢。BNM 將該國之支付清算體系分為大額支付及零售支付，零售支付架構並可再細分為系統、工具及通路三個層面，整體架構如圖 3。

[7] 馬來西亞證券業主管機關為馬來西亞證券委員會。

馬來西亞支付清算體系基礎設施主要由民間公司PayNet負責營運，PayNet係由BNM與馬來西亞11家金融機構組成，BNM為最大股東。PayNet負責營運的大額支付系統RENTAS為馬來西亞支付清算體系的樞紐，藉由與金融機構及結算機構連結，提供全國性的支付清算服務。

與 RENTAS 連結的主要零售支付系統，包含全國支票資訊結算系統(national electronic cheque information clearing system, **eSPICK**)、跨行資金調撥 GIRO 系統 (interbank GIRO, **IBG**)、即時資金調撥系統(interbank funds transfer, **IBFT**)、 網上支付結算系統(financial progress exchange, **FPX**)及直接扣款系統(direct debit, **DD**)等。RENTAS並連結香港的美金CHATS系統及Euroclear證券保管系統，提供多幣別、跨境的支付清算服務。

圖 3　馬來西亞支付清算系統架構圖



資料來源：BNM。

(一)馬國大額支付系統概況

RENTAS系統簡介說明如下：

1. 系統營運及清算程序

RENTAS 系統於 1999 年 7 月開始上線，營運時間為營業日上午 8 時至下午 9 時，處理銀行間資金撥轉、貨幣市場操作、外匯交易清算及第三方交易等。RENTAS 採 RTGS 清算機制，以先進先出原則處理支付指令，若參加機構帳戶餘額不足，將使先進之交易進入佇列，並逕予執行次筆交易。系統營運截止時間所有尚在排序等候之支付指令由系統逕予取消。

2. 參加單位

截至 2019 年 5 月，RENTAS 系統共有 69 家參加單位，包括 BNM、商業銀行、伊斯蘭銀行、投資銀行及資本市場與貨幣市場重要單位。RENTAS 採直接參加及間接參加制，直接參加單位與 RENTAS 連線進行支付交易，並於 BNM 開立馬幣清算帳戶進行清算。直接參加單位之間的資金移轉不設限，惟間接參加單位透過 RENTAS 直接參加單位承作之資金移轉(第三方交易[8])，每筆交易金額需達 1 萬馬幣。

3. 收費機制

參加單位須支付手續費，以支應系統建構、維護及營運成本，手續費分為固定費用及每筆交易手續費：

(1) 固定費用：每年 15,000 馬幣。

(2) 每筆交易費用：直接參加單位間為 2.5 馬幣，第三方交易為 1.5 馬幣。

---

[8] 第三方交易係指交易之收款人(beneficiary)非 RENTAS 之直接參加單位，而是間接參加單位(如政府或企業等)。

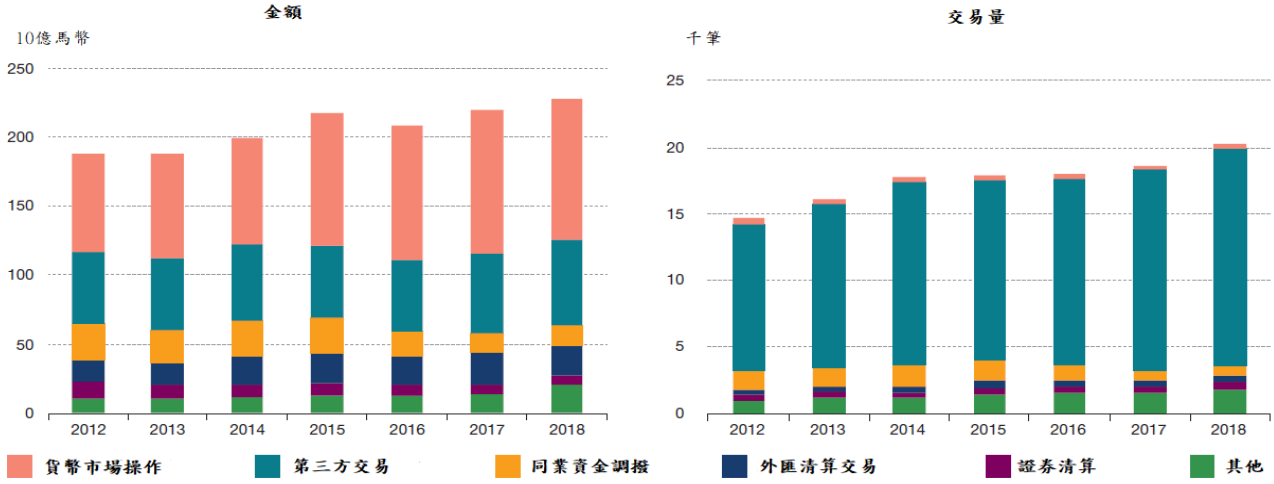
4. 日間透支機制

BNM 為降低流動性風險，解決參加單位資金互卡問題，當參加單位資金短缺，致交易無法順利進行時，BNM 於其提供擔保品限額內提供日間透支，日間透支雖免支付利息費用，惟仍須支付每筆 12 馬幣之手續費。

5. 營運量

2018 年大額支付系統 RENTAS 系統共處理支付業務 490 餘萬筆，金額 55.2 兆馬幣，成長率分別為 8.1%、2.7%，金額高達馬來西亞當年 GDP 的 39 倍；日均交易筆數為 20,240 筆，成長率為 8.5%，日均交易金額為 2,271 億馬幣，成長率為 3.1%，如圖 4。

圖 4　RENTAS 日均交易金額及交易量



資料來源：BNM。

RENTAS 系統中，交易筆數以第三方交易為主，占系統總處理筆數的 80.5%；交易金額則以貨幣市場操作及第三方交易為主，分別占系統總交易金額的 44.6%及 27.3%，如表 3。

表 3　2018 年馬來西亞 RENTAS 系統業務量

交易種類	業務量		業務量占比	
	筆數(萬)	金額(兆馬幣)	筆數	金額
貨幣市場操作	8	24.63	1.6%	44.6%
外匯交易清算	11	5.42	2.2%	9.8%
第三方交易	396	15.06	80.5%	27.3%
其他	61	8.40	12.4%	15.2%
證券清算	16	1.67	3.3%	3.1%
合計	**492**	**55.18**	**100%**	**100%**

資料來源：BNM。

(二)馬國零售支付系統概況

馬國主要零售支付系統，包含全國支票資訊結算系統(eSPICK)、跨行資金調撥 GIRO 系統 (IBG)、即時資金調撥系統(IBFT)、 網上支付結算系統(FPX)及直接扣款系統(DD)等(詳表 4)，說明如次：

表 4　馬來西亞零售支付系統

系統名稱 / 比較項目	eSPICK	IBG	IBFT	FPX	DD
交易類型	支票	小額收付款	小額收付款	網銀交易	定期繳款
清算方式(營業日次數)	DNS(1)	DNS(5)	RTGS	DNS(1)	DNS(5)
交易限額	—	每日 3 萬馬幣 (共同交易金額上限)		個人：每筆 1 馬幣~3 萬馬幣； 企業：每筆 2 馬幣~100 萬馬幣	—
2018 年交易量(筆)	101 萬	2.07 億	2.39 億	8,990 萬	400 萬
2018 年交易金額(馬幣)	1.43 兆	1.05 兆	2,800 億	548 億	384 億
參加單位	45	32	20	23	27
營運機構	PayNet	PayNet	PayNet	PayNet	PayNet

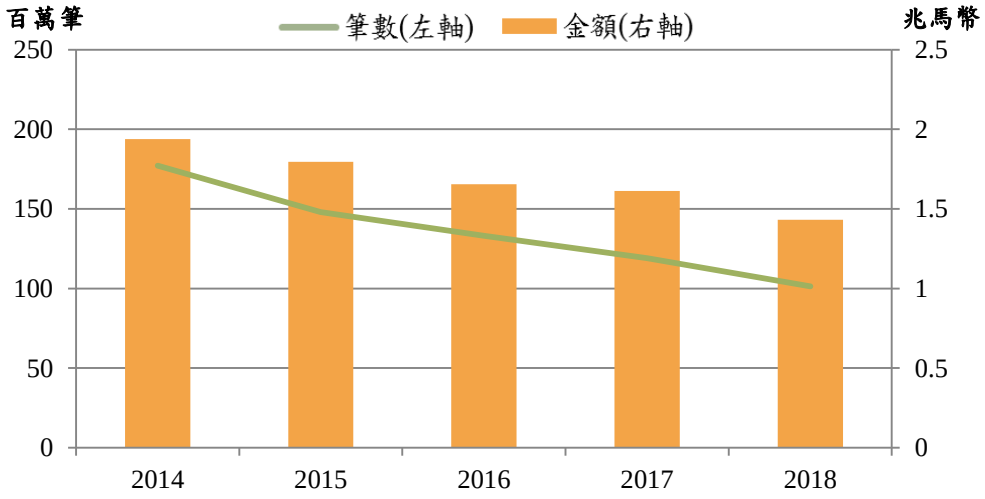
資料來源：BNM、PayNet 及作者整理。

1. 全國支票資訊結算系統(eSPICK)

eSPICK 於 2009 年 7 月正式上線，現由 PayNet 負責營運，共有 45 個參加單位，eSPICK 每日結算 1 次，並送至 RENTAS 清算。eSPICK 取代支票結算系統(SPICK)；舊系統 SPICK 之結算主要仰賴支票實體運送，新系統以支票截留影像取代。eSPICK 營運後，有效降低支票處理成本、提升支票的結清算效率，且支票入帳時間由 2~8 天縮短為提出交換隔日。

2018 年 eSPICK 系統營運量達 101 百萬筆交易，金額約 1.43 兆馬幣，筆數及金額分別較前一年減少 14.8%及 11.2%；日均營運量 42 萬筆，金額約 59.1 億馬幣。全國支票資訊結算系統業務量已缺乏成長動能，近幾年系統處理之交易筆數及金額雙雙衰退，如圖 5。

圖 5　eSPICK 營運量



資料來源：BNM。

2. 跨行資金調撥 GIRO 系統(IBG)

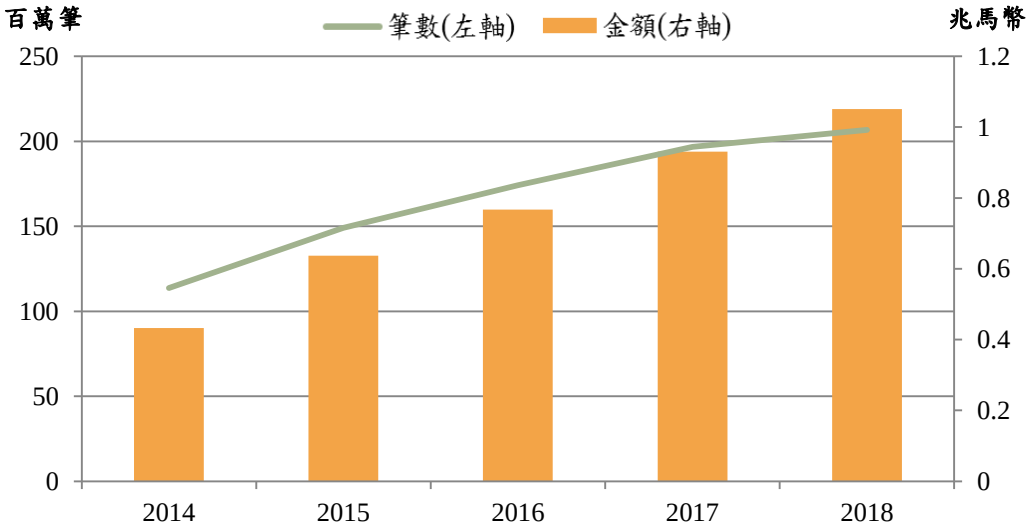
IBG 於 2000 年 10 月正式上線，現由 PayNet 負責營運，2018 年共有 32 個參加單位，IBG 每日結算 5 次，並交由 RENTAS 清算，IBG 採

行指定時點淨額清算(designated-time net settlement，DNS)機制。

客戶可透過臨櫃、網路/行動銀行及 ATM 的方式，透過 IBG 處理資金移轉，且多為相對小額、筆數較多且較不具時間急迫性之資金移轉，例如小額跨行匯款、貸款與信用卡收付款及工資支付等。營業日 17 時前之交易同日入帳，17 時後及非營業日之交易則於下個營業日入帳。

2018 年系統營運量達 2.07 億筆交易，金額約 1.05 兆馬幣，分別較前一年成長 5.1%及 12.9%，日均處理 85.53 萬筆，金額約 43 億馬幣，近 5 年其處理之交易筆數及金額快速成長，如圖 6。

圖 6　IBG 營運量



資料來源：BNM。

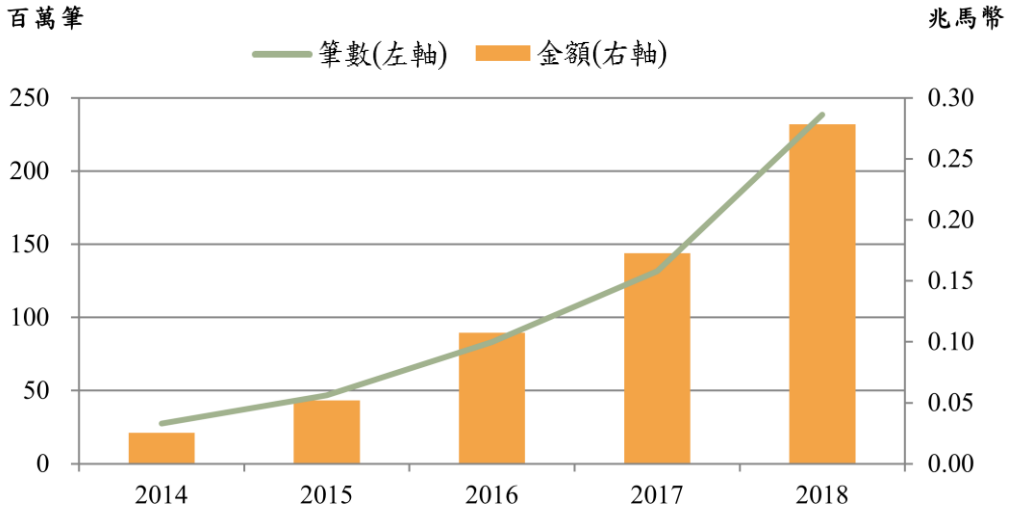
3. 即時資金調撥系統(IBFT)

IBFT 於 2006 年正式上線，現由 PayNet 負責營運，至 2018 年底共有 20 家參加單位。IBFT 營運業務大致與 IBG 相同，主要不同在於自

2014 年起採行 RTGS 機制，任何時點經由 IBFT 處理之交易，參加單位的受款人均可立即收到款項，惟手續費較 IBG 為高，以網銀/行動銀行或 ATM 方式承作每筆約 0.5 馬幣，並與 IBG 設有共同交易金額上限，每天交易金額上限為 3 萬馬幣。IBFT 係透過 RENTAS 進行清算。

2018 年系統營運量達 2.39 億筆，金額約 0.28 兆馬幣，分別較前一年增長 80.8%及 61.1%，日均處理 98.6 萬筆，金額約 11.6 億馬幣，因 IBFT 採行 RTGS 機制，近 5 年其處理之交易筆數及金額快速成長，如圖 7。

圖 7　IBFT 營運量



資料來源：BNM。

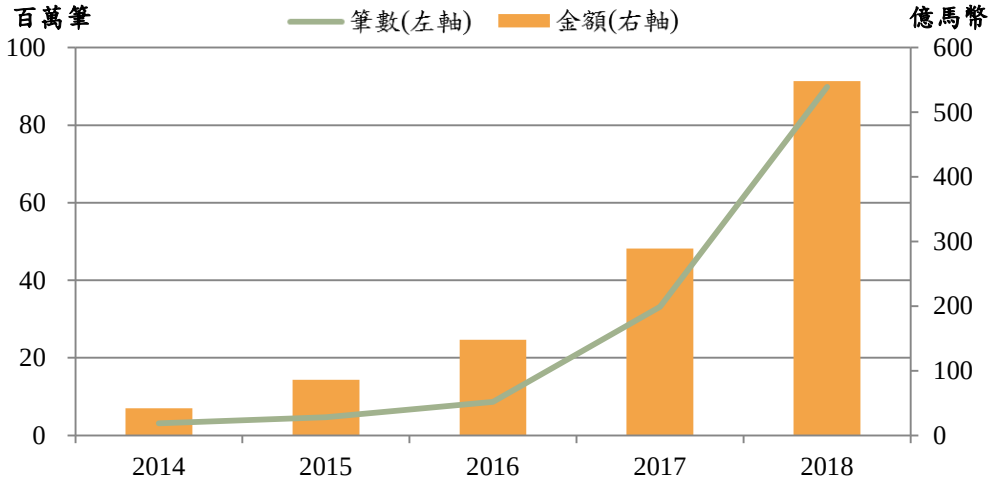
4. 網上支付結算系統(FPX)

FPX 於 2004 年正式上線，現由 PayNet 負責營運，至 2018 年底共有 23 家參加單位，包含 19 家銀行及 4 家非銀行業者，FPX 每日定時結算 1 次，並交由 RENTAS 清算。FPX 主要處理客戶使用網路銀行進

行各種電子商務 (e-commerce)[9]支付業務，包含網路刷卡購物、投資理財、貸款還款、交易退款、即時代收付等。FPX 之參加單位多提供近 24 小時服務，客戶於網銀進行交易後，透過 FPX 立即於其帳戶扣款，並於電子信箱收到交易訊息通知及線上發票。FPX 並有交易額度限制，個人戶每筆最低 1 馬幣，最高 3 萬馬幣；企業戶每筆最低 2 馬幣，最高 1 百萬馬幣。

2018 年系統營運量達 8,990 萬筆交易，金額約 548 億馬幣，分別較前一年成長 171%及 89.5%，日均處理 37.1 萬筆，金額約 2.3 億馬幣，網上支付結算系統受惠於馬來西亞電子商務發展及網路交易日益普及等因素帶動，近 5 年處理之交易筆數及金額大幅成長，如圖 8。

圖 8　FPX 營運量



資料來源：BNM。

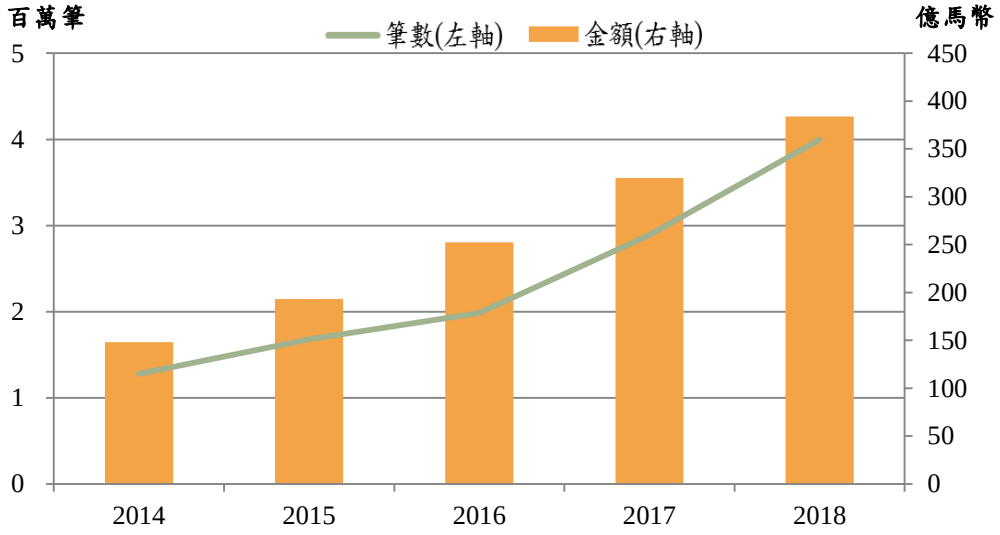
[9] 指企業與企業(B2B)或企業與顧客(B2C)間利用網際網路，進行資訊交換或交易傳送處理，完成產品/服務的使用權或所有權及款項的移轉。

5. 直接扣款系統(DD)

DD 係指處理客戶定期收付款之結清算系統，客戶進行授權後，系統即可直接於客戶指定之日期進行扣款。DD 現由 PayNet 負責營運，至 2018 年底共有 27 家參加單位，DD 每日定時結算 5 次，並交由 RENTAS 清算。

2018 年系統共處理業務 4 百萬筆，金額 384 億馬幣，分別較前一年成長 33.6%及 20.2%，日均處理 1.6 萬筆，金額約 1.6 億馬幣，近 5 年處理之交易筆數及金額逐漸成長，如圖 9。

圖 9　DD 營運量



資料來源：BNM。

(三)近年支付系統風險改善措施

1. 大額支付系統

(1) 信用及流動性風險之措施

- 2014 年 12 月實施隔夜資金自動擔保機制(Automatic Collateralized

Overnight Funding Facility, ACOFF)，即馬幣夜間清算透支機制[10]，當參加單位進行 IBG 及 DD 馬幣夜間清算而帳戶餘額不足時，由 BNM 依其設質之合格擔保品先提供流動性，參加單位至隔天再行還款之機制。

- 2016 年 9 月實施資金互卡解決機制(gridlock resolution mechanism)；RENTAS 每 20 分鐘偵測 1 次，若參加單位發生資金互卡的情形，RENTAS 將計算出可行的解決方案，將參加單位間可互抵的支付款項以淨額清算，以解決資金互卡的情形。

- 未來，馬來西亞研議採用流動性最適化清算機制(liquidity optimization settlement facility, LOSF)，參加單位可將交易分成緊急交易之 RTGS 交易及不緊急之 LOSF 交易，若設定為 LOSF 交易，僅須於 RENTAS 系統上輸入特定交易代碼(transaction reference number, TRN)。LOSF 交易不進行 RTGS 清算，而係於 RENTAS 滯留一段期間後再進行淨額互抵，以節省參加單位之流動性；此外，交易單位亦可在 LOSF 交易未完成清算前，將 LOSF 交易更改為非 LOSF 交易。

(2) 提升作業互通性之措施

- 2016 年 9 月採用 SWIFT 訊息標準，提升跨系統及跨境支付訊息互通性。

- 未來，擬採用 ISO 20022 訊息標準，提升不同基礎設施間的相容性，讓交易過程更順暢。

---

[10] ACOFF 馬幣夜間清算透支機制於營業日下午 6 時開始，截止時間為下午 9 時。

2. 零售支付系統

(1) 交易概況

BNM 將馬來西亞零售支付架構分為系統、工具及通路三個層面，零售支付系統已於上節介紹。零售支付工具除現金外，非現金支付工具主要包含支票、支付卡及電子貨幣(如預付卡(prepaid card))，支付卡包含信用卡、簽帳卡(charge card) 及轉帳卡(ATM 卡(debit card))。

表 5　2018 年非現金支付工具比較表

交易工具	交易金額(億馬幣)	年成長率	交易筆數(百萬)	年成長率	人均交易金額	人均交易筆數	流通卡數(千)
支票	14,319.06	-11.2%	101.4	-14.8%	45,284.8	**3.2**	-
信用卡	1,352.25	7.7%	447.1	10.0%	4,276.6	**14.1**	10,325
簽帳卡	124.73	13.6%	5.2	11.4%	394.5	**0.2**	128
轉帳卡	402.79	35.3%	245.7	51.5%	1,273.9	**7.8**	42,493
電子貨幣	109.69	20.6%	1,920.3	3.2%	346.9	**60.7**	60,986

資料來源：BNM。

馬來西亞 2018 年非現金支付工具中，交易金額雖仍以支票為主(占 85%以上)，惟民眾交易最常使用信用卡及電子貨幣，人均交易筆數分別為 14.1、60.7 筆，且轉帳卡之交易筆數與金額均呈快速成長，如表 5 。

2018 年底流通卡數 5,295 萬張，平均每人持有 1.67 張，其中轉

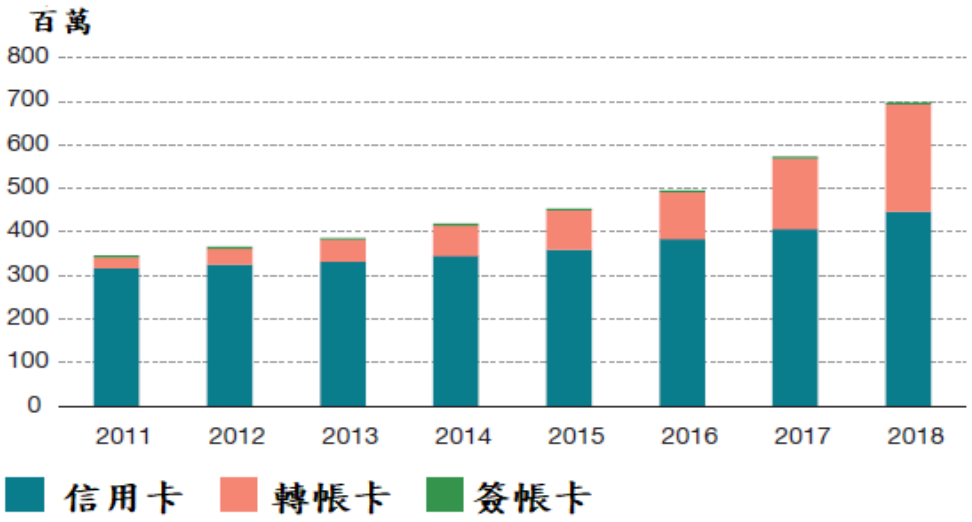
帳卡占比約 83.30%；支付卡總交易筆數約 6.98 億筆，交易金額 1,880 億馬幣，其中信用卡之交易筆數與金額約占 71.93%、64.05%，顯示該國發卡量最多為轉帳卡，但交易以信用卡為主。

(2) 風險管理改善措施

近年支付卡之交易不僅交易金額上升，交易筆數亦快速增加，如圖 10。由於支付卡交易愈形重要，馬來西亞強化支付卡交易之安全性，自 2005 年後針對零售支付交易採行之風險管理改善措施，包括：

- 2005 年支付卡完成晶片卡之轉換。
- 2012 年規定持卡人進行網路交易須輸入一次性交易密碼。
- 2017 年 7 月後持卡人進行實體信用卡交易須於 POS 機輸入 PIN 碼。

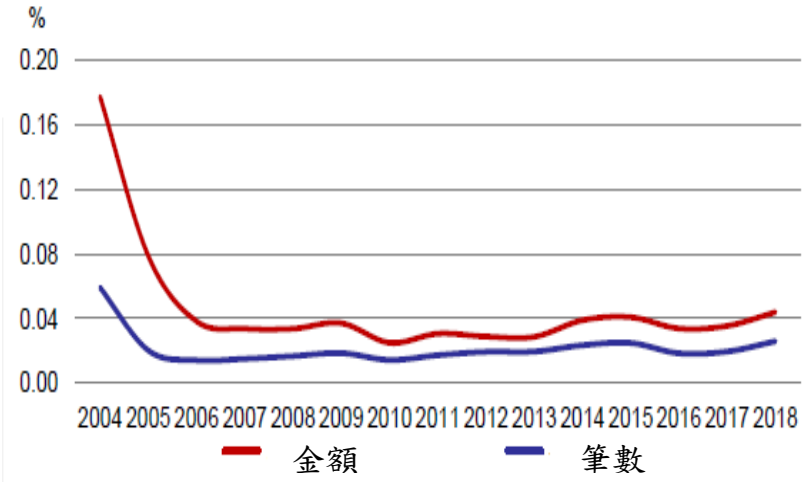
圖 10　2011-2018 年支付卡交易筆數



資料來源：BNM。

除上述措施外，BNM 亦要求金融機構加強交易授權碼(transaction authorization code)之安全性，如用戶註冊手機號碼接收交易授權碼，僅能至金融機構分行辦理，且用戶僅能透過 ATM 或電洽金融機構變更該號碼。透過這些措施的施行，馬來西亞支付卡詐欺交易金額與筆數之比重自 2005 年後大幅降低，近年則分別穩定維持在 0.04%、0.02%，2018 年支付卡詐欺金額與筆數占總交易金額與筆數的比率分別為 0.044%和 0.026%，如圖 11。

圖 11　馬來西亞詐欺交易金額與筆數比重
(占整體支付卡交易比率)



資料來源：SEACEN 課程講義。

參、業務持續運作管理概述

安全有效的支付清算系統有助於經濟成長及金融穩定，作為金融市場基礎設施的一環，若能制定良好的管理及營運標準，可有效減輕金融系統的風險。

國際清算銀行於2006年出版「高階業務持續運作原則」，以支持國際標準制定組織及各國金融當局提高金融系統對重大營運中斷的抵禦能力。其中提到業務持續運作管理(Business Continuity Management, BCM)通常包括：

- 營運衝擊分析(Business Impact Analysis, BIA)
- 災難復原計畫(Disaster Response Planning, DRP)
- 營運不中斷計畫

此外，國際清算銀行支付暨市場基礎設施委員會(Committee on Payments and Market Infrastructures, CPMI)與國際證券管理組織(International Organization of Securities Commissions, IOSCO)亦於2012年發布金融市場基礎設施準則(Principles for Financial Market Infrastructures, PFMI)，包含橫跨五個面向的24個原則，其中的第17項原則係有關作業風險的原則，摘述如下：

- 作業失靈可能會損害支付清算系統的聲譽或可靠性，導致法律後果及所有參與者的財務損失。在某些情況下，作業失靈也可能是系統性風險的來源。
- 業務持續運作管理是作業風險管理架構的關鍵組成部分。

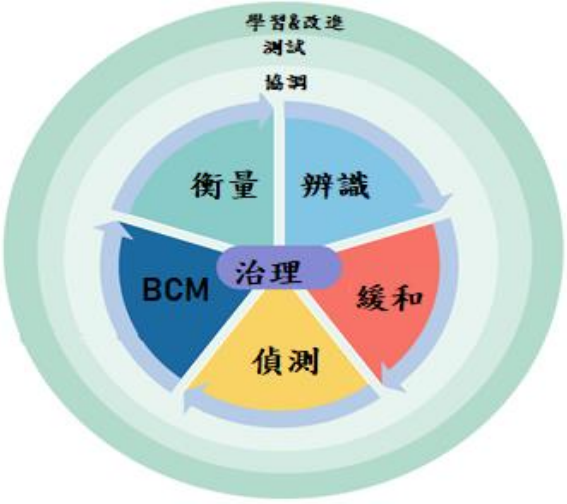
近年來，由於支付系統對資訊科技的依賴提升，業務持續運作管理亦應對網路攻擊提出對策。以下就針對業務持續運作管理之各項議題作概略介紹。

一、 業務持續運作管理

依據國際清算銀行之說明，業務持續運作管理指應包括整體營運策略、標準及程序，以確保營運中斷時及時維護或回復特定的作業。其目的是儘可能減少因中斷而產生的作業、財務、法律或聲譽損失及其他重大後果。

在金融市場基礎設施的作業風險管理架構中(如圖12)，業務持續運作管理處於其核心部分，旨在及時恢復營運及履行金融市場基礎設施的義務，包括在發生大規模或重大中斷的情況下。

圖12 金融市場基礎設施的作業風險管理架構

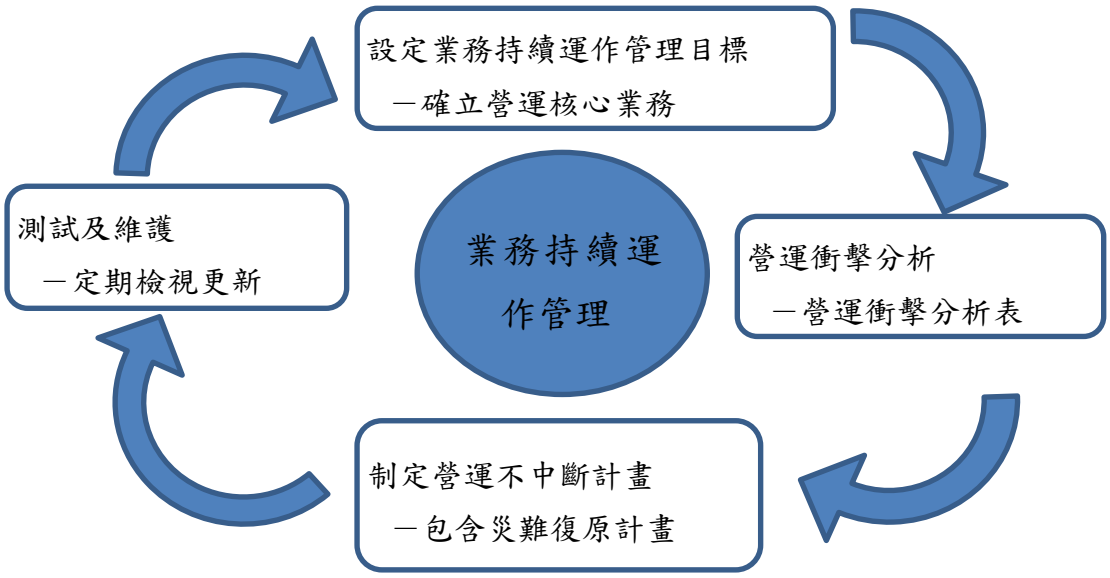


資料來源：SEACEN 課程講義。

業務持續運作管理需探討的範圍相當廣泛，包括組織、人員、資訊科技及環境等，以下列舉幾項原則性要點：

- 營運作業流程的持續、週期性管理(如圖13)

圖13　業務持續運作管理流程



- 風險管理
  - 分析安全缺失等風險來源
  - 使用控制措施降低風險
  - 制定預防及復原措施，減輕風險造成的影響
- 機密性、完整性及可用性之保證
  - 機密性：確保系統資料未洩漏與未經授權的對象
  - 完整性：確保系統資料未被未經授權的對象修改
  - 可用性：確保系統可於經授權對象需要時使用
- 法規遵循
  - 定期檢視法規是否修正，並確認營運不中斷計畫是否應隨之調整
  - 高階主管應重視法規遵循之重要性

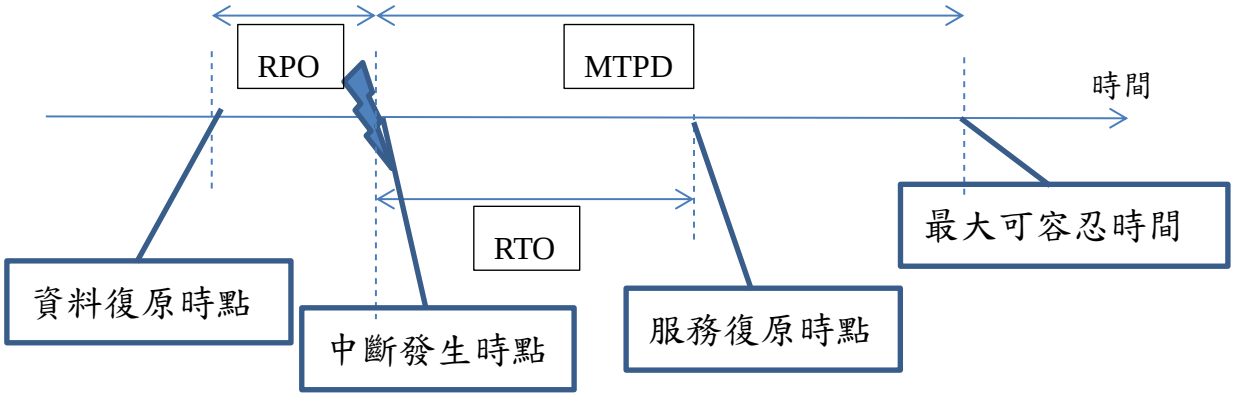
二、營運衝擊分析

營運衝擊分析為考慮組織營運的需求，衡量重要功能或設施遭受災害時，若無法在特定時間內回復正常營運，將遭受的損失。通常是徵詢業務單位有關其服務的重要程度及對資源的使用需求，來判別服務遭中斷的機率及中斷後造成之衝擊程度。

當災害發生造成金融市場基礎設施服務中斷時，組織遭受的損失及衝擊必定隨中斷時間延長而擴大，故管理者在進行營運衝擊分析時，除依照重要程度及對資源的需求來定義不同作業程序的復原次序，設定復原目標也是必要的步驟之一，常見的復原目標(如圖14)如下所述：

- 回復時點目標(recovery point objective, RPO)：系統資料復原的時間點，即中斷發生後，將系統回復至上一次備份資料的時間點。
- 回復時間目標(recovery time objective, RTO)：系統回復提供服務的時間點，即中斷發生後，不致因缺乏此服務而造成嚴重衝擊的時間。
- 最大可容忍中斷時間(maximum tolerable period of disruption, MTPD)：系統服務中斷被視為不可接受前的最長允許時間。

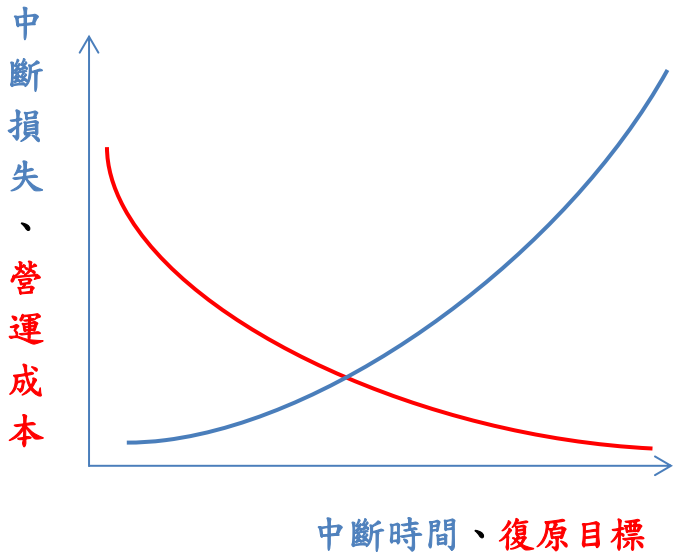
圖14　RPO、RTO與MTPD



資料來源：作者整理。

在制定復原目標時，固然回復時間越短，服務中斷事件對組織所造成的衝擊越小，然而同時也要考量復原策略所帶來的成本。例如，若要中斷事件不造成系統任何資料損失，也就是RPO為零，只要系統在營運的同時，將系統內所有資料即時同步至備援地點。然而這樣的策略，會需要即時同步軟硬體設置、額外的管理技術等，造成營運成本增加，要如何平衡成本及效益，也是營運衝擊分析的課題(如圖15)。

圖15　回復目標的成本與效益



資料來源：作者整理。

由於營運衝擊分析為服務中斷事件發生後，決策使用何種復原方案的重要基礎，需要整個組織，從業務單位、資訊單位乃至於管理階層的參與，才能將營運衝擊分析制定妥善，要點如下：

1. 確認營運流程各環節重要性、評估中斷所受之衝擊
2. 確認營運回復所需之資源
3. 制定營運衝擊分析表(如表6)
4. 定期或不定期反覆檢視

表6　營運衝擊分析表範例

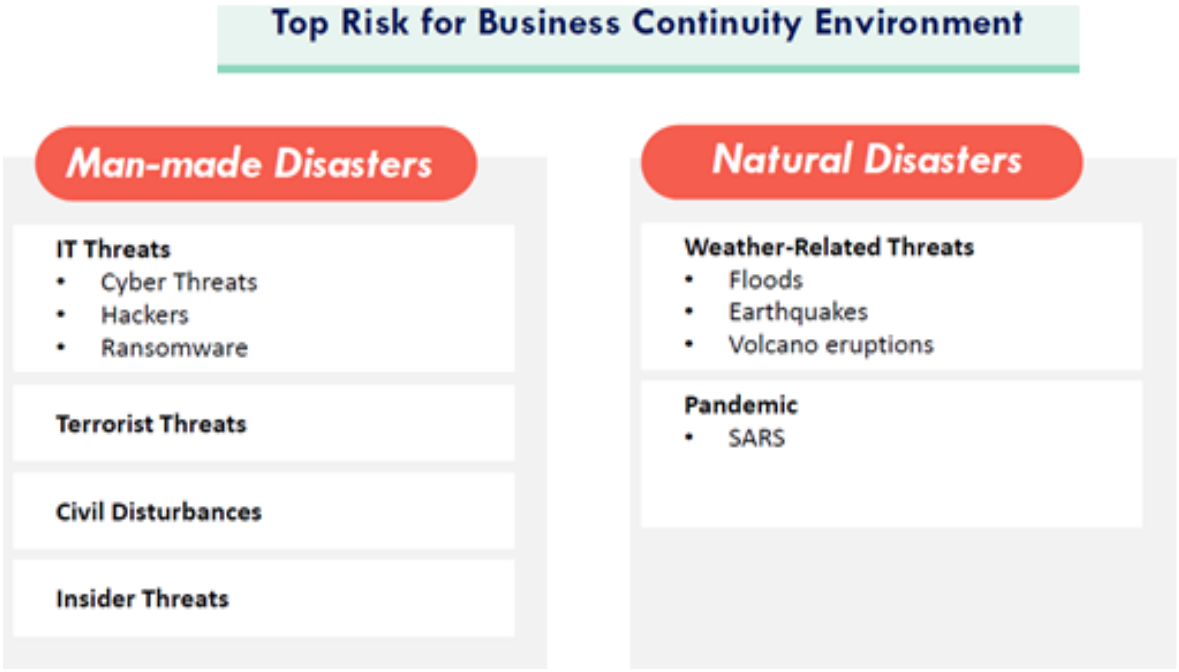
復原順序	作業項目編號	資訊系統	MTPD	RTO	RPO	發生中斷機率	不同中斷時間所造成之衝擊程度 L：輕微　M：中等 H：嚴重				
							0-1小時	1-4小時	4-7小時	1日	1日以上
1.	36		1 小時	1 小時	0 小時	L	M	H	H	H	H
2.	37		1 小時	1 小時	0 小時	L	M	H	H	H	H
3.	10		1 小時	1 小時	0 小時	L	M	H	H	H	H
4.	11		2 小時	1 小時	0 小時	L	L	M	H	H	H

資料來源：本行資訊處文件。

三、 災難復原計畫

金融市場基礎設施尚仰賴其他基礎設施，如電力、通訊及資訊設施等，當這些基礎設施受到天然災害、傳染病或人為因素造成服務中斷時(如圖16)，金融市場基礎設施也會因此無法提供服務。災難復原計畫即是為了因應此情況發生時，金融市場基礎設施服務如何恢復。

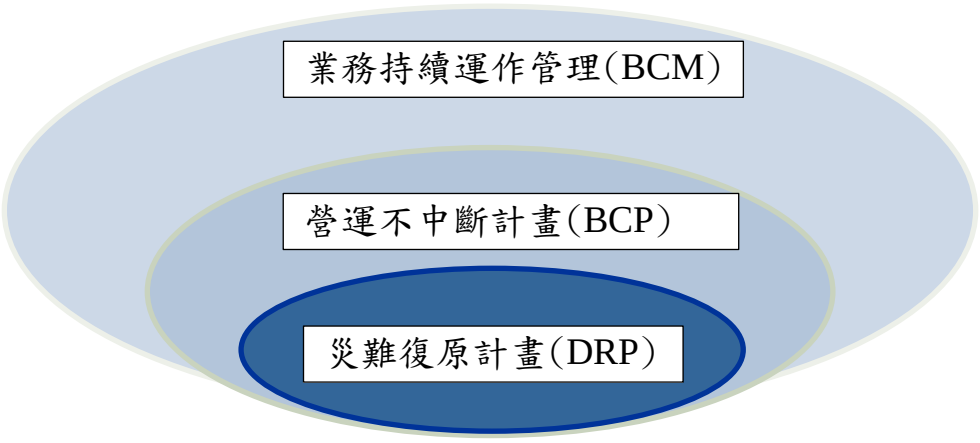
圖16 營運環境的主要災難種類



資料來源：SEACEN 上課講義。

與業務持續運作的全盤考量不同，災難復原著重於面臨災難時，在一段時間內基礎設施無法使用的情況下，採取必要的措施確保資源、員工和業務能繼續運行，將災難造成的資訊服務中斷影響減少到最小程度，進而回復資料的完整及系統的正常運作，故災難復原僅為業務持續運作之一環(如圖17)。

圖17 BCM、BCP 與 DRP 之關係



資料來源：作者整理。

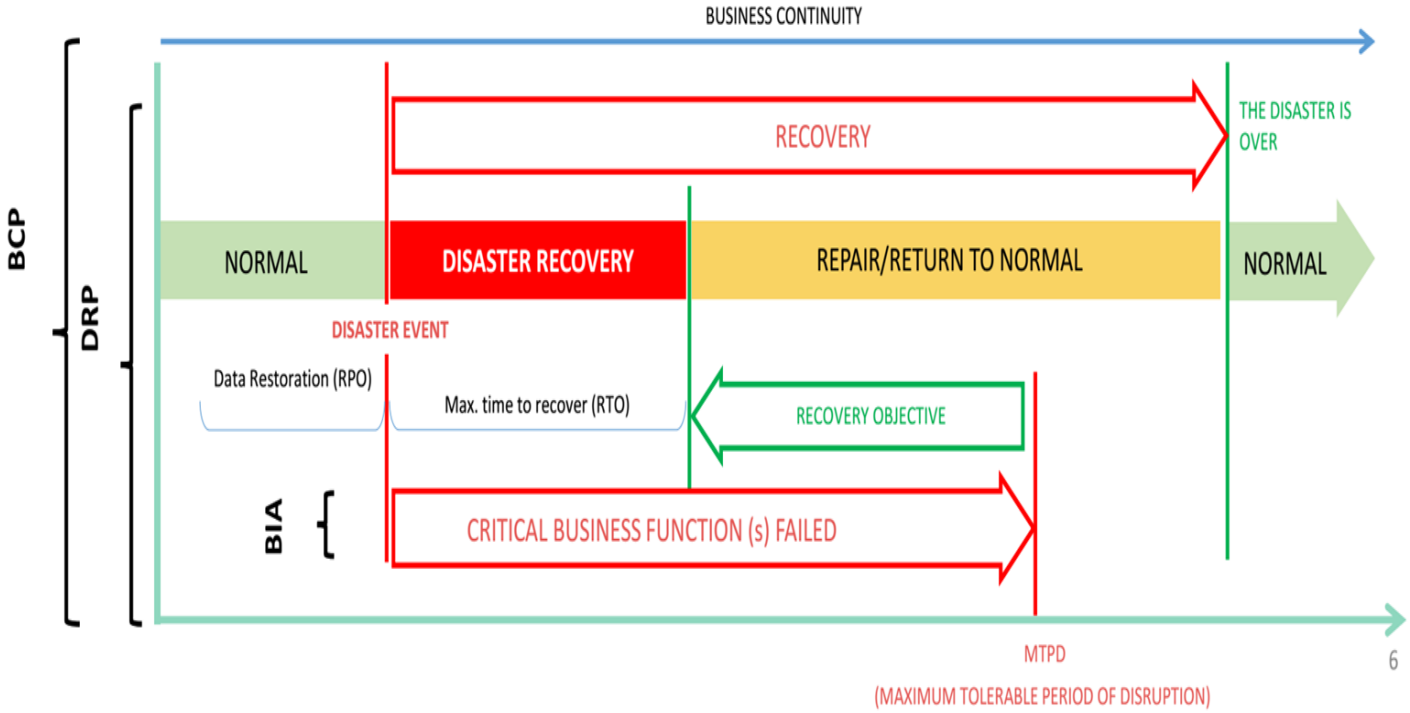
災難復原的重點在於，事先規劃資訊設備、營運環境或業務人員，全部或部分無法提供服務等多個復原方案，並在災難發生時選擇最適合、影響層面最小或最快速之解決方案，以下為災難復原之步驟：

1. 確認災難原因
2. 評估災難損失程度及影響範圍
3. 選擇災難復原方案(可同時選用多種方案)
   - 人力復原：使用代理人代替無法執行業務之人員。
   - 環境復原：使用發電機代替電力或使用備援線路代替原網路設定。
   - 資訊設備復原：硬體復原、作業系統復原、應用系統復原、資料庫復原。
   - 異地復原：由異地中心取代原中心提供服務。
4. 測試運作
5. 復原報告

四、營運不中斷計畫

營運不中斷計畫為進行業務持續運作管理的核心部分，係將組織所有營運服務納入考量，取得自管理階層以下的所有部門人員支持，並制定與實施風險管理、營運衝擊分析及災難復原計畫，其目的在於發生中斷事件後能夠儘快恢復服務，以達成業務持續運作之目標(如圖18)。

圖18　營運不中斷計畫



資料來源：SEACEN 課程講義。

以下為制定及實施營運不中斷計畫之原則：

- 管理方面
  - 陳述明確的目標，包括所有的回復目標、政策、程序，以及與利益相關單位的溝通渠道
  - 資源分配
  - 詳盡的文件
- 風險評估及分析
  - 識別造成重大風險的事件
  - 評估是否需要異地備援中心
- 備援

- 硬體、軟體、資料及網路環境等備援方式
- 異地備援中心需配置足夠之資源

● 復原方案

- 確保金融市場基礎設施能夠在當天結束時復原所提供的服務
- 應涵蓋不同的情境，從輕微到極端的情況，甚至切換至異地提供服務

● 反覆測試及檢視

- 測試應該含括所有的情境及復原方案
- 定期或不定期重新檢視計畫是否合宜

五、科技進展對業務持續運作之影響

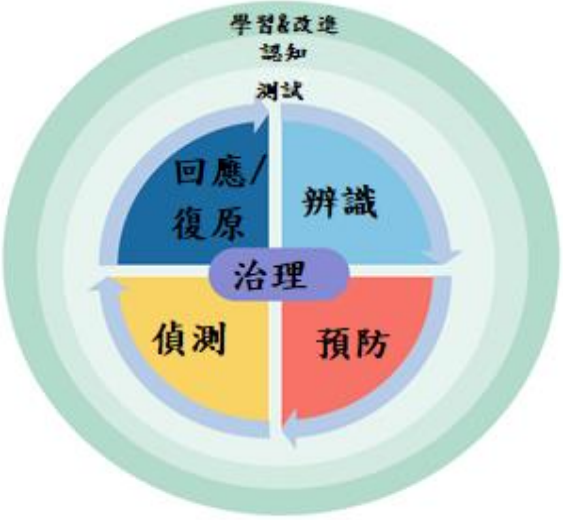
資訊科技的快速發展，使得支付行為更為方便快速，然而對於金融市場基礎設施來說，此類金融服務與資訊服務之高度互聯方式，也讓資訊安全成為一種日益增長的威脅。

由於資訊攻擊的方式非常複雜，並且具有多種攻擊類型，例如：阻斷攻擊(DoS)，或藉由偷取敏感資料以獲取經濟利益，這些攻擊都會造成系統的不穩定。因此，資訊攻擊將給金融市場基礎設施的作業風險管理帶來與以往不同的挑戰。

面對這樣快速變動的情勢，業務持續運作策略也勢必需要作出調整，包括即時偵測中斷、甚或是預防性預測，以及採取較為彈性或具韌性之技術；此外，當多數支付服務都透過網路互相連結時，相關機構不可能獨善其身，透過與其他組織通力合作，達到聯防資安風險。

考量資訊攻擊手法日新月異，CPMI 於2015年提出金融市場基礎設施網路攻擊復原作業指引，使金融市場基礎設施即使在部分功能遭受攻擊或危害時，仍然可以繼續提供服務，以提升對資訊攻擊之作業復原能力。

圖19 作業復原架構



資料來源：SEACEN 課程講義。

此作業復原架構包含8大議題(如圖19)，簡述如下：

- 資訊治理：有效的資訊治理及具有韌性的資訊策略與架構。
- 辨識：識別關鍵業務功能、流程及所有資訊資產的存取，並進行風險評估。
- 預防：實施適當、有效的主動式措施，以防止或限制潛在資訊事件的影響。
- 偵測：進行廣泛的監控，檢視是否有導致資訊事件的異常活動。
- 回應與復原:關鍵系統應能夠安全且快速的復原,以減輕系統性風險，並滿足使用者的期許。
- 測試：針對框架內所有元素及情境均應嚴格測試。

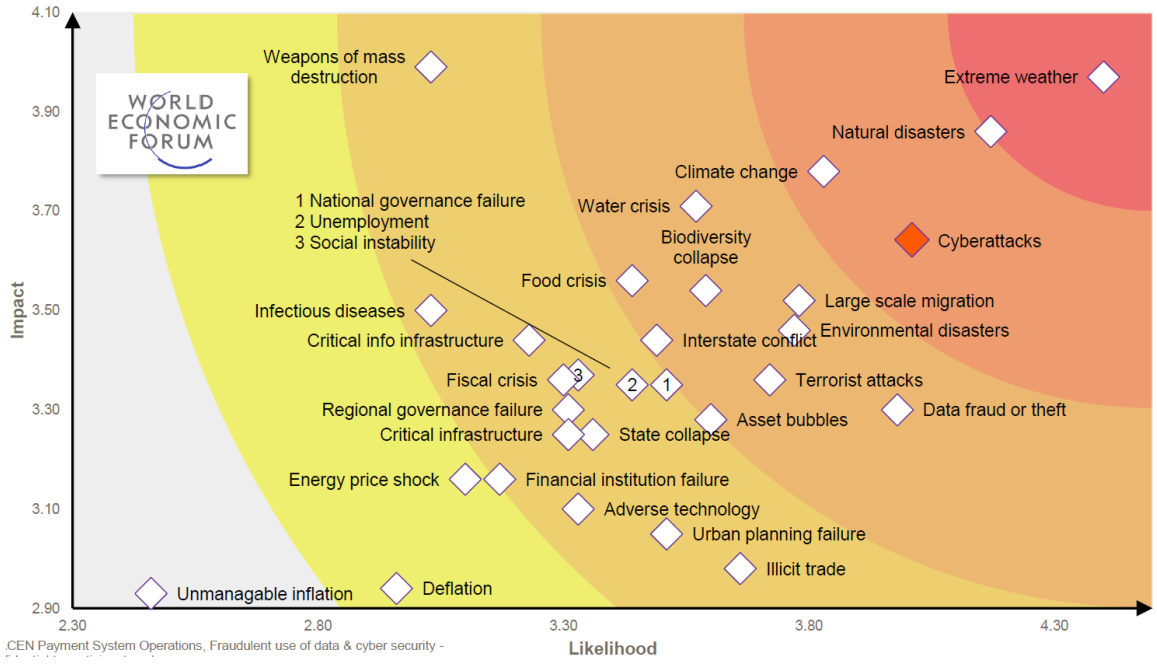
- 認知：組織內人員均應對資訊韌性有所認知，並了解在其中所擔任的角色。
- 學習與改進：定期或不定期檢視上述所有議題，並改善之。

肆、資訊安全相關原則與措施

由於資訊科技的進步，支付系統乃至金融服務出現了許多變革，例如透過網路連上銀行網站，無須至櫃檯使用銀行的服務；使用手機應用軟體或 QR-code 掃碼，即可完成轉帳或支付。除了個人的金融行為便利性提升之外，不同機構間也因系統連結更為緊密，使得資金的流動與清算更加快速。

然而這些行動裝置、雲端服務，甚或是金融科技等技術的普及，除了帶來商機，同時也大大的改變了組織現有的資訊架構及增加了許多未曾考量到的問題。例如使用硬體或軟體供應商提供的雲端服務，固然可以降低自行建置的成本，但相關的風險、安全及其他管理議題，均會與之前不同；又或是透過行動裝置提供或使用服務，其交易或個人資料就會面臨外洩的風險等。據世界經濟論壇(WEF)於2018年的調查，資訊攻擊已成為組織營運中，發生的風險及衝擊最大的幾項災害之一(如圖20)。

圖20　影響組織營運的災害



資料來源：SEACEN 課程講義。

在課程中，來自 SWIFT 的講師就針對這種與傳統教科書不同的環境變動，講述金融服務的監管單位或相關的資訊人員，面對如此的情況應注意的原則，以及使用哪些相關技術或措施應對：

- 安全的基礎架構
- 適當的監控工具
- 身分驗證

雖然課程中所提到的技術與應對措施是施行於 SWIFT 系統中，但亦可作為其他系統或環境設計相關措施時的參考。

一、安全的基礎架構

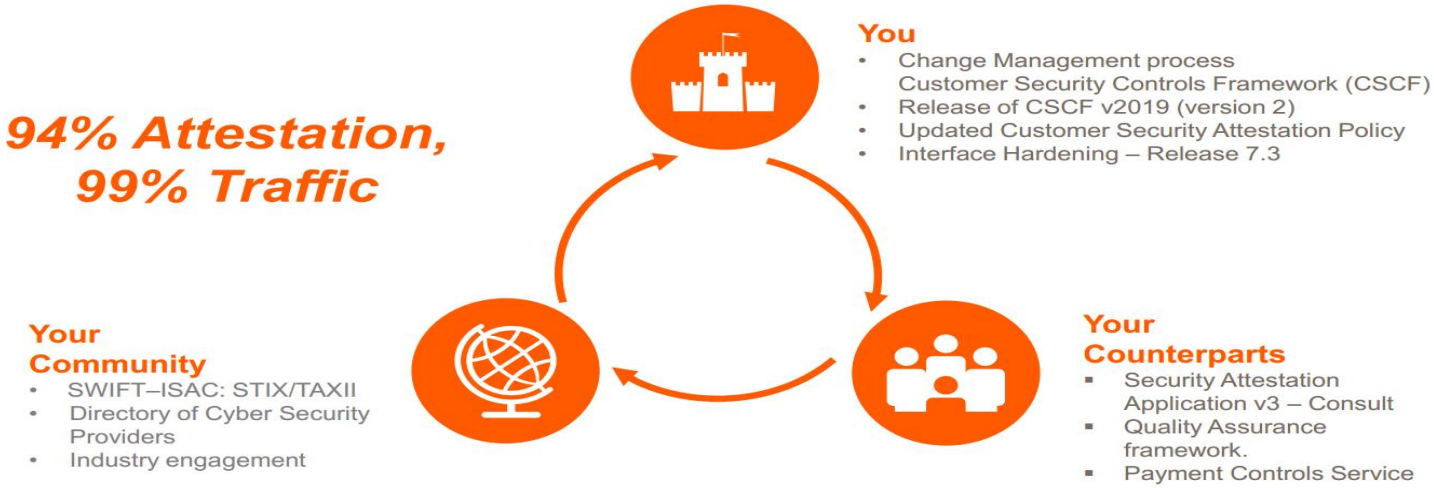
傳統上，資訊安全議題均由資訊相關人員負責，而這些資訊人員甚至可能沒有受過資訊安全訓練，導致在處理安全議題時，常將相關措施委由廠商代為規劃及處理；隨著資訊安全議題越發受到重視，專職於資訊安全的人員出現，對組織內的系統或營運流程均訂立嚴格的規範及處理條例；然而在組織間相互依賴程度大幅增加的現在，彼此的連結也應納入安全的資訊基礎架構中(如圖21)。

圖21　資訊安全範疇沿革

資料來源：SEACEN 課程講義。

為因應近年來日漸增多的世界各國遭受網路攻擊事件，SWIFT 國際組織於2016年8月啟動客戶安全計畫(CSP)，此計畫藉由強化系統工具之安全性、提供指引與評核框架以及資訊共享機制，旨在提升 SWIFT 系統整體的安全，範圍含括 SWIFT 用戶、交易對象及社群等三個領域(如圖22)。

圖22　SWIFT 客戶安全計畫

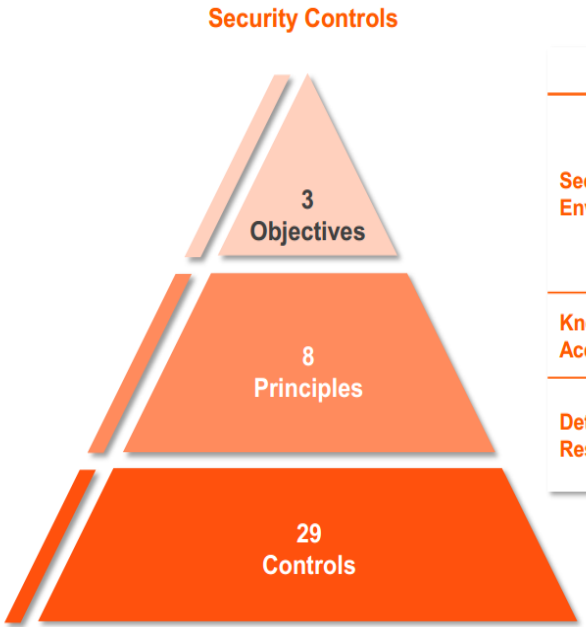


資料來源：SEACEN 課程講義。

此外，SWIFT 為協助會員機構建構安全的資訊基礎架構，另發展一個通用的客戶安全控制框架(CSCF)，以防護資訊環境、了解並限制存取及偵測與應變為3個主要的安全強化目標，並依據各個目標的強化領域，制定8項安全原則，再分別規劃列出相對應的29項安全控制措施，以確保 SWIFT 整個環境體系的安全。

這 29 項的控制措施中，最主要的核心概念為建構「安全區域」，將系統核心功能與資料置放於安全區域，且除了以防範惡意程式、弱點掃描、防火牆，以及異常行為監測等機制，防範外部滲透攻擊外，亦著重於特權帳號控管、資料及操作過程之安全及人事審核程序等，強化內部行為管理，以降低無論是來自組織內或外部的資訊安全風險(如圖 23)。

圖 23　SWIFT 客戶安全控制框架



CSP Security Controls Framework		
Secure Your Environment	1.	Restrict Internet access
	2.	Segregate critical systems from general IT environment
	3.	Reduce attack surface and vulnerabilities
	4.	Physically secure the environment
Know and Limit Access	5.	Prevent compromise of credentials
	6.	Manage identities and segregate privileges
Detect and Respond	7.	Detect anomalous activity to system or transaction records
	8.	Plan for incident response and information sharing

資料來源：SEACEN 課程講義。

二、適當的監控工具

在攻擊事件發生時組織內的所有系統均有潛在的危險，即使沒有直接對外相連的設備，仍有透過內部網路連結而被攻擊的可能性，對於關鍵的營運核心系統，若因為被攻擊而接收或發出錯誤的交易訊息，將導致組織遭受嚴重的衝擊或損失，故每個系統或至少核心系統應具有監控事件甚或阻止錯誤交易訊息送出的能力。

為確保不會送出錯誤的重要交易訊息，SWIFT 發展出一套支付控制警示工具，於此工具中可設定合法交易的訊息規格、金額區間、交易時點、幣別及對象等資訊，每當交易訊息要送出時，均須經過此工具之檢核，若有任意一項內容不符設定好的規則，即無法送出交易並以電子郵件或其他方式通知監控人員，以達到阻止錯誤交易的目標。

除了即時監控是否有預期外的交易，定期彙整的營運或交易事件報告也是不可或缺的，SWIFT 也針對此類報告的內容作出建議：

- 標準事件報告：圖形化介面、標示有人為介入的事件，或預期外的錯誤交易事件，以及彈性的過濾工具
- 營運報告：稽核紀錄、錯誤事件的統計資訊及錯誤處理紀錄
- 客製化報告：針對大額且特定幣別或對象的錯誤交易，以及交與組織外部單位之報告

SWIFT 也建議與外部其他單位合作，建立聯合資訊倉儲，共享資安事件資訊、監控方式及對策，以提高整個體系的安全性。

三、 身分驗證

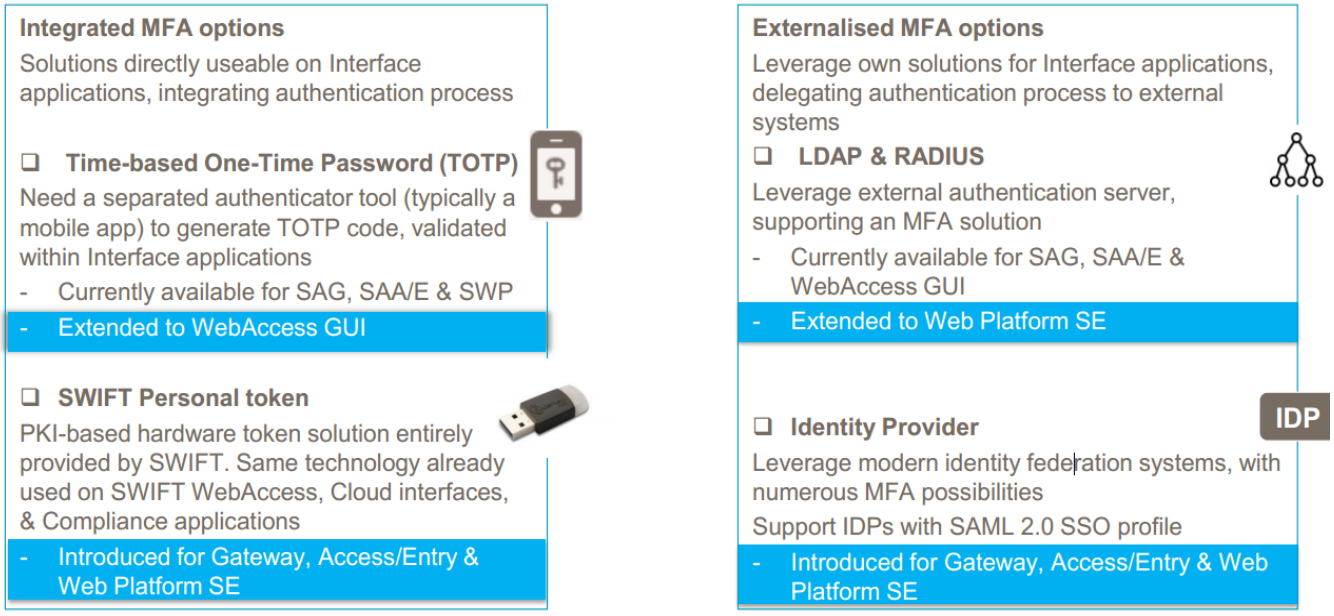
有鑑於許多重大資安事件均是起因於內部員工的帳號密碼被竊取，導致攻擊者取得權限進行不合法的操作，針對這類常見的組織內部風險，講師也提出多因子認證機制(multi-factor authentication, MFA)(如圖24)以為對策。

常見的驗證因子有三種：

- 知識因子：以只有使用者知道的事情作為驗證，例如帳號密碼及安全提問設計等。
- 持有因子：以使用者持有的物品作為驗證，如一次性密碼及憑證卡片等。
- 固有因子：以使用者與生俱來的生物特徵作為憑證，如指紋、聲紋或虹膜辨識等。

多因子驗證即為利用兩種以上驗證因子，來進行使用者之識別與授權，由於外部攻擊者通常只能竊取帳號密碼等知識因子，但難以取得持有因子及固有因子這類使用者本人之特徵或其持有之物品，故可降低組織內部之風險。

圖24　可採用的多因子驗證方式



資料來源：SEACEN 課程講義。

伍、心得及建議

一、心得

(一) 支付及清算系統運作順暢攸關貨幣及金融穩定

支付及清算系統處理伴隨經濟活動而生的各項收支與債權債務的清算業務，其為所有經濟金融交易的基礎，且為一國的重要金融基礎設施，系統運作攸關央行貨幣穩定與金融穩定之政策目標。

因大額支付系統一年系統營運金額通常達該國 GDP 之數十倍，並與該國金融機構相連結，當系統無法提供服務時，資金便無法於金融體系順利流通，利率形成將受到影響，進而影響貨幣政策之執行，若情況嚴重時，更可能引起系統性風險，影響金融穩定。因此，央行須維持安全有效率的支付清算系統。

(二) 馬來西亞與我國均定期檢視支付系統之風險管理措施

鑑於支付及清算系統之重要性，央行等系統營運者應辨識、控制支付及清算系統風險，並定期檢視風險管理工具，包括擔保品、折價率、日間透支、佇列等候機制、款券同步交割、款對款同步收付機制、即時總額清算、強化維運支付系統資訊基礎設施，以及擬定備援機制與營運不中斷計畫等。

馬來西亞近年來新增之支付系統風險管理工具，包括隔夜資金自動擔保機制、資金互卡解決機制，並採用 SWIFT 訊息標準等，目前亦研議未來採流動性最適化清算機制及 ISO 20022 訊息標準。

我國近年新增之風險管理工具，包括 2008 年將中央登錄公債的交割款項，納入本行同資系統清算，採 DvP 機制，提升結算交割效率及降低清算

風險；2012 年建置延時管理機制；2013 年將聯合信用卡中心結算的應收應付款項，納入同資系統清算，提升信用卡清算效率；2014 年起與外幣結算平台連結，辦理美元與新臺幣換匯交易款對款同步收付機制功能；以及 2019 年強化同資系統備援演練。本行要求各參加單位，每年至少辦理 1 次媒體備援作業演練，以增進其業務持續運作能力等。

(三)僅靠資訊技術無法完全確保營運韌性

由於金融市場基礎設施對資訊技術的依賴性提高，且各種資訊攻擊具有方式複雜及沒有明確復原方式等特性，對於作業風險管理帶來與以往不同的挑戰。

面對這樣的情勢，持續營運策略也必需要作出調整，採取持續且較為彈性的管理方式、以及管理金融服務與資訊服務或其他組織相互依賴所產生的問題，均是需要考量的議題。

因此確保組織的營運韌性並非僅是單純的資訊技術議題，而需高階管理階層的重視、投入足夠的資源，並透過與其他單位通力合作才能使組織具有足夠的能力，以因應各種來源及形式的攻擊。

(四)資訊分享為金融體系安全的重要元素

資訊科技的演進可說是日新月異，為防止來自網路的各種攻擊，組織內的資訊安全規範與措施須不斷改善。對於現代的金融體系來說，最重要的可能並非是資訊安全架構本身，而是此架構因應環境的應變能力。

然而單一組織所具有的資訊安全能量未必充足，因此如何與其他外部組織合作、整合彼此間的安全架構以及分享資安訊息與事件處理方式，就成為建構安全且具有彈性的金融體系之重要元素。

二、建議

(一)持續關注主要國家央行對大額支付清算系統之改革成效，以作為強化我國同資系統之參考

本次與會各國央行之大額支付系統，多已採行 RTGS 機制(除柬埔寨及尼泊爾)並有改造計畫，逐步發展為結合更多功能及清算幣別的新世代 RTGS 支付清算系統，如印尼及菲律賓等國。另外，馬來西亞為改善大額支付系統之信用及流動性風險，2014 年實施隔夜資金自動擔保機制，2016 年實施資金互卡解決機制，未來則擬採行流動性最適化清算機制。

我國央行同資系統自 1995 年建置以來，持續實施改造計畫，逐步強化其功能。本行同資系統採即時總額清算機制，有效降低系統之信用風險，且本行為提供參加單位流動性，兼採日間透支等機制，同資系統已成為全國金融支付之樞紐，提供完善的支付基礎設施。然而，雖然同資系統現行運作頗為順暢，惟考量日後國內資金可能出現資金緊俏的情況，似可研議同資系統導入資金互卡解決機制或流動性最適化清算機制之可行性。另為提升本行之監管職能，本行已於 2019 年建置「同資系統日間流動性監控系統」，未來可持續關注主要國家央行對大額支付清算系統之改革成效，以作為強化同資系統之參考。

(二)本行應提高系統之營運韌性

營運持續管理是金融市場基礎設施作業風險管理架構的關鍵組成，包含營運衝擊分析、災害復原策略及營運不中斷計畫等，本行除應定期檢視上述策略或計畫之可行性及完整性，亦應落實備援演練、人員配置與訓練，以提高抵禦營運中斷的能力。本行為確保大規模失序狀況發生時，同資系統仍能維持營運不中斷，現已建置備援中心，隨時接替主中心作業，並定期辦理演練作業，以驗證備援中心之作業可靠性。此外，本行要求連線機

構應強化同資系統備援演練。

除此之外，本行亦應加強行內單位間合作，以及蒐集外部相關單位之資訊。業務與資訊單位的相互了解，可使業務政策在安全性上更加周延，且資訊系統更能滿足業務需求；定期蒐集來自政府機關、金融及資訊業界的資訊安全資料，亦可作為本行改善政策或系統之參考，以強化資訊架構安全，提升營運韌性。

(三)加強與本行連線機構之合作與監管

金管會為提升金融體系資安防護能量，於 2017 年 12 月建立「金融資安資訊分享與分析中心(F-ISAC)」，並委請財金公司營運，提供金融機構通報及資安資訊分享等服務，以協力營造金融資安聯防體系。

本行可加強在金融資安聯防體系內的角色，除定期自 F-ISAC 蒐集資安資訊，同時亦可針對參加央行同資系統之連線機構要求進行內部資安風險評鑑並內部查核辦理情形，以達到提升資訊安全之目標。

參考資料

1. 本次訓練課程主辦單位提供與會學員講義資料(2019)。
2. 中央銀行(2009)，「中華民國支付及清算系統」，9 月。
3. 陳南光(2013)，「貨幣銀行學」，雙葉書廊出版社，5 月。
4. 曹世樺(2016)，「參加 SEACEN 第 1 屆支付及清算系統基礎課程」公務人員出國報告，7 月。
5. 張逸綸(2018)，「參加 SEACEN 支付及清算系統基礎課程」公務人員出國報告，5 月。
6. 龔玲雅(2019)，「本行同資系統營運管理近期措施」，中央銀行支付清算季刊，108 年第 2 期。(內部資料不公開)
7. BNM (2018), "Financial Stability and Payment Systems Report 2017," *BNM Publications*, Mar.
8. BNM (2019), "Financial Stability and Payment Systems Report 2018," *BNM Publications*, Mar.
9. ECB (2008), "Payments and Monetary and Financial Stability," *ECB-BANK of ENGLAND Conference*, Nov.
10. PayNet (2018), "Operational Procedures for Malaysian Ringgit (MYR) Settlement in the Real Time Electronic Transfer of Funds and Security System (RENTAS)," *PayNet Publications*, Jul.