出國報告（出國類別：實習）

臺灣銀行上海分行資訊業務培訓心得

服務機關：臺灣銀行股份有限公司資訊處
姓名職稱：蔡欣蓓/高級辦事員
派赴國家：中國大陸(上海)
出國期間：113 年 10 月 21 日至 12 月 13 日
報告日期：114 年 3 月 5 日

摘要

臺灣銀行上海分行於 101 年 7 月 10 日正式成立，於上海分行成立初始，大陸分行使用之相關系統即落地建置於上海。為了讓總行資訊處人員更加深入瞭解大陸分行當地資訊系統相關業務的實際作業與數據中心相關系統維運之實務經驗，本行資訊處指派職蔡欣蓓至上海分行接受培訓任務。

職於 113 年 10 月 21 日至 113 年 12 月 13 日赴上海分行進行大陸資訊系統維運作業培訓，培訓期間承蒙上海分行行長、副經理、各部門主管及同仁的指導，職依據培訓期間分為前、後二期，前期為配合上海分行將導入資訊服務管理(ITSM)制度著手進行規章修訂作業，規章修訂期間經過多次與總行資訊處開會討論，透由大陸分行信息通報作業流程中了解到程式換版的運作過程；後期為配合總行資訊單位規劃導入零信任架構相關作業，參與零信任架構工作小組相關會議及構建企業零信任解決方案研討會，加深了解零信任對公司的重要性。另外，透過到上海分行實習的機會，前往上海萬國機房進行磁帶備份作業，得以體驗數據中心系統維運相關作業，並藉由主動詢問、實際參與中學習到維持資訊系統穩定運作的寶貴經驗。

實習過程在主管和同事們的細心關懷和指導協助下，可以在短時間內快速了解上海分行工作內容，並且熟悉本行業務的作業流程，現在能逐步掌握所分配到的專案、跨業務部門間的溝通協調、日常維運監控與處理，以及分行日常業務營運及維護作業。

目　　次

壹、目的

此次奉派赴上海分行進行實習，主要培訓目的為了解大陸當地資訊業務運作流程及學習數據中心相關系統維運之實務經驗。經由本次至上海分行進行近兩個月實習過程中，實際參與系統換版上線作業流程，可以更加深入了解各項大陸分行日常資訊作業流程及數據中心系統維運作業。並且提升對於分行各業務部門日常作業及操作系統的熟悉度，得以協助資訊處同仁在處理及溝通協調大陸分行維護相關事務，讓系統專案的推動上更加順遂。

貳、過程

一、赴上海實習計畫說明

依據總行人資處 113 年 10 月 1 日銀人資乙字第 11200054491 號函之「業務培訓計畫」，職蔡欣蓓奉派赴上海分行實習計畫如下：

(一)時程：113 年 10 月 21 日至 113 年 12 月 13 日。

(二)培訓項目：1.大陸分行數據中心維運管理相關業務實習

大陸分行數據中心資訊系統維護管理，含當地機房系統設備管理、資料庫管理、網路管理、資訊安全等作業項目 。

2.大陸分行數據中心系統維運相關業務

各類資訊系統業務需求梳理、業務系統問題處理以及專案採購建置管理等作業項目 。

二、培訓業務概述

(一)大陸分行數據中心信息維運作業管理手冊修訂相關業務

1.資訊通報作業流程

為符合實際運作流程，召集上海分行信息維運小組及總行資訊單位進行多次線上開會討論，需求者透過資訊作業通報單提出事件、問題或服務請求，資訊人員配合作業流程進行系統程式開發、測試、上版……等作業，除了遵照「大陸分行數據中心信息維運作業事件、問題及服務請求管理作業手冊」、「大陸分行數據中心信息維運作業應用系統變更管理作業手冊」及「大陸分行數據中心信息維運作業應用系統開發管理作業手冊」訂定的規範外，發現與現行實務作業流程稍有不同，例如：原總行資訊處程式設計二科負責大陸相關業務已調整改為程式設計七科負責處理，經由會議討論修正規範內容及附件表單，以符合現行作業。

2.大陸分行數據中心信息維運作業管理手冊

為強化大陸分行數據中心相關安全規範制定管理手冊總共 11 本，配合總行 ITSM 相關規範及主管機關規定修改規章內容，例如：數據安全及保密管理作業手冊中，第十三條密碼管理之密碼長度，由原先的至少 8 個字符調整為至少 12 個字符。另外，為精簡規章內容，將各手冊中的數據中心申請單彙整至 CNIT1000 大陸分行數據中心信息維運作業規範之附件。

(二)大陸分行數據中心系統維運相關業務

1.例行性業務

為維護系統安全性與維持系統穩定運作，配合上海分行信息維運小組維運作業時程，實際參與每月例行之作業，例如：

(1)113 年 10 月 25 日參與 10 月份 windows update 前置派送作業。先前因工作權責及業務內容有所不同，以往僅負責執行系統更新作業。藉由維運小組同仁的帶領下，了解到派送更新前的所有作業流程及 Windows Server Update Services(WSUS)部署設定作業，並於 10 月 26 日完成伺服器更新作業。

(2)與維運小組同仁於 113 年 10 月 28 日一同前往萬國機房，著手進行磁帶備份及機房巡檢作業。除了親自體驗磁帶抽換的作業過程(包含操作指令)，也看到上海萬國數據中心管理規模，受益良多。

2. 大陸網路銀行系統分散式阻斷服務攻擊(DDoS)演練

對於分散式阻斷服務攻擊日益頻繁，將導致系統面臨無法正常運作之風險，為確保大陸網路銀行系統發生 DDoS 攻擊時，能立即應變處理，於 113 年 11 月 30 日參與「分散式阻斷服務攻擊（DDoS）演練」，確保防護作業能夠順適進行，本次演練共 3 種不同情境。

此次 DDoS 演練順利完成並於 113 年 12 月 9 日召開 113 年網銀 DDoS 演練檢討會議，能夠參與 DDoS 演練實屬難得經驗，透過定期演練來確保 IT 人員的應變能力以及測試系統面對 DDoS 攻擊時，對外服務之防護力是否充足。另外，規劃明年度執行防護演練時評估增加其他演練情境，並參考總行建議使用非泛洪攻擊、其他協議漏洞攻擊等方式。

(三)零信任相關業務

零信任的核心是保護系統及資料安全，任何身分、任何人還是機器存取應用程式和系統，對任何的訪問請求都抱持著永不信任的原則下，透過嚴格的身分驗證和持續監控，確保每次存取請求都經過充分的安全檢查，來降低資料外洩和駭客攻擊的風險。公司為了提升資安的防護能力，降低資安風險，著手進行零信任導入作業來確保系統安全與穩定。另外，於 113 年 12 月 3 日參與構建企業零信任解決方案研討會。解決方案的核心理念在於「永不信任，始終驗證」，確保每一次訪問請求都經過身分驗證、授權和監控，以降低內部與外部威脅的風險。

(四)IBM QRadar 教育訓練課程

公司本身除了維持基礎運作、保護客戶身分並避免業務中斷，不能只是依賴監

控日誌和網路流量數據，透過 QRadar 提供即時資訊及監視、警示及攻擊，以及對網路威脅的回應，使用該資料來管理網路安全。為增進資訊安全相關知識與技能，實習期間以視訊方式參與總行安排之 QRadar 初階、進階及系統維護教育訓練課程。

IBM QRadar 提供即時收集、處理、聚集及儲存網路資料，並透過即時資訊及監視、警示及攻擊，以及對網路威脅的回應，來確保網路安全。將連結所有資料來源，透由 IBM QRadar SIEM 可以自動追蹤日誌和網路串流來找出真正威脅，並在攻擊傳播時專注於建立警報，縮短事件回應時間，降低端點取證調查和處理誤報花費的時間。藉由 IBM QRadar SIEM 增強網路流量和事件日誌資料的擷取能力，更快速偵測可疑活動，提高資安人員調查可疑活動的能力，降低重大安全漏洞的風險和成本。

參、心得及建議

職於 109 年進入臺灣銀行資訊處擔任大陸地區資訊系統維運人員一職，期間因疫情影響而延宕實習計畫，至 112 年疫情狀況緩解恢復辦理實習計畫，感謝長官給予機會派赴上海分行實習近兩個月，在上海分行進行實習，是個非常寶貴與難忘的經歷及經驗。在實習培訓期間，對於資訊系統維運與資訊安全有更深的理解，從伺服器管理、存取控管到網路資訊安全都有實際參與經驗，包括：每月部署伺服器更新作業及磁帶備份作業、大陸網路銀行系統分散式阻斷服務攻擊(DDoS)演練、系統故障及資料復原演練行前作業，經由上海分行維運小組同仁們的引領下，對於資訊系統維運管理有了更多的認識，獲益良多。

現今網際網路日益龐大且更加複雜，防範與日俱增的資安惡意攻擊是一大挑戰，加上大陸地區監管機關法令規範更新非常快速，上海分行合規部門收到監管單位所發布的相關法令公文，為符合監管中心之要求，信息部門配合相關法令進行資訊系統功能、流程之調整。因此，建議可以持續進行大陸分行人員培訓計畫，讓資訊處維運人員可以輪流參與熟悉大陸分行業務的迅速變化，有助於強化資訊系統的

維護及安全性。

在這段實習期間中配合協助修訂大陸分行數據中心信息維運作業規範及管理作業手冊，了解到資訊業務流程及數據中心管理規範，涵蓋範圍包含系統維運、機房及門禁管理、網路安全、媒體存取管理，透過業務的熟悉及參與，更加深全面化資訊業務的相關知識，深知自己還有許多要學習的地方，期許未來強化自身綜合素質的修養，不斷提高自身工作能力，圓滿地完成交付之各項任務。

肆、參考資料

IBM QRadar 概觀