出國報告（出國類別：其他）

# 參加「SEACEN Course on Operational Risk Management and Business Continuity」心得報告

服務機關：中央銀行
姓名職稱：林淑貞　副科長
派赴國家：泰國
出國期間：100 年 5 月 17 日至 5 月 25 日
報告日期：100 年 8 月 8 日

目　　次

## 一、前言

本次研習主要集中於作業風險管理（Operational Risk Management，ORM）與業務連續性計畫（Business Continuity Program，BCP）兩項主題，學員分別來自汶萊、柬埔寨、大陸、香港、印度、印尼、馬來西亞、尼泊爾、新幾內亞、菲律賓、斯里蘭卡、台灣、泰國之央行[1]，共 45 人，以內部稽核及風險管理二部門代表爲最多。

主講者分別爲來自馬來西亞、西班牙、英國及泰國等央行相關部門主管，其中更邀請到泰國央行前總裁 Dr. Tarisa Watanagase 女士講授央行的聲譽風險及政策風險。由於泰國去年剛發生紅衫軍暴動事件，泰國央行所在地也被包圍。爲穩定金融秩序，員工被通知照常上班，惟地點改在備援處所或自己家裡，利用 e-mail 互通訊息，而當時的央行總裁即爲 Dr. Watanagase，據稱，當時她必須不斷地打電話，讓溝通管道暢通無阻。事後證明泰國央行的業務連續性計畫，確實發揮了「營運不中斷」的功能。

或許因爲近年來天災人禍頻傳，更凸顯作業風險管理與業務連續性計畫的重要性。SEACEN 訓練中心爲落實研習功效，除要求學員於上課之初接受一能力測驗，上課結束時又再接受相同測驗，藉以測試學員對於整體課程的理解情形，還請各國學員根據所學，上台發表未來的行動計畫（Action Planning），陳述該國的作業風險管理及業務連續性計畫，可能遭遇的挑戰及應改進之處，足見 SEACEN 對於本次上課的重視。

以下擬就企業風險管理（Enterprise Risk Management，ERM）、作業風險管理及業務持續性管理（Business Continuity Management，BCM）等三項提出心得報告，作爲分享。

## 二、企業風險管理

[1] 泰國另有存款保險局代表 1 人參加。

## （一）概述

2004 年 9 月，美國國會 COSO 委員會（Committee of Sponsoring Organizations of the Treadway Commission）繼 1992 年發布「內部控制－整合架構」[2]後，順應潮流，將內部稽核及企業風險管理作一整合，發布「企業風險管理－總體架構」，該架構結合沙氏法案[3]對於財務報告的要求，以內部控制架構的三大目標、五個構成要素爲基礎，擴增爲四大目標、八個構成要素及二個概念，亦即新增一個目標（策略性目標）、三個要素（目標設定、事項辨認、風險因應）、及二個概念（風險偏好、風險容忍度）。故其涵蓋內部控制，包含更強而有力的概念及管理工具，希冀成爲公司治理的强大支援。

根據 COSO 的定義，所謂企業風險管理，爲一遍及企業各層級的程序，由董事會、管理階層或其他員工共同促成，可適用於制定策略，藉以辨識可能對企業造成影響的潛在事項，並在企業之風險偏好範圍內，做好企業風險之管理，俾於目標的達成上提供合理的保證。

由此可知，企業風險管理爲：

◎ 一種持續於企業內部運作的程序。

◎ 涉及企業各階級的人員。

◎ 適用於制定策略上。

◎ 應用時遍及於企業各層級、各部門，並涵括從企業整體角度來看的各類風險。

◎ 用於辨認可能影響企業的潛在事項，並在企業之風險偏好範圍內，做好企業風險之管理。

◎ 能向管理階層及董事會提供合理的保證。

---

[2] 其中除定義內部控制外，還提出包括內部環境、風險評估、控制活動、資訊與溝通，以及監控等五項組成之內部控制架構。

[3] Enron 案爆發後，美國參眾兩院於 2002 年 7 月底通過「Sarbanes-Oxley Act of 2002」（簡稱沙氏法案），由布希總統簽署生效。該法案係美國自 1930 年代制訂證券交易法案以來，監督該國證券市場最重要的立法。沙氏法案又稱「企業改革法案」，重點在於：（1）強調公司及其主管人員的責任；（2）強化資訊之揭露；（3）提高對會計及審計之規範；（4）提高對違法行爲的處罰。

◎ 適合用於達成一到多個不同類別但有重疊性的目標。

妥善的企業風險管理，可以避免組織失序、避免高估整體風險、確保所有重大風險均已列入考慮、目標更明確而集中及提供更廣泛可行的風險解決對策，以達到消弭或減少風險的目標。

根據美國國際損失控制協會（International Loss Control Institute, ILCI）針對美國企業 18,000 件巨災統計，其中 70%未設置風險管理系統的企業，在遭遇巨災後 5 年內發生嚴重損失或結束營業，相對地，已建立風險管理系統者，在面臨損失事故時，則具有較大的競爭優勢。美國 911 恐怖攻擊事件，造成航空業的經營危機;臺灣 921 大地震，造成全球電腦配件價格的急漲。企業若風險管理能力不足，應變不及，將造成危機四伏，由此更突顯風險管理需求的必要性及急迫性。不過，科技的進展，需求的轉變，以及預防性的管理，都會牽動風險管理模式的更易，而全球化的發展與金融工具的推陳出新，也會增添風險管理的複雜度；風險管理必需因時、因地制宜，方得發揮其效用。

風險管理既然至關緊要，應使其成爲企業的一項自覺行爲，也就是說，將其融入企業的經營策略、決策及各項活動之中，深植於企業文化，並視其爲企業經營的要素之一。

## （二）COSO 的 ERM 的架構（framework）

此一架構可借如圖一之三維立方表示，分別爲：風險管理的目標、風險的組成要素（risk components）、企業單位組成。管理階層先預設目標，再憑藉風險組成要素及企業單位組成達成其目標，故可著眼大如企業風險管理整體，或僅著重小至某特定組成要素、企業單位等，來達成其風險管理之目的。若此一風險管理架構，已經具備並運作適當，則風險應可控制在所預設的風險偏好範圍內。

### 1．風險管理的目標

可分爲四類：

—策略性（Strategic）：爲較高層次（high-level goals）之目標，用以追

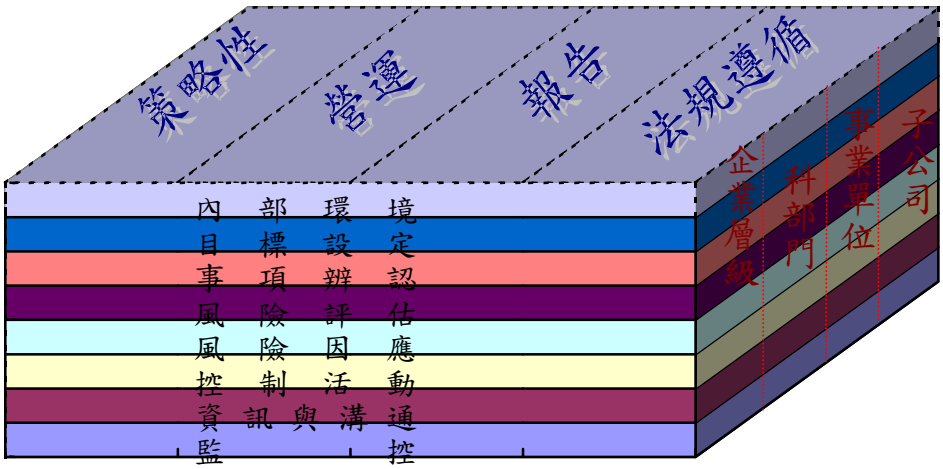
隨並支援企業的願景。

—營運（Operations）：追求資源之使用效率與效果。

—報告（Reporting）：完成可資信賴之財務報告。

—法規遵循（Compliance）：遵循相關法令規章。

圖一、ERM 的架構




## 2．風險的組成要素

企業風險管理包含以下 8 項要素，彼此相關，依管理階層經營企業之模式發展而來，與其管理過程互相結合：

—內部環境：指組織架構及文化、風險管理哲學與風險偏好、道德倫理與價值觀、營業處所環境等。

—目標設定：目標設定後，管理階層即可辨識影響目標達成的潛在事項。再經由企業風險管理，保證管理階層所設定目標能追隨及支持該企業的願景，並符合企業的風險偏好。

—事項辨認：企業應能辨識會影響目標的內部事項及外部事項，這些事項包括風險與機會，故管理階層亦應將機會列入策略或目標之流程中。

—風險評估：指分析風險，衡量其發生機率及影響，並據以決定管理方法。評估風險時，應考慮基本風險及殘餘（residual）風險。

—風險因應：指管理階層選擇風險的因應方式，如規避、承受、減輕及分擔等，並採取一些行動，以符合企業之風險容忍度及風險偏好。

—控制活動：指可用以保證風險因應能有效執行的政策與程序。

—資訊與溝通：指辨認、蒐集、傳輸資訊，以確保相關人員能夠履行職務。組織由上而下、由下而上、或橫向之間，均可溝通無礙。

—監控：指全面監控企業風險管理，必要時加以修正。

3．企業單位組成

可分爲子公司、事業單位、科部門、企業層級（entity-level）等四類。

## （三）企業風險管理的執行要件

首先，建立風險管理的共識。管理階層爲創造企業最大價值，在企業成長、報酬與風險間，取得最適平衡，依此原則訂定風險目標、政策、制度、及監督架構，並作明確地權責劃分。再經由教育、培訓，建立員工面臨風險的正確思維與處理態度，進而經由制度來規範員工的行爲。風險控管應置於一超然獨立的位階，以不擔負企業盈虧責任爲前提。

其次，建立一套共通的風險管理語言，因爲不同領域或部門的員工，對於風險的看法及接受度可能不一，故宜建置統一的風險分類及管理辭彙，以協調各部門的風險語言標準。再經由風險特性進行風險辨識，將其標準化、量化，進而整合不同類別風險，並分析風險曝露及風險承受度，作爲企業發展預防風險、控制策略、分配資本及衡量績效的重要指標。

## （四）智利中央銀行的經驗

中央銀行的風險，主要包括政策及決策風險、聲譽風險、作業風險及財務風險等。其中，作業風險包括因 IT 系統、人力資源、程序監控、營運持續、法規遵循、安全權限、計畫等因素所造成的風險；政策及決策風險爲衍生自制定貨幣政策、穩定金融等而來的風險；而財務風險則包含流動性風險、信用風險及市場風險等。這些風險環環相扣，例如，若政策及決策不當、作業失誤、或財務失靈，

都可能會危及中央銀行的名聲，造成聲譽風險。

智利中央銀行於 2003 年發生資訊外洩事件。此事件肇因於智利央行總裁 Carlos Massad 的私人秘書 Pamela Andrada，在 2 月時因涉及出售敏感性資訊給一家投資銀行而遭到逮捕，經過深入調查後，另發現有價值億元的存單從其他政府單位不翼而飛，之後也被移轉入這家投資銀行中。這起事件造成智利金融秩序大亂，Carlos Massad 事後向總統請辭，旋即獲准[4]。

因應上述事件，該國央行遂於 2004 年推動一可以監控其作業風險的計畫[5]，由管理及公司服務部門（Management & Corporate Services Division）擔任規劃、執行工作，該部門同時也肩負該行所有的行政及管理事務（包括人事方面）。此外，該行又新設立一風險管理單位（Risk Unit），負責提供部門主管相關的技術支援及預警措施。此二單位均隸屬於一新的管理單位，後者的成員雖均來自民間的專業人士，但是都不曾具備央行的實務經驗；也就是說，風險單位的員工都是風險方面的專家，但是對於貨幣政策、財務金融等領域是全然陌生的。相對地，在該行的核心主管或員工，則都不曾涉獵作業風險分析及控管業務。

其結果是：因爲風險單位的專家對於業務的不熟稔，造成其於規劃風險時，採取由下往上的策略（bottom-up approach），風險管理流程圖（risk map）出現大量的程序，例如：僅人力資源一項在流程圖上即出現多達 60 個以上的程序，另外，執行時缺乏優先順序的概念，也是一大致命傷。因此，該計畫顯得一團糟，其目標遙不可及，風險專家開始失去信譽，計畫成效倍受質疑。

## 三、作業風險管理

### （一）概述

如同前述，作業風險管理爲企業風險管理之一環。根據新巴塞爾資本協定（英文簡稱 Basel II），作業風險係指因爲內部作業、人員、系統及外部事件等之不當或失誤，而導致財務損失、聲譽受損、或無法達成營運目標的風險。上述定義，

[4] 該國財政部長 Nicolas Eyzaguirre 表示，Carlos Massad 其實是無辜的受害者。
[5] 智利的風險及績效評估系統過去主要係供作監控該行的外匯存底之用。

不含信譽風險、政策風險及策略風險。

根據巴塞爾銀行監理委員會（The Basel Committee on Banking Supervision）的統計資料，銀行面臨的主要風險中，以信用風險所占比重最高，約爲 60%；其次爲作業風險，約占 30%；市場風險與信譽風險等，則約占 10%，由此顯示作業風險的重要性，應予妥善地監督管理；若處置不當，可能損失難以估計。例如：內控不周，讓交易員兼任交割或保管等業務，使其得便僞造文件矇騙主管，隱匿損失。最常見的例子就是 1995 年的英國霸菱銀行尼克李森（Nick Lesson）事件及日本大和銀行（Daiwa Bank Ltd.）井口俊英事件。前者造成高達 13 億美元的損失，最後霸菱以 1 英鎊的象徵性價格，被荷蘭國際集團（ING）收購；後者則藏匿逾 10 億美元的交易損失達 11 年之久。又例如：Bear Stearns 因某職員誤將 400 萬美元股票賣單輸入爲 40 億美元，導致紐約股市尾盤湧現巨額賣壓，險些釀成大股災。而證券交易員 Frank Gruttadauria 於任職 Lehman Brothers 及 Cowen 期間，竊取客戶帳款，並寄發僞造對帳單達 15 年，結果兩券商須賠償投資人 1 億美元的損失。國內的作業風險事件也不遑多讓，例如：華僑銀行國際金融業務分行副理越權操作衍生性金融商品，造成高達新台幣 52 億元的鉅額虧損；國際票券楊瑞仁盜開商業本票、僞蓋公司章，掏空約新台幣 102 億元。此外，台灣銀行公債盜賣案、財金公司客戶資料外洩案、台北銀行吉時樂彩券辨識碼疑遭人破解，致全面回收作廢等，均起因於作業不當所致。

許多中央銀行已開始採用作業風險管理架構，依各自的規模、文化、組織等特性，進行風險類型辨識、風險評估與衡量，注重品質更甚於數量，採取適用的方法來減低曝險。對於中央銀行來說，作業風險管理日趨重要，其原因一如前述：若作業不當或失誤，對於財務成本、聲譽所造成的傷害，後果往往不堪設想。尤其近年來金融市場的營運方式已有鉅幅的改變，例如，在全球化的趨勢下，即時式的管理模式（real time management）趨於普遍；新的金融商品的不斷創新，導致作業程序更爲複雜；委外作業的盛行，可能衍生新的作業風險問題；自動化資訊科技的大幅應用，加深 IT 系統的複雜性，潛藏許多隱性的風險；最近更因恐怖攻擊、震災等外部事件的影響，而意識到高衝擊/低頻率的事件，亦不容小覷。

## （二）作業風險之主要類型

1. 駭客入侵、系統失靈：在高度自動化下，若電腦系統管理不當，可能產生系統風險，甚而影響全球相關系統。例如：電腦當機、容量不足、運作遲緩、通訊中斷、程式錯誤等問題，導致業務無法或難以連續。

2. 系統不相容：在大規模併購及策略聯盟下，各系統間的轉換或整合，彼此無法相容。

3. 作業疏失：資料輸入錯誤或遺漏、簽章不符、未完成合法文件、擔保品不符、未具備或無法啓動備援系統等。

4. 內部詐欺：從事未經授權的交易、故意製作不實的財務資訊，內線交易、竊取顧客機密資訊、僞造文件等。

5. 員工能力不足、缺乏誠信、溝通不良。

6. 有形資產的損害：地震、火災或是水災等自然災害，甚至恐怖攻擊、蓄意破壞等。

7. 委外作業增加：降低己方的作業風險後，卻可能衍生他方的作業風險。

## （三）作業風險管理的建置

在 Basel II 中，關於作業風險管理的建置要求包括：

1. 銀行董事會及高階管理者的承諾與支持，積極參與監督作業風險管理架構。

2. 銀行具備健全、可行的風險管理系統。例如：製作作業風險之風險圖像（Risk Profile），辨識各業務流程潛在之威脅、機會、優勢與弱勢；辨識各項作業風險及其來源；以適當且一致之定性或定量的標準，衡量各類風險、商品或服務的曝險程度；定期評估風險的發生頻率及嚴重性，持續監測、追蹤風險控制不足之處；提供作業風險之預警訊息，即早通報超過作業風險限額狀況及例外狀況。

3. 定期演練、測試與維護，俾確認緊急防護措施的有效性。

4. 建立風險管理的溝通模式，包括角色、責任、計畫標的、關鍵成功因子、績效量測、資源和風險管理概要，並施行教育訓練；定期向董事會、高階

管理者及業務管理者報告作業風險曝險情況，並針對管理報告所反映之資訊採取適當行動。

5. 建立健全的內部稽核制度，例如：建立稽核計畫及程序，定期評估及驗證作業風險管理架構及流程；查核時所發現的缺失或異常，應詳列於稽核報告中持續控管，並定期提出追蹤報告；查核範圍與頻率應與曝險程度相當；聘任具備作業風險管理專業知識及經驗的稽核人員，以瞭解、檢核及驗證相關的執行程序及衡量機制。另外，應確保作業風險管理功能獨立於稽核單位及風險承擔單位。

## 四、業務持續性管理

（一）概述

經歷了美國 911 恐怖攻擊事件、日本震災，以及各國因地球暖化、人心浮動，天災不斷，戰亂頻傳，加上科技發展，人類對於自動化系統高度依賴，電腦病毒、駭客攻擊、系統當機、軟硬體毀損等潛在威脅，對於政府或企業的生存環境增添許多不確定性，致使災害防治、永續經營的觀念開始廣受重視，紛紛制定相關的營運持續計畫及流程，希冀當重大意外事故發生時，營運仍不中斷，將損失降至最低。

「持續經營管理」的發展，在 1970 年代，主要著重於電腦災害復原方面，至 1980 年代，逐漸轉向企業風險管理，1990 年代，全力籌建千禧年緊急應變措施，近期，則回應 2001 年 9 月 11 日的恐怖攻擊事件，「業務持續性管理」更為世人重視。

根據世界銀行估計，因為 911 恐怖攻擊事件，導致股市連續休市四日、飛機停飛一週、企業暫停下單、百老匯及職業運動停止演出數日等營運中斷，造成美國之國內生產毛額減少 250~350 億美元。不過，在同一事件中，位於世貿大樓的摩根史坦利銀行，有 3,528 名員工身在其中，當恐怖份子駕機撞上第一大樓後，其安全主管在一分鐘後緊急廣播，員工立即進行疏散，不到半個小時，該行已在 Seventh Avenue 成立應變指揮中心，又 10 分鐘內，緊急啓動位於 Varick 街的資

訊備援中心，同時建立位於紐澤西州 Harberside 的第二辦公室，恢復各系統的運作。因爲立即啓動營運持續計畫，使其營運得以迅速復原，不僅維護客戶的權益，更能建立與客戶間的長遠信任關係。摩根史坦利的成功經驗，已成爲全球仿效的典範。

國際上制定的企業營運持續計畫，舉其重要者包括：美國國家防火協會（NFPA）制定的「NFPA 1600 災害/緊急管理與企業營運持續計畫」，加拿大財政部的「保全及營運持續管理標準」、新加坡金融管理局的「新加坡營業持續管理架構及標準」（Business Continuity Management Guidelines）、香港金融管理局的「營運持續計畫」（TM-G-2 Business Continuity Planning）等。台灣工研院環安中心在 SARS 及禽流感流行期間，也制定了「企業營運持續管理技術手冊」。英國標準協會（British Standards Institution，簡稱 BSI）更是積極地推動 BS25999[6]，此國際標準提供一套可供衡量的準則與指導綱要，適用於各行各業，指導其建立完善的防護機制，俾確保營運持續，維持競爭力。

BSI 於 2006 年 11 月公布的 BS25999-1[7]，內含營運持續管理的作業要點，包括建立程序、作業過程與指導原則，爲營運持續管理之參考手冊；2007 年公布的 BS25999-2，說明營運持續管理之必要條件，若遵照施行並通過審核之後，即可獲得 BS25999 認證，故亦爲一驗證標準。總體而言，BS25999 提供一營運持續的施行策略與架構，在發生重大事故之前，預先做好防範的準備，落實復原演練，當災難來臨時，即可降低營運上的損失，強化組織的應變與復原能力。

根據 BS25999-2 的定義，「業務持續性管理」指一種全面性的管理程序，可用以辨識企業的潛在威脅，以及，設若這些威脅真實發生時，對企業營運可能造成

[6] 在此之前，BSI 曾制訂「PAS56 營運持續管理指導綱要」，提供企業維持關鍵企業營運的參考。

[7] 該協會制定的 BS7799，亦涉及營運持續管理，不過，其內容策重於資訊（IT）安全方面。其中，BS7799-1 爲「資訊安全管理實施指南」，於 2001 年 2 月爲國際標準化組織（ISO）納入國際標準 ISO/IEC17799，主要提供資訊安全管理概要性的指導原則。而 BS7799-2 則爲「資訊安全管理體系規範和應用指南」，說明資訊安全管理體系的必要條件，可作爲一認證標準，對機構的資訊安全管理體系進行考核和認證。在 BS7799 中，只要涉及資訊機密性、完整性與可用性者，均需併入計畫，定期進行測試與改良。

的衝擊。經由這套程序，企業可建置有效地回復正常運作的作業架構，藉以守護重大股東的權益、企業的名聲、品牌、價值創造活動等。

綜合言之，「業務持續性管理」的目標，在於增長企業的復原能力。其方式爲：辨識可能造成企業營運中斷的潛在性衝擊、認同回復企業核心業務的優先順序、建置相關的基礎架構及復原策略。

## （二）建置業務持續性管理架構

建置一「業務持續性管理架構」，需將資訊安全、風險管理、工作環境安全、產品品質、物流等管理系統全面納入考慮。

先進國家已陸續將其納入法規中，例如：新加坡政府規定上市公司的營運中斷時間以 4 小時爲限，違反規定即開立罰單，限制其業務拓展。當美國二房危機、雷曼兄弟等銀行陸續出現問題或倒閉後，新加坡、香港、中東、日本、歐洲等國也越來越重視 BCM 的立法問題。台灣在相關認證上，目前係以 IT 服務等業務爲主要取得認證的單位。

在業務持續性管理的推動流程中（如圖二），其前置準備包括：

1. 取得高階主管的支持。

2. 三層組織共同推動：

—制定策略（Strategic）方面：由高階主管說明持續經營管理的重要性，並宣示推動的決心，及針對相關問題作回覆。

—執行戰術（Tactical）方面：指定持續經營總召集人，以統一對內及對外之聯繫溝通管道，及管控計畫進度及成本。

—實際操作（Operational）方面：指派各部門專責人員，例如：部門資深人員或部門主管，以協助公司推動BCM計畫。

3. 分配權責

—由中央負責指導、監督、檢討。

—各部門負責計畫施行細節。

以中央銀行爲例，高階主管可能意指其理事會，取得其承諾，對於持續經營的成敗極具關鍵，因爲持續經營管理涉及經費、行動優先次序的設定、風險及成本之間的取捨、置入組織文化的影響力、外部協調及其結果。有了理事會的支持，在行動上，較易發揮全面的作用。

圖二：業務持續性管理的推動流程


依 BS25999-Ⅰ之標準建置 BCM，其生命週期（Lifecycle）大致包括以下階段，

執行時可依 PDCA 模型[8]循環採用，以尋求一最適化的 BCM：

1. 營運持續管理方案：主要爲建立BCM系統架構，指定角色、權責，並持續維護與監控，故爲BCM生命週期的核心。

2. 瞭解組織：包括營運衝擊分析（Business Impact Analysis, BIA）與風險評鑑（Risk Assessment, RA）。目的在於鑑別關鍵活動、依存項目、及所需的資源，並建立每一關鍵活動可容忍的中斷時間及復原目標時間（Recovery Time Objective）、最低的運作程度，藉以支持關鍵商品或服務的持續提供，瞭解威脅所在，並選擇處理風險模式。

（1）營運衝擊分析：先鑑識可引起營運過程中斷的事件，如設備故障、水災和火災，再根據破壞程度及還原時間評估中斷後的衝擊。進行分析時，可先利用面談、填寫問卷、研討會、觀察、文獻、及上述綜合等方法蒐集資訊。

（2）風險評鑑：至少每年鑑別、定義與評估面對的外部或內部威脅、其發生的機率與弱點；尤其當面臨類如市場、法規、資訊科技、程序、場所等較重大的改變時。

3. BCM策略：依據前述營運衝擊分析與風險評鑑，找出各種可行的方案，進行其優缺點及成本效益分析，辨識場外需求及替代設備，決定較適當的處理策略，並取得主管的承諾，設若發生業務中斷情境時，即採取策略因應。例如：處理風險的策略可從下列面向考慮：

[8] 爲 Dr. W. Edwards Deming 於 1950 年受邀至日本講習時所介紹的一項管理理念，由 P 計畫（Plan）、D 執行（Do）、C 查核（Check）、A 處置（Action）四大步驟構成，爲一連串追求改善的行動。其中，P 應採目標管理，包括：訂定目標、決定達成目標的方法及評估標準；D 指依據計畫執行，而爲了落實行動，此一階段應做一小型的 PDCA 循環；C 爲依據評估標準，查核實際績效，亦即，比較目標值與實際成果；A 若發現未能達成目標，先採取緊急對策，消除該現象後，再重複 PDCA 循環，避免同樣的失誤。利用 PDCA 循環來達成目標，甚至超越目標後，應將結果標準化、製作範本。

（1）避免風險：對於較大的風險，應設法予以阻隔。

（2）降低風險：採取適當控制措施，以減少損失。

（3）轉移風險：例如購買適當保險。

（4）接受風險：某範圍內的風險，可予接受。

設置有效的備援場所是有必要的，因爲可以：

（1）增加IT的基礎設施、資料系統及操作上的回復能力。

（2）達成快速復原的功能。

（3）作爲危機管理的場所。

（4）建立集中的聯絡及資訊中心。

（5）提供所有主要工作人員共同作業的場所。

（6）異地備援。

4. 開發和執行業務連續性計畫：包括預防及管理危機事件、營運持續及復原等。

5. 測試演練、系統維護、查核績效。

6. 建立並置入BCM文化。

## （三）業務連續性計畫

經營持續計畫爲經營持續管理的一環，經歷了 BCM 的準備期、架構規畫期之後，即進入計畫發展期，每一個部門應即著手針對其關鍵流程，擬定事件發生時的 BCP，這是組織對事故採取緊急措施的重要依據，通常包括緊急應變計畫（Emergency Response Plan）、危機溝通計畫（Crisis Communication Plan）與營運復原/持續計畫（Disaster Recovery/ Business Continuity Plan）、或其他危害削減計畫（Hazard Mitigation Plan）等。擬定計畫時，其內容務必清楚明白，主管當局及責任歸屬明確易懂，對於跨及多單位的事項，須確保溝通、協調管道的順暢，於開創及維護計畫上，人力資源充足無虞、配置適當。

對於中央銀行，其所擬定的計畫尚須考慮者包括：計畫所涵蓋的對象包括中央銀行自己以及其他金融機構；對於中央銀行的核心業務，例如設定利率目標，是否可達成連續、不中斷；以及，本國其他金融主管機關的計畫等。

1．緊急應變計畫：應用於災害或緊急事件發生時，可根據其中的標準作業程序進行應變；建立緊急應變中心作業指揮中心，以利整合人員、物資、設備及資訊。其注意事項包括：

（1）辨識緊急狀況的潛在類別，例如：火災、化學物質外洩，及其應變所需資源。

（2）辨識及採用適當的緊急應變措施。

（3）於企業持續經營計畫中，加入緊急應變程序。

（4）釐清各角色的職責和溝通流程，以有效掌握緊急事件。

（5）配合主管機關的要求，維持良好互動，並確認符合法令規章。

2．危機溝通計畫：進行危機處理，由指定發言人與利害關係人溝通，說明目前受損狀況，安撫利害關係人情緒，增加客戶的信心，以維持企業正面形象與價值。因此，執行時機可能爲事故發生後 0 至 48 小時內。災害損失的評估與協調，亦爲本階段的重要工作。

3．災後復原計畫：營運復原/持續計畫階段的執行時機，可能爲事故發生後的數天至數個月內，其功能爲設計流程與行動方案，進行災後復原策略的細部工程。依據既有的行政組織，確立工作原則，與各部門溝通、確認復原計畫的時程及可行性及工作內容，俾逐步恢復正常運作，以降低災害的衝擊。

俟計畫擬定後，即進入最後階段：系統矯正期。指針對相關計畫進行訓練與測試，且配合各項計畫進行沙盤演練測試。

1．教育訓練：針對營運持續計畫總召集人及各部門專責人員，進行 BCM 各發展階段之專業訓練，其中，訓練文件應回歸管理系統中作維護並予管制。

2．演練測試及修正：定期檢討、測試、報告、績效衡量和演練，評估方案是否仍有缺失，針對不足部分進行修正。

## （四）兩個例子：英格蘭銀行與泰國中央銀行

1．英格蘭銀行：

（1）與衝擊營業持續有關的重大歷史事件：

—2005 年 7 月 7 日：倫敦運輸系統的恐怖攻擊事件。

—2009 年 4 月：倫敦的 G20 示威遊行事件。

—2009 年夏：豬（swine）流感事件。

—2009 年冬、2010 年、2011 年初：英國倫敦等處雪災。

—此外，電力中斷、火災、運輸罷工、火山灰等。

（2）關於營業持續管理的改進措施：

—製作營業持續及危機管理程序的相關文件。

其目的在於：

◆讓營業持續管理得以更有效率地進行。

◆在審計查核期間，得據以證明已落實營業持續管理。

◆在營業中斷期間，隨時有一份可憑以因應的參考文件。

—改進備援場所。

—建置鄰近的危機聯絡中心。

—針對核心業務建置局部的工作場所。

—IT方面的重大突破，包括資料儲存、擷取、遠端連線等。

—人力資源的回應及福利安排，如：救援部隊（Help-Team）。

—資深主管參與例行性、協調性的測試計畫。

—建置管理指標。

（3）與營業持續策略相關的新議題：

—新的威脅：例如，2012年將舉辦的倫敦奧林匹克運動會。

—保持營業持續管理的真實性及整體性。

—承擔新的法定責任。

—金融服務局（Financial Services Authority）將併入英格蘭銀行。

—改變的組織架構：例如，三方主管機關（Tripartite’ Authority)。

2．泰國中央銀行：

（1）BCP在泰國金融體系的發展情形：

—2006 年 8 月，適用國際清算銀行下的巴塞爾銀行監理委員會（BCBS）規範的營運持續管理高階原則。

—2007 年 1 月及 2008 年 8 月，央行發表金融機構建立 BCM 及 BCP 的政策聲明，作爲金融機構的指導原則及重要主張。

—2009 年 12 月，因政治動亂情勢緊張，央行重新檢討政治動亂方面的 BCP，並調查銀行的 BCP 是否都已準備就緒。

—2010 年 4 月，紅杉軍暴動，金融機構逐漸啓動異地備援機制，央行則在 5 月 17 日啓動備援機制。

—2010 年 5 月，評估央行的異地備援機制，包括硬體設施及支付系統；並調查金融機構異地備援之困難或障礙。

（2）泰國央行重新檢視其與政治動亂相關的BCP：

—模擬當動亂日益升高，致金融體系發生流動性不足時，央行的因應對策。

—檢討危機管理委員會的角色及職權。

—檢討在各種事件下的因應對策。

—檢討央行員工的角色及職權。

—檢討溝通聯繫計畫。

—測試異地備援的 IT 系統及硬體設備。

—備份資料。

（3）調查銀行的BCP準備情形：

—與金融機構的高級主管洽談。

—重點在於員工、業務操作、IT 及通訊方面。

—所有與政治動亂相關的 BCP 都已準備妥當，類如金庫、存款等重要的業務，其功能可否持續運作，都已測試完畢。

—大型銀行另需考慮自己與其交易對手的流動性問題。

（4）央行與金融機構之異地備援啓動時機[9]：

—動亂爆發並擴散。

—總行位於暴動區內。

—交通受阻，致員工無法上班。

—最後的決定權在於總裁（僅適用於央行）。

（5）關鍵業務的運作情形：

—支付系統：包括 BAHTNET 及票據交換。

- 在交割方面，提供一些彈性，例如：允許以 e-mail 交換交割訊息，延長交割週期等。

—貨幣市場操作：

- 透過換匯方式，挹注美元至市場以增加流動性。
- 在 5 月 17、18 兩天，延長央行的電子債務憑證窗口的營業時間。

—紙鈔發行：

- 在 5 月 20 日及 21 日，仍開放銀行領取鈔票，讓銀行的 ATM 供應無虞。

（6）總檢討

央行方面，除了極少數的辦公室缺少計算機、印表機墨水、擴音器、電線插頭等物件，無線電通訊品質不佳、電話機短缺，致對外聯繫較爲困難外，其他類如硬體設施及 IT 等，都運作順暢，回復良好。

在金融機構方面，發現有些銀行之備援地點，不是太接近原基地，就是

[9] 位於動亂區域的銀行分支機構，提前結束營業、全天未營業、移至他地營業者，商業銀行方面分別有 960、195 及 67 家分行，啓動異地備援者有 10 處，外商銀行方面則僅有 1 家提前結束營業，啓動異地備援者有 11 處。

距離央行備援地點太遠，當動亂擴散時，難收其效；而對於租用備援場所的金融機構，則發生設備不足的窘境[10]。

此外，有家大型金融機構因爲與票據交換所連線失敗，造成整個交換系統作業停滯。有些無法與交割系統連線的銀行，必須改採手動方式傳送訊息；有些銀行的通訊錄未更新，無法與員工聯絡；還有部分客戶或其他關係人，因爲不知道銀行備援場所的電話號碼，而電話轉接系統又失靈，故無法得到需要的服務。

## 五、建議

於前言曾提及之「行動計畫」，簡報時大致表達兩點想法：

（一）我國央行的作業風險管理，不像與會各國代表般，有一專設的內部稽核或風險管理部門，而是以一工作小組（task force）來負責統籌該項業務，落實風險管理與執行。我們的挑戰主要在於風險識別方面，在現今詭譎多變的金融環境下，對於風險數量與種類的掌控，似乎還是有可加強之處，而各部門間的溝通、聯繫，也可以再多加努力。

（二）在業務連續性計畫方面，我們定期都會執行演練計畫，確實做好備援措施，尤其在資訊系統（IT）方面。不過，關於人力資源方面，可能爲比較弱的一環。例如，當發生緊急災難時，員工顯現的恐慌、不確定與焦慮之情形，人事單位是否有足夠的訓練可以加以輔導、安撫，協助身體、心理的安定，可能是我們的挑戰之一。

[10] 在家工作的員工，可能因爲缺少安全程式、驅動軟體，或 INTERNET 速度太慢等因素，無法與銀行系統連線。