

金融監督管理委員會因公出國人員出國報告

(出國類別：其他)

參加 APEC 金融監理人員訓練倡議 「反洗錢及反資助恐怖主義金融 監理研討會」報告

服務機關：金融監督管理委員會銀行局

姓名職稱：劉萬基 副組長

派赴國家：庫克群島

出國期間：107 年 9 月 29 日至 10 月 7 日

報告日期：107 年 10 月 19 日

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－反洗錢及反資助 恐怖主義金融監理研討會APEC Financial Regulators Training Initiative (FRTI) – Regional Seminar on Anti-Money Laundering & Counter Terrorist Finance Supervision
會議時間	107 年 10 月 1 - 4 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	劉萬基、金融監督管理委員會銀行局、副組長
連絡電話、 e-mail	(02) 8968-9782 gordonl@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)	本次研討會研討會旨在從金融監理人員之立場， 評估洗錢及資恐對銀行在操作、法律及信譽風險 等各方面之影響，檢視銀行之風險評估、盡職審 查、交易監控作業及內部遵循方案，並適時採取 強制行動。
後續辦理事項	無。
建議資深官員 發言要點(★請 務必依會議最 新情形提建議， 並提供簡要 中英文說詞，以 1 頁為限)	(無建議可免填)
檢討與建議	1. 風險評估應增加威脅及弱點之實證案例。 2. 強化國際合作。 3. 檢視裁罰案件之監理政策。

1. 參加資深官員會議暨相關會議，請於會議當日填列此表，以 e-mail 寄至外交部 APEC 小組電子信箱: apccct@mofa.gov.tw
2. 出席其他各項會議人員，請將本表附於與會報告首頁。

3. 14 號字標楷體，行距行高 20pt，請自行調整表格大小。

目錄

壹、 課程目的.....	1
貳、 課程介紹.....	2
一、 課程時間.....	2
二、 主要講座簡介.....	2
三、 課程內容.....	2
參、 課程內容摘要.....	3
一、 洗錢防制及打擊資恐導論.....	3
二、 風險分析及法令遵循.....	5
三、 Antigua-Columbia 案例研討.....	7
四、 可疑交易申報及場外監理.....	10
五、 客戶驗證.....	11
六、 行動支付及新興科技.....	13
七、 強制行動之案例研究.....	16
肆、 心得與建議.....	19

壹、課程目的

APEC 金融監理人員訓練倡議 (Financial Regulators Training Initiative ; FRTI) 成立於 1998 年，提供有系統、完整且持續的方式，以促進金融監理之品質及效率，亦為 APEC 財長會議下歷時最久之倡議。

APEC FRTI 成立宗旨，在於強化 APEC 會員國家金融監理能力及訓練計畫之合作，訓練對象以初、中階監理人員為主，包括各國央行和證券交易員，以及金融監理機關人員。

本次研會係由亞洲開發銀行主辦，邀請東南亞國家中央銀行聯合會 (以下簡稱 SEACEN)、澳洲金融情報中心 (以下簡稱 AUSTRAC)、菲律賓 BSP 銀行及庫克群島金融監理委員會人員擔任講座，課程目的在於使學員了解，並透過案例討論方式使學員互相交流各國監理經驗。

本次參與研討會之學員來自國，計 16 人：庫克群島 (9 人)、巴布亞新幾內亞 (2 人)、索羅門群島 (2 人)、東加群島 (1 人)、臺灣 (2 人)。

貳、課程介紹

一、課程時間

107年10月1日至10月4日

二、主要講座簡介

- (一) Mr. Mark McKenzie：SEACEN 金融穩定監理及支付清算系統部資深分析師。
- (二) Ms. Sue Wong：AUSTRAC 資深經理。
- (三) Mr. Heinz Ryan H. Espinosa：菲律賓 BSP 銀行金融系統組長。
- (四) Ms. Cheryl McCarthy：庫克群島金融監理委員會副委員。
- (五) Mr. Alan Taylor：庫克群島金融服務發展部。

三、課程內容

日期	主題
10月1日	洗錢防制導論
	打擊資恐導論
	洗錢防制風險分析
	法令遵循方案
10月2日	高風險客戶及加強盡職調查
	洗錢防制案例研討
10月3日	可疑活動之監控及申報
	客戶驗證方案
	法人及法律協議之風險分析

	場外監理
	行動支付之比例性管制法令
10月4日	新興科技對洗錢防制之意涵
	強制行動之案例研究

參、課程內容摘要

一、洗錢防制及打擊資恐導論

(一) 洗錢防制導論

1. 由於科技進步，金融交易之速度及便利性提高，犯罪者隱藏資金而不易查緝，致使洗錢金額難於正確統計。據聯合國毒品及犯罪辦公室估計，全球每年洗錢金額，約占 GDP 百分之 2 至 4，相當於 800 billion 至 2 trillion 美元。
2. 在洗錢之定義及流程方面，特別提到在處置（placement）階段及時阻絕之重要性，這通常是銀行負擔的任務。
3. 為杜絕洗錢，須注意 5 項法遵基本要素。1 指派法遵主管。2 將政策及程序書面化。3 將評估風險及抵減風險之措施文件化。4 持續的員工訓練計畫。5 至少每 2 年進行 1 次獨立審查。
4. 常見之法遵缺失有：1 紀錄保存不足。2 過時或不具針對性的政策及程序。3 投入到法遵之資源不足。4 不適當的認識客戶或加強客戶審查。5 不適當的風險評估。6 不充分的交易監控程序。7 不適當或不具針對性的員工訓練。8 未及時申報大額或可疑交易報告。9 不適當或

不具獨立性的測試。

(二) 打擊資恐導論

1、 洗錢與資恐之區別

在資金之來源及去向方面，前者，是將非法資金轉變為合法外觀；後者，是將合法資金提供予恐怖分子使用。因此，前者需追查資金來源，後者要了解資金去向。

2、 資恐之流程

(1) 簡言之有 3 個步驟：1 資金匯集 (Collection)，資金來源可能是合法或非法。2 資金輸送 (Transmission)，透過一系列經過設計的交易以隱藏資金來源。3 資金使用 (Use) 於恐怖分子或恐怖行為。

(2) 就資金匯集言之，有 4 種資金來源：合法來源自行籌資 (Self-funding from legitimate sources)、非營利組織 (NPO, Non Profit Organizations)、社群媒體或群眾募資 (Funding through social media and crowd funding)、犯罪行為 (Criminal activity)、銀行或其他匯款服務業者。

(3) 就資金輸送言之，有 4 種主要方法：銀行系統、其他匯款業者 (替代匯款業者 Alternative Remittance 或貨幣服務業者 Money Service Business)、跨境資金移轉、國際貿易系統。

(4) 就資金使用言之，有 4 種用途：線上支付帳戶、信用卡或貸記卡、數位儲值、捐款予慈善機構。

3、 AUSTRAC 於 2016 年發布之東南亞及澳洲資恐風險評估區域研究報告 (Regional Risk Assessment on Terrorist Financing 2016 South East Asia & Australia)

本報告所做出之各國風險評估表，頗具參考價值。

- (1) 在資金匯集方面，依 4 種資金來源之風險高低，賦予高、中、低之評等。評估結果，印尼在 4 種資金來源均為高風險，澳洲、馬來西亞、泰國次之，再次為菲律賓，風險最低為新加坡。

資金匯集	澳洲	印尼	馬來西亞	菲律賓	新加坡	泰國
合法來源自行籌資	高	高	高	Negligible	中	高
非營利組織	高	高	中	中	低	高
社群媒體或群眾募資	中	高	高	中	低	中
犯罪行為	中	高	低	高	低	中

- (2) 在資金輸送方面，由於澳洲之金融系統發達，在各種輸送管道都具有高風險。風險最低者亦為新加坡。

資金輸送	澳洲	印尼	馬來西亞	菲律賓	新加坡	泰國
跨境資金移轉	高	高	高	高	中	高
銀行系統	高	中	中	中	中	中
其他匯款業	高	中	低	中	中	低

4、 風險控制的方法

- (1) 建立制裁名單。
- (2) 採取風險基礎方法之防制措施。建立下列風險指標：消費者行為模式、經濟圖象、地理風險、消費活動、產品及服務。

二、 風險分析及法令遵循

(一) 洗錢防制風險分析

- 1、 風險管理架構 5 步驟：確立目標、辨識風險及控制、評估風險及控制、衡量及採取行動、監控及報告。
- 2、 風險評等矩陣圖

風險要素	法遵風險			法遵風險管理之品質		
	低	中	高	強	滿意	弱
產品及服務	低	中	高	強	滿意	弱
客戶	低	中	高	強	滿意	弱
地理位置	低	中	高	強	滿意	弱

說明：

- (1) 風險要素：產品及服務、客戶、地理位置。依照各個風險要素，分別賦予高、中、低評等。
- (2) 法遵之品質：對威脅管控之程度：強、滿意、弱。
- (3) 金融機構須紀錄風險分析之結果並說明其合理性。

(二) AMLCFT 法令遵循方案

1、 AML 風險分析之流程

- (1) 辨識及衡量風險：產品及服務、客戶、地理位置。
- (2) 內部控制：政策、程序、系統、控制。
- (3) 產出結果為風險基礎方案：內部控制、稽核、法遵主管、員工訓練。

2、 AML 法令遵循方案之 4 個支柱

- (1) 政策及程序
- (2) 法令遵循主管
- (3) 員工訓練
- (4) 獨立稽核

3、 防制措施

- (1) 客戶盡職審查 (CDD, Customer Due Diligence)
- (2) 確認客戶程序 (CIP, Customer Identification Process)
- (3) 了解員工
- (4) 持續監控

(三) 高風險客戶及加強盡職調查

1、高風險客戶 (Higher-Risk Customers, HRCs)，指客戶之下列事項暴露於高風險業務活動：股權架構、預期或實際之交易量、交易型態（包含涉及高風險國家之交易）。

高風險客戶包括：高知名度政治人物 (Politically Exposed Persons, PEPs)、通匯銀行 (Correspondent Banking)、金錢及價值移轉服務業 (Money/Value Transfer Services, MVTs)、電匯 (Wire Transfers)。

2、對於高風險客戶應加強盡職調查 (Enhanced Due Diligence, EDD)，亦即更詳細審視開戶，並更頻繁的檢視客戶與銀行之交易關係。

銀行應取得下列資訊：開戶目的、資金及財富來源、帳戶之實質控制人（包括實質受益人、文件簽署人、保證人）職業或業務類型、財務報表、銀行同業照會、住所或登記地、地緣關係、雇員所在地及營業所在地、帳戶活動變更之說明。

盡職調查是持續的過程，銀行應確保帳戶資訊及時、以風險為基礎進行交易監控、適時調整風險圖象、可疑交易申報應與風險圖象具有一致性。

三、 Antigua-Columbia 案例研討

(一) 案情摘要

1、1989年12月，哥倫比亞警方逮捕販毒集團首腦並扣押其財產，其中有232件以色列製造的自動步槍，經檢視貨運流程係由以色列運送至安地卡 (Antigua)。表面上是 Antigua 向 Israel 買武器之合法交易，實際上武器卻運送到了毒梟手中。

本案是發生於1988至1989年間之真實案件，具有指標意義。高知名度政治人物、通匯銀行、跨國合作等洗錢防制措施之發展，無不與本案有關。

2、 主要涉案人

- (1) Yair Klein 是卸任以色列國防部官員，在特拉維夫設立 Spearhead 公司，提供軍事訓練及保全服務。
- (2) Maurice Sarfati 是安地卡首相 Vere Bird Sr. 及其子 Vere Bird, Jr. 部長之好友及生意合作夥伴。
- (3) Pinchas Shachar 是卸任以色列准將，現任以色列軍事工業公司 (IMI) 設於邁阿密之代表，於邁阿密銀行設立私人帳戶。
- (4) 透過 Sarfati 牽線，安地卡政府國防部與 Klein 合作設立軍事訓練學校，向 Shachar 購買 500 件武器。

3、 金流

- (1) 預付款 Down payment (November, 14, 1988, \$98,131) : Spearhead 在巴拿馬 Banco Aleman-Panameno 銀行之帳戶，經過中轉行位於紐約市之費城國際銀行及漢諾威信託公司，匯至 Shachar 在邁阿密 Hapoalim's 銀行之帳戶。(註：國際銀行間交易常使用中轉行，因為銀行彼此間未必有直接通匯關係。本例之漢諾威信託公司即屬通匯銀行。)
- (2) 尾款 Balance due, L/C (April, 19, 1989, \$228,705) : Shachar 在 Hapoalim 銀行邁阿密分行開立支票存款帳戶，收取信用狀，支付予 IMI。
- (3) 有趣的是，在 February, 3, 1989 同一天，有一筆 \$44,000 資金，自 Spearhead 透過中轉行，匯至 Luis Meneses Baez 在特拉維夫 Hapoalim 銀行之帳戶。Luis Meneses Baez 是已退役的哥倫比亞軍事武官，擔任的國外傭兵及毒品販運之中間人。

4、 物流

運送 500 件武器於 March 28, 1989 自以色列之丹麥船 Else Thuesen

啟程，於 April 22 至安地卡，卸貨至巴拿馬船 Seapoint。其後航程失去紀錄，據調查係將武器運送至哥倫比亞海域之私人遊艇。

(二) 調查結果

1、 美國國會司法調查委員會

- (1) 在取得以色列武器之交易中，安地卡政府有嚴重貪瀆現象。
- (2) 譴責以色列政府未盡武器販運之管制查證責任。
- (3) Klein 及 Sarfati 偽證及偽造單據，但由於巴拿馬政府不配合，委員會未能取得 Klein 及 Sarfati 之存款帳戶資料。

2、 結論

- (1) 原本應運送安地卡之武器，卻轉運至哥倫比亞毒梟手中，Klein 及 Sarfati 負主要責任。
- (2) 預付款及尾款均係由 Spearhead 在巴拿馬之 Banco-Aleman Danemeno 銀行帳戶匯出。其資金來源，據 Klein 說明係巴拿馬流亡政府合法利用美國提供之資金（目的在推翻當時巴拿馬的諾瑞加政權），但顯然並非事實。
- (3) 雖然\$44,000 匯款之目的未明，但可作為一項佐證，證明安地卡政府購買之武器，其資金是來自哥倫比亞毒梟。
- (4) 巴拿馬政府拒絕提供銀行帳戶資料，以致執法人員無法釐清案情。（註：Spearhead 帳戶之資金似應來自哥倫比亞毒梟，但因未能取得巴拿馬銀行帳戶資料而無法證明）

(三) 小組討論議題

- 1、 以銀行立場，對重要涉案客戶進行風險分級，檢視高知名度政治人物及實質受益人之合理審查程序。
- 2、 對本案提到的產品、服務、交易型態進行分類，分別賦予高中低之評等。

- 3、以巴拿馬銀行監理者之立場，評估銀行之洗錢資恐政策及銀行內部風險評估之有效性。
- 4、分析費城國際銀行及漢諾威信託公司於金融交易中之地位。以銀行監理人員之立場，說明通匯銀行應有之作為。
- 5、說明電匯應有之政策及程序。並說明 MSB 業者如西聯 (Western Union) 及速匯金 (MoneyGram)，其風險控制及抵減應有之步驟。
- 6、本案在不同層面 (犯罪偵查、金融監理等) 國際合作之重要性。

四、可疑交易申報及場外監理

(一) 可疑活動之監控及申報

1、交易監控方案 (Transaction Monitoring Program, TMP)

應基於下列要素評估風險：客戶資料、產品、交易地點及目的地、交易管道。

特別應注意：定期評估控制系統、處理紅旗警示 (close alert) 之時間、必要時向上級陳報 (escalation procedures)、充足的資源。

2、監控紅旗指標 (Monitoring alerts and indicators)

紅旗指標：評估高風險客戶、複雜及不尋常的大額交易、無明顯經濟或法律目的之非典型交易、交易地點或目的地涉及高風險國家。

資恐指標：客戶行為、經濟資源、地理風險、支付活動、產品及服務。

3、可疑交易報告

澳洲法令規定，資恐案件應於 24 小時內申報可疑交易報告，其他則需於 3 個營業日內。

報告內容應包括：完整的交易細節、說明可疑之理由、起頭處以

一至二行簡要說明 (BLUF, Bottom Line Upfront Front)、明確且簡要說明可疑活動、引述 FATF 方法論之關鍵字。

可疑交易報告應具有之品質：明確、即時、相關性、精準。

情報循環 (Intelligence Cycle)：計畫→蒐集資料→評估→分析→分送

(二) 場外監理

1、資訊流程 (flow of information)：資訊來源 (評估、交易報告、年度法遵報告、其他主管機關、開放資訊) → 分析 → 作出報告 (弱點、趨勢及環境變化) → 交給第一線人員參考

此模型之優點：(1) 將資料摘要，以提供金融犯罪環境之細節。

(2) 具有目標性及優先順序。(3) 衡量介入之影響程度。(4)

評估報告機構之行為。

場外監理應定期檢視報告機構之風險圖象，並聽取執法機關之意見。

2、行為方法之 5 個步驟：(1) 分析 (假設、建立標準、無資料時應想辦法釣取資料、觀察) → (2) 選取目標 (哪一個報告機構符合標準而成為鎖定目標) → (3) 程序 (盡職調查、信函、篩選、評估反應、成果) → (4) 綜合 (評估整體遵循程度、分析影響) → (5) 未來策略

五、客戶驗證

(一) 客戶驗證方案

客戶驗證方案 (Customer Identification Programme, CIP)，指金融機構能具有合理的確信，了解每一個客戶的真實身分。CIP 必須書面化，符合金融機構之規模及業務型態。CIP 應包含開戶程序，詳述確認客戶身分之資訊。

高風險時應加強客戶審查，取得額外資訊：辨識實質受益人（**beneficial owner**）、客戶之性質及交易目的、客戶之控制權架構、資金來源。

實質受益人，大多數情形指法人或法律協議之控制權人。在客戶為自然人時，實質受益人指有代表人之本人。

（二）法人及法律協議之風險分析

- 1、 所有法人或法律協議均可能被用來隱藏實質受益人之身分，即使是最簡單的公司，也可能透過代名人（**nominee** 代名董事或代名股東）或單純不揭露事實等方式來隱藏身分。因此所有法人或法律均具有洗錢資恐風險。
- 2、 終極目標是透明化。方法是找出控制法人或法律協議之自然人。若未能回答此問題，則客戶具有高風險。
- 3、 法人之風險評估因子：（一）類型：公司（公開發行公司或非公開發行公司）、基金、合夥、協會。（二）類型間之差異：所有權、債務、治理。（三）法人內部行使控制權之方法（代名人、無記名股票、保證人）。（四）可向誰取得何種資訊：登記機關、公開資訊、主管機關持有之資訊、財務紀錄、機關報告（稅、**CRS**、**FATCA**）。
- 4、 法律協議之風險評估因子：（一）類型：普通法或成文法、可撤銷或不可撤銷、裁量權、固定利率、空白信託、信託目的、慈善。（二）受託人：國內或國外。（三）受益人：指定或未指定、裁量或固定。（四）委託人保留之權限：得否指定或撤換受託人、受益人、信託監察人。（五）信託資產：來源、性質、所在地、控制權人。（六）可向誰取得何種資訊。
- 5、 信託及公司服務業（**Trust and Company Services Providers, TCSP**）可能增加風險之情形：提供空殼公司、未直接控制活動或資產、

未與實質受益人面對面接觸、使用仲介、提供郵寄服務、組成客戶資金池。

- 6、 解決方案：TCSP 應許可或登記、要求 TCSP 持有實質受益人及法人資產與活動之即時資訊、申報可疑交易、員工訓練、監理稽核其法遵情形。

六、 行動支付及新興科技

(一) 行動支付之 AMLCFT 比例性管制法令

1. 客戶盡職調查

低風險時，採簡化盡職調查。一般風險時，採標準盡職調查。高風險時，採加強盡職調查。

簡化盡職調查指：(1) 要求較少的身分證明文件。開戶時，自然人僅須提示可接受的身分證明文件，法人僅需提示董事會決議或其他相當文件。(1) 簡化的驗證程序，在一定門檻下可接受郵遞方式驗證，也可以接受非標準化的文件。(1) 可在交易完成後，再確認客戶、實質受益人及授權簽署。(1) 減少更新客戶身分確認的頻率。(1) 減少帳戶監控的程度。

2. 比例性之洗錢防制措施

下表列示在不同的風險等級，依法令規定有不同的身分確認文件、帳戶金額上限、資金進出限額、服務項目。

	Requirements	Account Limit	Money-in (self-load)	Money-out	Services
Tier 1 KYC 0	Name, Mobile number	50,000 Aggregate Monthly	5,000 (transaction limit per	Not Available	Money-in Bills

		limit	channel in a single day subject to monthly account limit)		Payments Airtime Reload VISA/MC/Purchases
Tier 2 PRE KYC 1	Submit: Name, Mobile number, Birthday, Address, Nationality, Source of funds, Photo (ID and/or selfie)	50,000 Aggregate Monthly limit	5,000 (transaction limit per channel in a single day subject to monthly account limit)	5,000 Daily Limit 10,000 Aggregate Monthly Money-out ATM or P2P	Money-in Bills Payments Airtime Reload VISA/MC/Purchases Money-out
Tier 3 KYC 1	Face to Face Agent Validation with complete minimum information (ie. Nature of work and TIN, SSS, or GSIS)	100,000 Aggregate Monthly limit	50,000 (transaction limit per channel in a single day subject to monthly account	20,000 ATM Max Amt/day 50,000 P2P Max Amt/day	

			limit)	and/or 15 txn counts/day	
--	--	--	--------	-----------------------------	--

(二) 新興科技（比特幣、加密貨幣）對 AML 之意涵

1、發展趨勢

- (1) 數位貨幣之匿名性及交易欠缺透明度，使其成為洗錢、資恐、線上毒品販售、人口販運之工具。並助長軟體綁架、惡意程式攻擊之盛行。據雪梨大學估計，約有一半的比特幣交易涉及犯罪。
- (2) FBI 及執法部門使用近 75% 時間查緝與數位貨幣有關之洗錢犯罪。
- (3) 自 2011 年起有 6% 比特幣被竊，估計 2017 年底超過 6 億美元被駭，顯示比特幣交易平台（exchanger）欠缺保障資訊安全的能力，其認識客戶程序亦待改善。
- (4) 犯罪者傾向於以小額與特定交易對手重複交易比特幣，犯罪者之間比特幣交易之密集程度甚高，亦即將比特幣作為交換媒介。犯罪者持有的比特幣金額較小，以免被執法機關扣押。反之，合法交易之人，則傾向持有比特幣，將之視為價值儲藏之工具。
- (5) 由於加密貨幣匿名之特質，且採區塊鏈交易而欠缺中央清算機構，增加交易監控之難度。

2、監理議題

- (1) 在那一個加密貨幣之環節進行管理，挖礦或交易？
- (2) 加密貨幣是商品或有價證券？
- (3) 以區塊鏈技術如何驗證加密貨幣交易？

3、銀行之對策

- (1) 銀行對於將法定貨幣(fiat)兌換成虛擬貨幣(virtual currencies) 中介機構(intermediaries)，應課予洗錢防制及打擊資恐之監督作業。中介機構包括交易平台(exchanges)及經紀商(brokers)。
- (2) 對於比特幣及區塊鏈技術帶來的機會及風險，應建立風險模型以監視其對於洗錢防制及詐欺之威脅。
- (3) 依比特幣法令及最佳實務作業，在所有涉及之相關國家，進行持續性監督。監督方案包括：(1) 對於下列交易對手保持警覺：與比特幣團體進行業務交易之公司客戶、接受比特幣存款之金融機構或中介商。(2) 監督客戶及交易對手間之資金流向。
- (4) 列管已登記或註冊之比特幣交易平台。如此將有助於辨識那些未登記或註冊的平台，並有助於辨識實質受益人。
- (5) 已登記或註冊之比特幣交易平台及其實質受益人，應採取嚴格的客戶審查程序。例如，交易對手有無對公開的比特幣帳戶(存款人所持有比特幣之來源及去向)執行風險分析。
- (6) 對接受以比特幣支付之公司，評估其承受網路威脅之程度。

七、強制行動之案例研究

(一) 澳洲金融情報中心 AUSTRAC (Australian Transaction Reports and Analysis Centre) 採取強制措施之流程

1、辨識及確認違規事實

2、違規之靜態風險分析 (static risk)

自該違規行為之屬性決定風險程度：(1) 極端風險：建立洗錢資恐方案、執行客戶確認程序、交易監控、可疑交易報告。(2) 高風險：建立通匯銀行業務前執行盡職調查、國際資金移轉報告。

3、決定動態風險 (dynamic risk)

自報告機構之法遵情形決定風險程度：(1)報告機構之法遵歷史。

(2) 報告機構之違規行為。(3) 未遵循在規模及性質上之影響程度。

4、決定回應方式 (determine response)

回應方式之選項：(1) 什麼都不做。(2) 自動遵循如教育訓練及發布指引。(3) 命令採取改善措施。(4) 強制外部稽核及風險分析。(5) 強制行動。

(二) 強制行動

1. 考量因素：(1) 違規事實之性質及嚴重程度。(2) 有無導致犯罪者濫用金融機構管道之重大風險。(3) 報告機構法遵之意願及努力。(4) 有無自動陳報違規事實。(5) 強制行動之可能後果。
2. 強制權力之類型：(1) 警告函。(2) 改善命令。(3) 禁止命令。(4) 強制執行。(5) 裁罰。

(三) 澳洲聯邦銀行 (Commonwealth Bank of Australia, CBA) 裁罰案例研究

1、AUSTRAC 與 CBA 於 2018 年 6 月 4 日達成合意令，後者同意就下列違反洗錢及資恐法令之違規行為，支付澳幣 7 億元：

- (1) 自動存款機 (Intelligent Deposit Machines, IDMs) 此項新商品推出前，未分析洗錢資恐風險。
- (2) 未採取控制措施以抵減及管理 IDMs 之洗錢資恐風險。
- (3) 自 2012 年 11 月至 2015 年 9 月，計有 53,506 筆、價值澳幣 6 億 2 千 5 百萬元涉及 IDMs 之大額交易報告，未及時申報 AUSTRAC。
- (4) 於 3 年期間內，未依防制洗錢打擊資恐方案，對 778,370 個帳戶進行交易監控。

- (5) 對金額達數千萬澳幣之可疑交易未及時申報。
 - (6) 已意識到帳戶有可疑交易，卻未對客戶進行持續監控以抵減或管理風險。
- 2、 本案屬澳洲有史以來金額最大之裁罰案件，其考量主要係基於CBA防制作業之重大缺失，導致罪犯易於利用作為洗錢資恐之管道，使澳洲公眾暴露於重大風險中。其理念在於昭示銀行業，法遵成本固然很高，但未遵循法令之成本將會更高。

肆、心得與建議

本次研討會旨在從金融監理人員之立場，評估洗錢及資恐對銀行在操作、法律及信譽風險等各方面之影響，檢視銀行之風險評估、盡職調查、交易監控作業及內部遵循方案，並適時採取強制行動。課程重視與學員的互動，並鼓勵學員提出問題，透過分組討論，分享各國監理經驗，課程相當緊湊且充實。以下提出心得與建議：

(一) 風險評估應增加威脅及弱點之實證案例

我國首部國家風險評估報告（NRA）於本（107）年完成，已取得初步成果，但仍有許多待改進之處：1.多數結論基於理論推導，欠缺實證數據及案例之支持。2.僅辨識固有風險，欠缺殘餘風險之分析。3.行動方案之制定，程序上未經各部會詳細討論審視。從而銀行業者反映，威脅及弱點分析因欠缺案例支持，對於銀行業者辦理機構風險評估（IRA）之效益有所減損。

此外個別執法機關所作之風險分析，僅有法部調查局提供之少數案例，類型有限且數量較為不足。

本研習會提供之 Antigua-Columbia 洗錢案及澳洲聯邦銀行裁罰案，前者在洗錢防治之制度演進上具有指標性意義，後者係銀行監理機關以嚇阻性方式促使業者遵循，參考價值甚高。未來我國進行第二次國家風險評估或執法機關辦理洗錢資恐風險分析時，宜提供更多實證案例，並深入分析其洗錢資恐手法，以供銀行業者遵循。

(二) 強化國際合作

APG 第三次相互評鑑重點之一在於國際合作，其原因係跨境交易本即具有洗錢資恐高風險之本質，無論在犯罪查緝、監理合作或銀行之洗錢防制作業均如此。金融監督管理委員會（下稱金管會）一向致力於國際金融監理合作，包含書面協議（MOUs、換文或協定書）、正式/

非正式會議或會談（監理官會議、雙邊對談和電話會議）等，據以交換洗錢防制之相關資訊，並掌握國際金融監理趨勢及獲取其他國家監理經驗。

本研討會所引用 AUSTRAC 發布之東南亞及澳洲資恐風險評估區域研究報告，係由東南亞國家每年輪流舉辦會議，各國在會議中分享實務經驗並提供執法資料，對跨國合作有相當大的助益，可惜我國未能參與相關會議。其次，自 Antigua-Columbia 洗錢案可知，以色列政府未盡武器販運之管制查證責任，以及巴拿馬政府拒絕提供銀行帳戶資料，均係本案最終無法確認犯罪事實之原因。本研討會所提及通匯銀行、跨境電匯等均因涉及跨境而屬於高風險業務；另有關境外法人或法律協議、涉及跨境之行動支付及虛擬貨幣等議題，銀行在辦理客戶審查時均面臨相當程度的困難。以上均顯示國際合作之必要性。

（三）檢視裁罰案件之監理政策

本研討會引用之澳洲聯邦銀行裁罰案，其所列違規情節，係考量新商品推出前未分析洗錢資恐風險、未採取控制措施以抵減風險、在長達 3 年期間內未監控帳戶交易、未申報大額交易及可疑交易，致使銀行成為犯罪者易於利用之弱點，對公眾安全造成重大危害，爰以高達澳幣 7 億元之罰鍰，促使銀行改善。

為強化洗錢防制，金管會近年來之監理作為，包括大幅修正法令、要求銀行改善內部作業、辦理產業別風險評估、推廣宣導及教育訓練、舉辦模擬評鑑等。此外並加重裁罰力度，裁罰家數及額度均顯著增加。經檢視裁罰案件之違規事由，其態樣多屬未申報大額交易或可疑交易，裁罰額度依現行法律規定上限為新臺幣 1 千萬元。

為發揮金融監理效能，達到嚇阻違法之效，金管會參考德國、日本立法例及我國銀行規模，全面檢討罰則章之罰鍰上限，對於銀行違規情

節重大者,原條文最高罰度為新臺幣 1 千萬元者調高 5 倍至 5 千萬元。
未來若通過立法，並在執行時考量增加相應於風險之違規態樣，對於
洗錢防制及打擊資恐必將更有助益。