

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)

參加法國央行舉辦之「後台作業研討會」 心得報告

服務機關：中央銀行

姓名職稱：李禹彥辦事員

出國地點：法國巴黎

出國期間：105 年 12 月 10 日

105 年 12 月 18 日

報告日期：106 年 3 月 3 日

目錄

壹、前言.....	1
貳、BdF 後台作業部門.....	2
一、BdF 後台作業部門之組織架構.....	2
二、後台作業部門之業務內容.....	3
三、市場操作組之後台作業運作實務.....	3
參、作業風險之管理.....	9
一、風險管理架構.....	10
二、作業風險管理方法.....	13
肆、資訊安全概述.....	16
一、資訊安全的基本概念.....	16
二、常見的資安攻擊入侵方式.....	18
三、資安防護之方法.....	20
伍、心得與建議.....	22
參考資料.....	24

壹、前言

職奉派赴法國巴黎參加法國央行(Banque de France)於105年12月13日至12月16日舉辦之「後台作業研討會」(Back Office Operations Seminar)，本次研討會由法國中央銀行(Banque de France, 下稱 BdF)所屬國際銀行暨金融協會(International Banking and Finance Institute, IBFI)負責課程內容之規劃，邀請來自法國資深央行官員擔任講師。研討會內容主要包括近期外匯存底管理之趨勢、後台作業之定義與應用、交割操作流程、貨幣政策執行方式、作業風險管理、資訊科技相關議題。

參加本次研討會人員共 35 位，參與國家共計 26 國，除我國外，尚包括美國、阿爾及利亞、俄羅斯、摩洛哥、克羅埃西亞、巴基斯坦、菲律賓、西班牙、義大利、伊拉克、墨西哥、日本、南韓、印度尼西亞及印度等國。

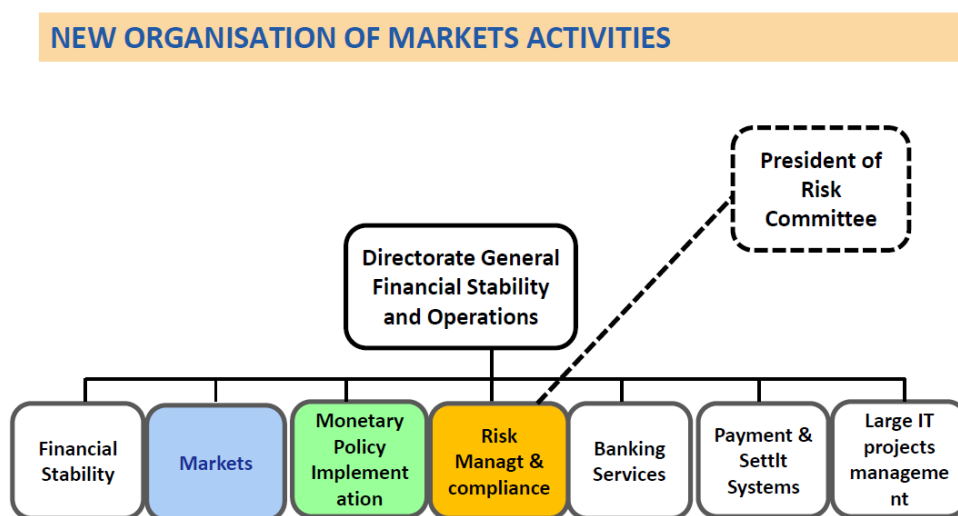
本報告共分為五部分，第一部分為前言；第二部分概述 BdF 後台作業部門；第三部分介紹作業風險之管理；第四部分概述資訊安全；第五部分心得與建議。

貳、 BdF 後台作業部門

一、 BdF 後台作業部門之組織架構

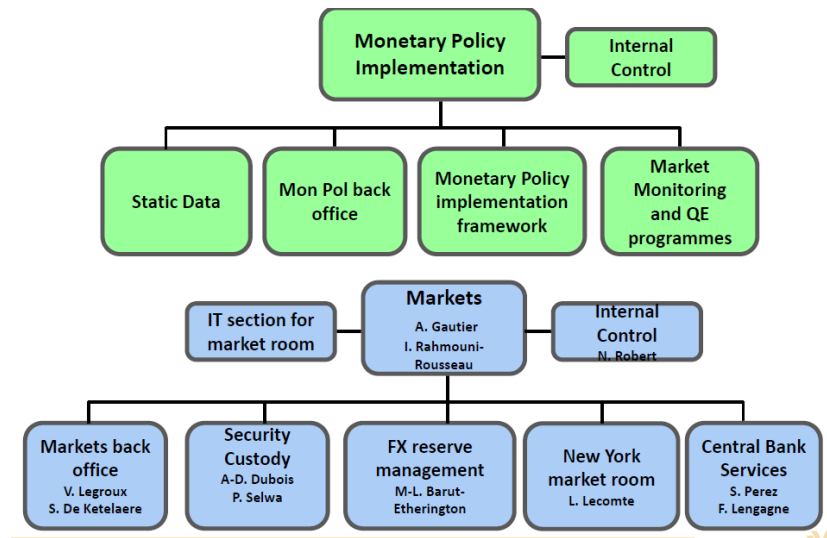
金融穩定操作局屬一級單位，除了執行 ECB 貨幣政策外，亦須管理 BdF 自有資產，並辦理國外機構委託投資；其下設有七組，分別為金融穩定組、市場操作組、貨幣政策執行組、風險管理及法遵組、銀行業務組、支付清算系統組、資訊管理組(圖 1)，各組分工合作，確保交易順利完成。

圖 1 BdF 所屬金融穩定操作局組織架構



BdF 之後台作業部門主要為貨幣政策清算科(Mon Pol back office)及市場操作清算科(Markets back office)，此兩科分別隸屬於貨幣政策執行組及市場操作組(圖 2)。

圖 2 貨幣政策執行組及市場操作組組織架構



二、後台作業部門之業務內容

後台作業部門主要負責貨幣政策執行與市場操作組所作交易之後台交割作業，除確保交易款券確實交割，且須盡快回覆來自交易對手與客戶之需求，其業務內容包括：

- (一) 確認交易之發送、接收與核對；
- (二) 發送現金支付與收受之交割指令；
- (三) 確認帳戶撥付款及帳務處理；
- (四) 持續監督操作程序；
- (五) 解決突發事件與執行內控和改善計劃。

三、市場操作組之後台作業運作實務

BdF 市場操作組主要係提供外匯存底管理的全方位服務，包括外匯交易、現金存款、借券交易及黃金等服務。服務對象遍及美洲、亞洲、非洲及歐洲等 120 個以上之各種機構與組織，包括各國央行、政府機構、國際組織及國際金融機構。

市場操作組所承作交易之後台交割作業主要由市場操作清算科(Markets back office)負責，詳細後台作業運作實務，茲分別說明如下：

(一)外匯交易

市場操作組所執行之外匯交易總類包括即期外匯、遠期外匯、換匯交易。當前台完成交易後，須在 15 分鐘內完成交易資料驗證，並更新外匯交易資訊。緊接著中台(作業風險組)確認交易對手的交易金額是否符合交易限額並更新相關資料，最後移由後台(市場操作清算科)進行以下作業完成交割：

1. 確認交易內容與授權權限相符，且交易對象為合格之交易對手。
2. 核對前台之成交單，並發送 SWIFT 電文請交易對手再行確認。

3. 發送交割指示電文執行款項收付。

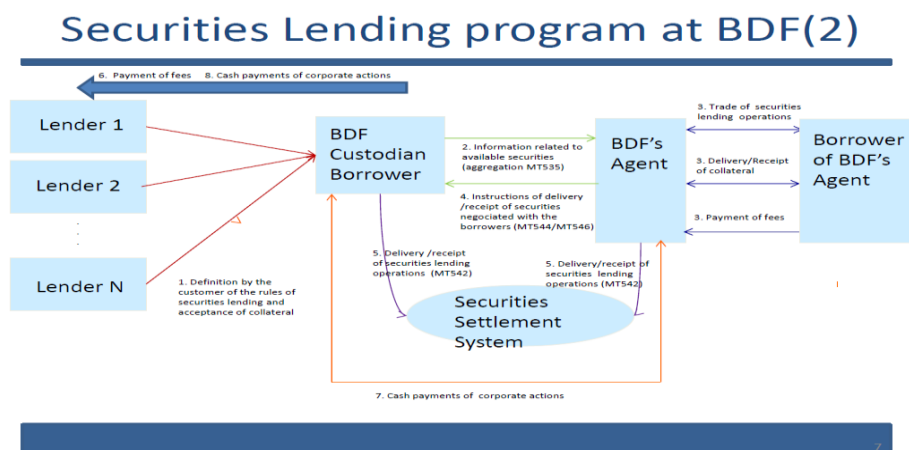
4. 完成記帳等帳務程序。

(二)借券交易(Securities Lending program)

BdF 為增加其所保管歐元計價的國庫券及公債之流動性及收益率，特別提供客製化的借券服務。

BdF 的借券服務著重在風險管理及交易彈性。市場上有借券需求的交易對手，直接向法國央行借入債券，透過央行的借券服務，借券人不知道真正的債券所有人，交易對手風險由法國央行承擔。債券所有人透過從法國央行的借券服務中得到利益。法國央行會依據市場狀況及債券的性質，支付部分借券收益給債券所有人。借券交易流程詳如說明(圖 3)：

圖 3 BdF 借券交易流程



1. 借券業務由 BdF 個別與債券所有人簽約，所有借券條件及比例都明訂在合約中。
2. BdF 之債券保管機構發送 MT 535 電文至 BdF 之代理行，提供相關債券資訊(例如 CUSIP、利率、到期日。)
3. BdF 代理行在市場上與有借券需求之交易對手進行交易，交易完成後收取擔保品及借券費用。
4. BdF 代理行發送 MT 544 電文通知 BdF 債券保管機構相關付券指示。
5. BdF 債券保管機構及借券行分別發送 MT542 電文至證券清算交割系統 (Securities Settlement System)，執行債券轉移交割作業。
6. BdF 債券保管機構從代理行收取借券費用後，定期轉交至債券所有人。

(三)黃金交易市場

BdF 為世界第 5 大黃金準備持有國，為了有效管理自己所持有且缺乏流動性之黃金，BdF 提供黃

金相關業務，包括實體與無實體之黃金存款、即期交易、遠期交易及保管等。

黃金最主要的交易市場為倫敦黃金交易所，其交割清算業務運作最主要由倫敦貴金屬結算公司 (London Precious Metal Clearing Limited ,LPMCL) 負責。

LPMCL 為非營利組織，主要由 HSBC、ICBC Standard Bank、JPMorgan、Scotiabank、UBS 這五家會員銀行來執行黃金之交割清算作業。黃金交割運作詳如說明：

1. AURUM 結算平台(圖 4)：

(1)黃金交割清算主要是透過 LPMCL 管理之 AURUM 電子結算平台來運作，LPMCL 清算會員幫其客戶在此平台開立帳戶進行後續交割業務。

(2)平台主要以美元進行交割，交割日期為 T+2，交易銀行須拍發 SWIFT 通知代理清算行及交易對手，通知黃金相關交割指示。

(3)在交割日當天，此平台會在倫敦下午四點以前完成所有交割作業。

圖 4 AURUM 結算平台



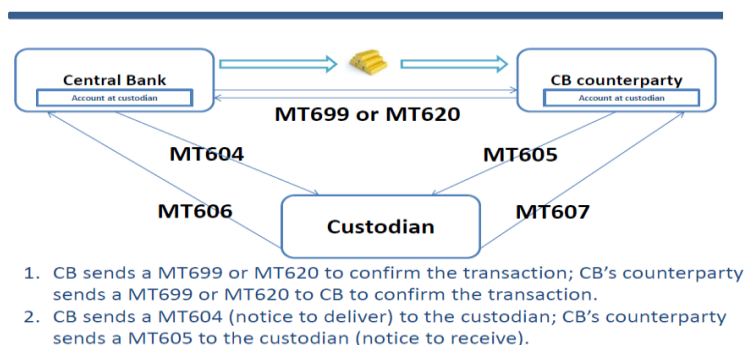
2. 後台 SWIFT 交割作業流程(圖 5):以黃金保管為例。

(1)交易完成後，CB 拍發 MT620 至交易對手，
確認交易的相關資訊。

(2)CB 拍發 MT604 通知保管機構，相關移轉黃金之指令；保管機構則拍發 MT606 回報移轉結果。

(3)CB 之交易對手拍發 MT605 通知保管機構接收來自 CB 之黃金；保管機構則拍發 MT607 回報接收結果。

圖 5 黃金保管交割流程



參、作業風險之管理

傳統上，外匯資產風險管理，主要是針對信用風險及市場風險所做之管理，作業風險（Operational Risk）管理一直居於次要地位。近年來，電腦自動化作業普及，加上網路金融的蓬勃發展，金融商品複雜度提高，導致三項風險之間的連結更加緊密。凡此種種變革，均促使各國中央銀行必須重視作業風險管理。不當之作業風險管理，不僅可能使中央銀行蒙受金錢上之損失，亦可能危及聲譽，使社會大眾對央行喪失信心，因此絕不可輕忽其重要性。

根據 BIS 之定義，作業風險係指因內部作業、人員及系統之不當或失誤，或因外部事件所造成損失之風險。因此，人為因素（如員工檢查交易不確實或缺乏專業知識）、作業程序錯誤（如處理或輸入錯誤）、資訊科技失靈以及

其他外部因素（恐怖攻擊、詐欺等）皆可能導致無法達成機構所設立之目標。

BdF 為減少作業風險之發生，希望透過嚴謹的風控機制，來確保後台交割作業之順利，其管理架構與方式說明如下：

一、風險管理架構

BdF 作業風險由高層管理人員組成之管理委員會 (Management Committee) 與風險委員會負責風險監控 (圖 6)，監控架構共分為三個層次，第一層為金融穩定操作局之內控機制，第二層為內部稽核單位，第三層為外部審查。

圖 6BdF 風險監控架構圖



金融穩定操作局第一層次之內控機制分為三級，分別說明如下：

(一) 第一級之內控

第一級為各科內之內控，各科主管除須落實其職責範圍之內控程序外，亦須督促科內同仁確實記錄風險事故，以後台交割作業為例，其職責說明如下：

1. 作業人員:科內作業人員先與前台確實核對交易資料，其後包括發送付款前交易資料之確認發送付款、確認交易對手帳戶收付款等相關細節之驗證，均由不同人員分工進行，嚴守兩人把關之四眼原則(Four-eyes Principle)。
2. 各科主管:對作業程序進行全日監督，以作業零風險為目標。督導範圍包含風險事故之發生與後續聯繫、交易待確認狀態與原因、檢查款戶實際收付情況，並即時監控異常狀況。

(二) 第二級之內控

第二級為各組之內控，主要由各組內控科負責。
主要業務及職責說明如下：

1. 監督各科之各項程序確實執行且定期更新驗證記錄，尋找各科作業缺失並施予嚴密監測。
2. 協助各科辨識風險等級，並根據作業風險狀況制定妥適之內控計劃，以防止風險發生。
3. 確保風險事故完整記錄，確認事故原因並追跡後續處理，防止類似事件再次發生。
4. 定期審查所有查核建議，並將後續處理情形報告主管及稽核單位。

(三)第三級之內控

第三級之執行者為風險管理者（Risk Managers），目前風險管理者主要由跨部門之風險管理組擔任，其職責說明如下：

1. 管理作業風險：參與各業務的風險圖像繪製過程、出席風險指導委員會、向風險委員會和管理委員會陳報風控狀況，以及協助其他單位制定改善計畫。
2. 辨識風險：定期與業務單位內之內控人員例行性會商、舉辦相關訓練計畫與資訊分享。

3. 強化風控機制：協調作業程序之訂定、監控作業程序之執行，並提供修正建議和預防措施予高層管理人員，以完善風控機制。

二、作業風險管理方法

「作業風險管理」是指風險的預期、認知與評估以及因此而產生的某種作為，企圖減少潛在之損失至可接受程度。作業風險管理流程可分為風險辨識、風險評估、風險衡量、風險控制、風險檢討。風險管理流程為一動態循環的過程，透過此循環的過程以確保機構具備完善的作業風險管理。茲分別說明如下：

(一)風險辨識

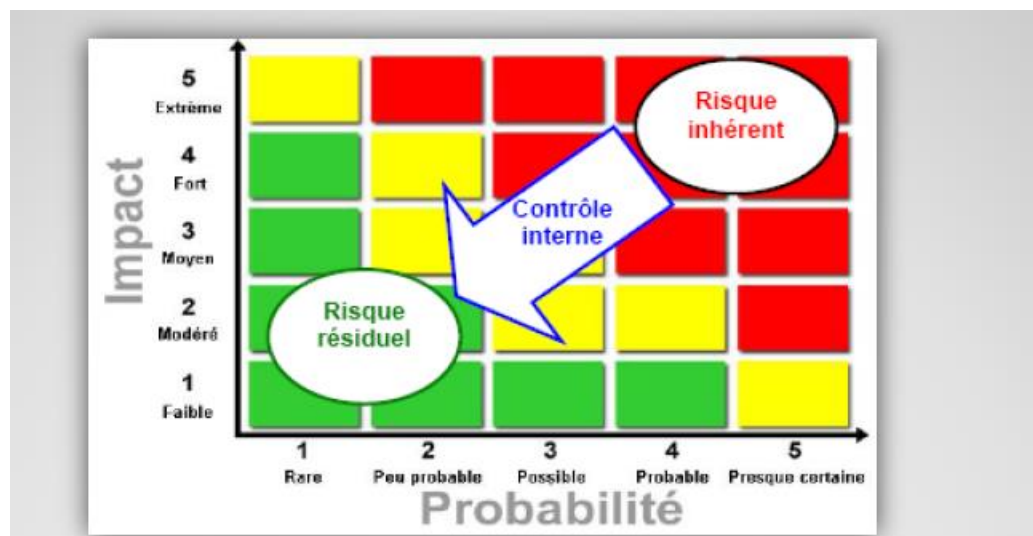
風險辨識為風險管理流程的第一步，其目的在於有系統地辨識風險事件，並排列出風險順序，以便對風險作全面性的定位及歸類，並提供進一步風險分析的資訊。風險辨識應從風險因子開始分析，當事件發生時，必須詳細記錄損失事件，例如，事件發生時間、發生地點及發生何種損失等資訊。接著將上述記錄的損失事件，分別考量其

如何發生及為什麼會發生的原因，以便後續進一步分析及對應方式。

(二)風險評估及衡量

在辨識出風險事件後，便對風險事故進行評估的流程。風險評估，須在未採取任何風險控制措施之前，先定義各種風險事故之屬性，並依據不同事故發生之可能性及影響程度給予權數，繪製風險圖像(圖 7)。最後透過風險地圖，將各作業風險加以分類及定位成四級：嚴重、顯著、中等、輕微，危害程度在「顯著」以上之風險事故，應陳報給高層管理人員。

圖 7 風險圖像



(三) 風險控制

風險控制之主要用意在於「減少損失」，其策略係指專門設計用來使事故之損失頻率或幅度趨小的風險管理策略，以及使損失更可預測的風險管理策略。主要風險控制策略包括：

1. 風險趨避：風險趨避為完全消除任何損失的可能性；其作法為放棄任何會遭致損失風險的活動。
2. 損失預防：損失預防是指事先採取措施，消除危險因素以減少損失發生之頻率。
3. 損失抑制：損失抑制是指風險事故發生前後，採取措施，來減少損失之範圍或程度。
4. 損失風險標的之隔離：此是一種不會使事故波及全體的策略，簡言之，預先把機構的活動與資源予以有計畫的安排，使單一事件不會同時波及全體或造成整體的損失。

(四) 風險檢討

風險管理之最後責任，即應檢討以上各步驟進行之是否確實，成效如何，是否能達成風險管理之

目標。如採用損失防阻與抑減計劃，應注意其是否妥善實施。如屬風險趨避，則應辨明有無任何依照風險管理決策所不應接受之風險。

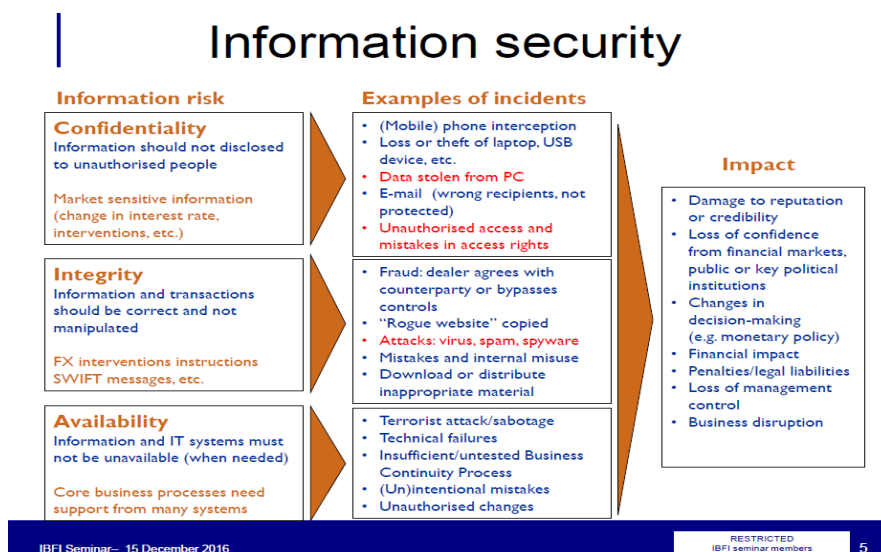
肆、 資訊安全概述

近年來，在數位金融、雲端化、物聯網科技快速發展下，網路金融犯罪快速增長。隨著諸多國際重大資安事件爆發，例如孟加拉央行遭盜轉、第一銀行 ATM 遭盜領等等案件，使機構名譽受到重大影響，因此如何有效控管資訊安全衍生之風險，儼然已成全球關注的焦點。

一、 資訊安全的基本概念

資 訊 安 全 有 三 要 素 ， 分 別 是 機 密 性 (Confidentiality)、完整性 (Integrity)、與可用性 (Availability)，這三項要素稱為資訊安全三原則，簡稱 CIA(圖 8)。能遵守這些主要原則就能掌握資訊安全的要領，分別說明如下：

圖 8 資安三要素



- (一)機密性:為維護資料在傳輸、儲存、與處理狀態時，不被非授權人員之存取、使用、或竄改。許多攻擊型態都是以破壞資訊的機密性為主，例如：網路抓取封包、偷取密碼檔案、利用監視軟體、網路掃描等，都是破壞機密性的攻擊行為。因此央行在敏感的市場資訊(利率變動決策)須非常注重機密性。
- (二)完整性:指確保維持資料原來的狀態，只允許有權限的使用者可以修改資料內容。在資料內部與外部均需維持資料的一致性，例如，傳輸資料時，在傳輸中的資料與接收、儲存的資料，均需要保持一致而且是可以確認的。

(三)可用性:為了確保資訊與系統能夠持續營運、正常使用，當合法使用者要求使用資訊系統時，例如，電子郵件、應用系統等，使用者均可以在適當的時間內獲得回應，並獲得所需服務。因此若有天然災害發生導致央行無法正常運作時，央行須有備援中心來維持正常之運作。

二、常見的資安攻擊入侵方式

網路攻擊者主要係經由資訊蒐集、目標掃描、弱點刺探等過程，最終取得系統控制權限，侵入系統，並消滅相關軌跡證據，以維持其系統控制權。以下介紹常見的攻擊入侵方式。

(一)病毒感染:電腦病毒係程式透過網路、檔案傳輸等管道，將程式本身加以複製及傳播，並藉著程式中的指令導致電腦或周邊失靈，甚至於破壞程式及資料等；當病毒到了一個特定的日期，或是使用者做了某一些特殊的動作，病毒便開始發作。有些病毒只做些惡作劇，妨害使用者正常地使用電腦，並不會造成資料的損毀。但是有些病毒卻專門破壞資料，甚至格式化硬碟。

(二)分散式阻斷服務攻擊(Distributed Denial of Service ;

DDOS):主要利用分散於不同地方的多部電腦主機，發送大量偽造來源地址的封包，癱瘓受害者所在的網路電腦主機伺服器，使得正常的接通率降到 1% 以下，導致無法服務。

(三)進階持續性滲透威脅(Advanced Persistent Threat ;

APT):攻擊者往往都是具相當規模且有組織系統的駭客集團，針對特定的攻擊對象設計專屬的攻擊策略，透過長時間且持續性的潛伏及監控，竊取其所需要的特定國家安全或商業機密等資訊。APT 事件可依序區分為「攻擊、控制、擴散」三個階段。

1. 在「攻擊」階段，駭客發動社交工程電子郵件、魚叉式網路釣魚攻擊，意圖滲透進入目標對象組織。
2. 「控制」階段，受駭電腦被植入後門及木馬程式，藉以建立與駭客的通訊管道。
3. 「活動與擴散」階段，駭客可在內網進行密碼、資料的竊取，甚至採取破壞行動。

三、資安防護之方法

(一)多層次縱深防禦架構:面對千變萬化的網路攻擊

與入侵方式，惟有建構多重防禦機制才能有效攔阻。

此架構是以管理、實體、技術三個控制層面來達成安全管理的目標，組織內部必須訂定管理政策與標準作業程序，強化員工資安意識，再建構網路、周邊、主機、應用程式及資料之各種分層防禦技術，以保護組織之重要資產(圖 9)。

圖 9 多層次縱深防禦架構



(二)異常行為分析:異常行為是指任何一種不尋常、不

正常或不屬於這個區塊之活動狀態。我們可以透過網路流量模式檢查位於特定主機的狀態，以識別自動安全監控工具錯過之惡意行為。網路攻擊者通常

在受損網路中形成一個網路集結區，他們會在這裡對其他主機發動攻擊並可能將偷來之資料存放在這區。通常這些資料會被壓縮、模糊化甚至加密使其看不出原始樣貌。因此我們可以用異常分析來辨識此不尋常之網路集結區並阻止機密資料外洩。

(三)區塊鏈技術應用：區塊鏈技術是一種去中心化的分散式帳簿系統，它通過網路中多個節點共同參與資料運算和記錄，能保證資料傳送儲存過程中的穩定性、完整性。且只有收受兩端才具有解密的「鑰匙」，因此能確保安全性。

傳統集中式管理架構因資料集中儲存，一旦遭受攻擊，就會出現全部被竄改的風險。另外，其僅就特定時點之餘額進行維護，當過去部分資料被竄改時，若無適當的確認機制，將難以發現；相對於此，區塊鏈之分散式帳本架構，非但新舊資料難以竄改外，亦可從外部確認資料是否被竄改，因此在資安防護上較為穩固。

伍、心得與建議

一、後台交割作業人員之專業能力實屬重要：

一項交易即便前台交易順利，若後台作業無法順利完成交割，將嚴重影響機構之聲譽。因此後台交割作業人員應嚴謹遵守內控機制，將作業風險降至最低；並且隨時學習新的專業知識，以因應日新月異之金融環境。

二、建議持續選派同仁參加國際研討會：

本次研討會課程內容偏重實務，授課講師主要為 BdF 部門主管，學員可藉課程瞭解 BdF 後台作業之實際運作流程，並透過互動課程向授課講師請益；未來本行可持續選派不同階層之同仁參加此類課程，除可與不同央行人員交換心得、了解各國央行實際操作流程，對於擴展同仁國際視野、提升專業能力、建立聯繫管道，甚有幫助。

三、可強化跨部門資安事件應變機制：

近年來資安事件頻傳，引起各界對資訊安全之重視。資訊安全非僅技術層面問題，此牽扯到跨部門間的合作，強化跨部門資安事件應變機制，如建立跨部

門資安事件通報程序及應變計畫，使事件發生時，各同仁能依其職務有效的進行應變處理及通報程序；定期進行跨部門資安事件防駭演練，以確保同仁皆有一致性作法及步驟。

參考資料

1. Imène Rahmouni-Rousseau(2016), “ RECENT DEVELOPMENTS IN THE ORGANISATION AND GOVERNANCE OF THE “MARKETS” FUNCTION IN BANQUE DE FRANCE”
2. Imène Rahmouni-Rousseau(2016), “Trends in reserve management”
3. Stéphanie De etelaere(2016), “Back office of market operations”
4. Vincent LEGROUX(2016), “Securities lending”
5. Vincent LEGROUX(2016), “Operations on gold”
6. Fabrice GASCON(2016), “Cyber-risk issues in a Central Bank”
7. Valérie BOUR(2016), “Information systems in back offices”
8. Mohamed BOUTAYBI(2016), “The operational risk management and its governance”
9. 陳怡娟(2016),「參加法央後台作業課程」,中央銀行公務出國報告。
10. 陳佑任(2016),「強化支付清算系統之資訊安全」,中央銀行公務出國報告。
11. 朱榮玲(2015),「法國央行外匯準備研討會」,中央銀行公務出國報告。
12. 賴怡伶、莊鯉銓(2015),「參加 SWIFT 國際金融年會」,中央銀行公務出國報告。
13. 林正弘(2016),「參加 FED 作業風險管理與內部稽核」,中央銀行公務出國報告。
14. 「金融科技發展策略白皮書」,金融監督管理委員會(2016)。
15. BdF 網站 <https://www.banque-france.fr/en/home.html>