出國報告（出國類別：其他）

參加中央銀行業務出版公司「Business Continuity Planning and Operational Risk Management for Central Banks」研討會報告

服務機關：中央銀行
姓名職稱：許玉明 三等專員
派赴國家：馬來西亞
出國期間：103 年 12 月 1 日至 5 日
報告日期：104 年 2 月 25 日

摘　要

近年來全球重大天災人禍頻傳，恐怖攻擊事件、地震、水災、風災、大規模傳染病等影響企業正常營運的案例層出不窮，如何有效進行作業風險管理，降低作業風險可能造成的衝擊，並確保營運持續性，成為各國央行十分重視的議題。

本次研習包含 3 天的訓練課程，內容主要針對中央銀行的作業風險管理方法及營運持續計畫實施情形進行經驗分享，並安排兩個主題情境的討論，讓學員可以就實務經驗互相交流，對工作知識與經驗的提升很有幫助。

本文為參加此次課程的心得報告，並提出研習心得及建議如下：

研習心得

1. 正視風險可能產生的危機，預防勝於治療。
2. 高階管理階層的支持是成功關鍵。
3. BCP 應定期檢討，與時俱進。
4. 內部稽核人員素質影響風險管理成果。
5. 溝通與協商是風險管理很重要的一環。

建議事項

1. 強化營運持續運作管理，適時調整修正。
2. 加強緊急連絡機制。
3. 辦理員工教育訓練，強化風險意識。
4. 加強討論技巧及表達能力的訓練。

目　次

壹、 前言.....1

貳、 識別及調查中央銀行的風險狀況.....2

一、 中央銀行面對的主要風險.....2

二、 菲律賓中央銀行風險管理方法.....3

參、 作業風險管理.....6

一、 風險控制與自我評估.....7

二、 作業風險管理組織.....11

三、 作業風險管理成功要素.....13

肆、 營運持續管理.....13

一、 營運持續管理方法.....13

二、 營運持續運作計畫.....16

三、 業務恢復基礎設施.....18

四、 危機管理及溝通.....20

伍、 研習心得.....21

陸、 建議事項.....22

附錄 1　研討會議程.....24

附錄 2　作業風險損失事件型態分類.....25

附錄 3　危機管理與風險管理循環示意圖.....27

參考文獻.....28

圖表目錄

圖 1 中央銀行面對的主要風險 3
圖 2 菲律賓中央銀行風險管理框架 4
圖 3 菲律賓央行的風險管理控制措施 5
圖 4 作業風險管理流程 7
圖 5 風險地圖.....10
圖 6 埃及央行風險管理組織架構 14
圖 7 埃及央行的 BCM 架構.....15
圖 8 巴基斯坦央行 BCP 治理架構.....17
圖 9 備援中心類型 18
圖 10 備援中心之成本效益 19

表 1 風險影響矩陣 8
表 2 風險機率矩陣 9
表 3 風險等級矩陣 9
表 4 營運復原場所選擇的參考 19

壹、前言

近年來全球重大天災人禍頻傳，恐怖攻擊事件、地震、水災、風災、大規模傳染病等影響企業正常營運的案例層出不窮，如何有效進行風險管理，降低風險可能造成的衝擊，並確保營運持續性，成為各國央行十分重視的議題。

本次奉　派參加由 Central Banking Publications 公司在馬來西亞舉辦的「營運持續運作計畫與作業風險管理」研討課程，學習其他國家中央銀行之作業風險管理(Operational Risk Management，ORM)及營運持續運作計畫(Business Continuity Planning，BCP)作法，期能以適當且成本效益較高的方式來確保關鍵性業務的持續運作，並協助本行資訊系統營運持續運作相關業務之推動。

本次研習包含 3 天的訓練課程，講師來自新加坡、菲律賓、巴基斯坦、埃及、馬來西亞、捷克等國風險管理或營運持續管理部門主管及具經驗的專家；學員共計 10 位，分別來自馬來西亞、香港、斯里蘭卡等國家及地區的中央銀行或金融管理單位。課程內容主要針對中央銀行的作業風險管理方法及營運持續計畫實施情形進行經驗分享，並安排兩個主題情境的討論，讓學員可以就實務經驗互相交流，對工作知識與經驗的提升很有幫助。

本文為參加此次課程的心得報告，內容包含五個部分，除前言外，課程內容部分包含：識別及調查中央銀行的風險狀況、作業風險管理及營運持續管理，並提出研習心得及建議。

貳、識別及調查中央銀行的風險狀況

一、中央銀行面對的主要風險

世界各國的中央銀行，因其國家或區域的規模、文化、組織、機構特性等的不同，而有不同的職能和目標，一般來說，中央銀行的職權包含貨幣政策的擬定與執行、金融機構的監管、支付系統的維運與監管以及協助經濟的發展。由於中央銀行在金融及物價穩定上的重要角色，在執行其職能時亦面臨相當的風險，講師將中央銀行面對的主要風險分為三類 (如圖 1)，說明如下：

(一)策略與政策風險(Strategic and Policy Risk)

政策風險是指因政策設計和執行的無效率，而產生不利影響的風險。例如 無效率的貨幣政策、金融不穩定、消費者保護不適當等。

(二)財務風險(Financial Risk)

財務風險是指因營運而進行市場活動和操作，造成財務損失的風險，如支付系統帳戶之日間透支、債券、或其他付款活動等日中可能之曝險、外匯存底投資及幣別組合之價值等受匯率變動之影響。

(三)作業風險(Operational Risk)

根據新巴塞爾資本協定(The New Basel Capital Accord)，作業風險的定義為「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」。其中內部因素來源包含人員經驗不足、作業程序錯誤、舞弊或詐欺行為、電腦系統缺乏穩定性等；外部因素來源如天然災害、恐怖攻擊等。

圖 1：中央銀行面對的主要風險

資料來源：課程講義

由於中央銀行肩負促進國家金融及維護對內及對外幣值穩定的重要責任，其作業風險可能對整個國家金融體系甚至全球金融體系造成嚴重影響，因此更需有明確的管理策略、清楚定義作業風險管理組織權責及職掌、規劃完善的作業風險管理流程及設計所需之作業風險管理資訊，以降低作業風險可能帶來的衝擊，並達成央行營運及管理目標。

二、菲律賓中央銀行風險管理方法

菲律賓中央銀行風險管理部門主管以實際經驗，分享該國央行在面對現今不斷變化的作業風險時，如何建構風險管理框架以識別、管理和降低營運風險。

(一)透過四大支柱：範例、模板、角色和方法 (如圖 2)，實現三個重要的目標：

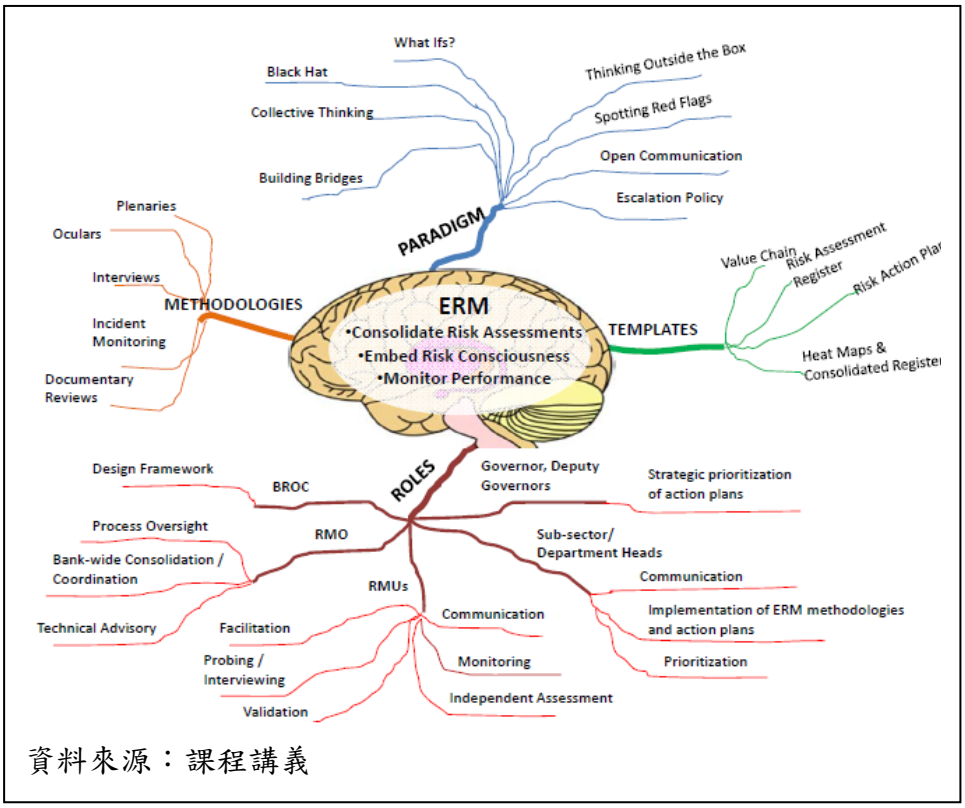
✧ 識別組織面對的風險：提供高階管理人員廣泛的

風險評估，並向董事會提出健全及審慎的政策建議。

✧ 提升組織的風險意識：促進銀行業務的風險管理意識。

✧ 監控風險管理的績效：監控企業風險管理的整體性能。

圖 2：菲律賓中央銀行風險管理框架



資料來源：課程講義

(二)風險管理方法

菲律賓央行於 2010 年訂定有關企業風險管理的相關文件，做為內部作業及決策時的指引，同時也讓外部機構對央行的營運持續運作更具信心。除此之外，定期召開風險管理會議，藉由事件報告、文件審查、訪談等，進行風險監控及審查。

✧ 事件報告(Incident Reporting)

包含事件發生的頻率和嚴重程度

✧ 文件審查(Documentary Reviews)

包含風險評估(Risk Assessment Register)、風險行動計畫(Risk Action Plan)、風險偏好陳述(Risk Appetite Statement)等

✧ 訪談(Interviews)

藉由與各部門業務主管進行訪談，發現各業務單位最亟需控管的風險，主要風險辨識出後，再對各單位作業人員進行更細節的訪談，了解各單位細部的作業流程，並設法在訪談過程中辨識出可能的風險來源

✧ 參考其他國際標準

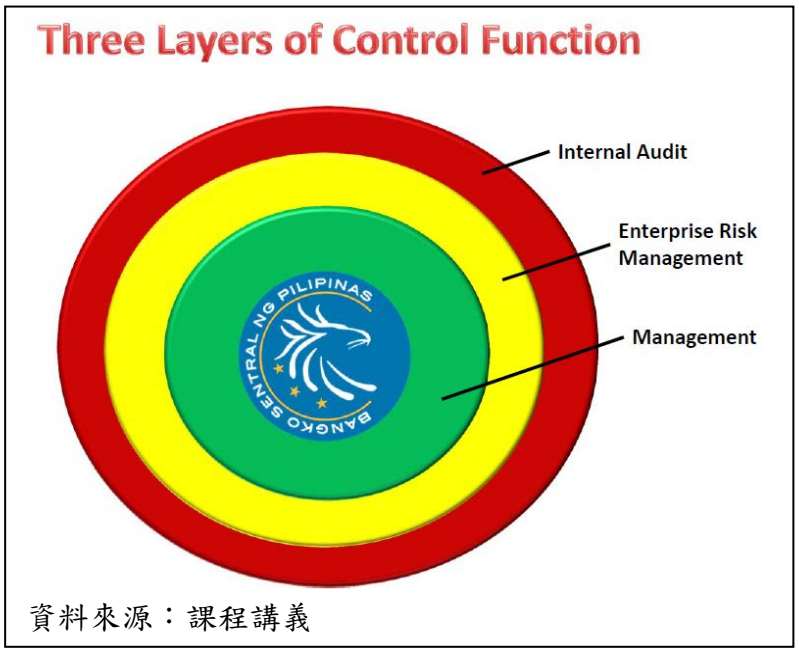
1. 風險管理原理及指導綱要

   ISO 31000：2010 on Risk Management – Principles & Guidelines

2. 風險管理-風險評估技術

   ISO/IEC 31010：2010 on Risk Management – Risk Assessment Techniques

圖 3：菲律賓央行的風險管理控制措施



資料來源：課程講義

參、作業風險管理

作業風險的定義在前面已經提過，一般來說，作業風險發生的主因可歸納為人員、系統、流程及外部事件四大類：

1. 人員：由員工行為引起或是有員工涉入，所引起之作業風險事件；包含不當的分權控管、人力不足、經驗或知識缺乏、不適任、舞弊、疏失等。

2. 系統:由於資訊設備或各類基礎設施失效而導致之作業風險事件；涵蓋中斷、系統控管不周、通訊中斷、程式錯誤、資料錯誤、執行與控管不周等。

3. 流程：由於交易失誤、客戶帳戶管理、清算以及每日營業流程之執行失誤導致之作業風險事件;例如模型或參數錯誤、執行/交割錯誤、錯帳、產品過複雜、逾越授權、安全控管不周等。

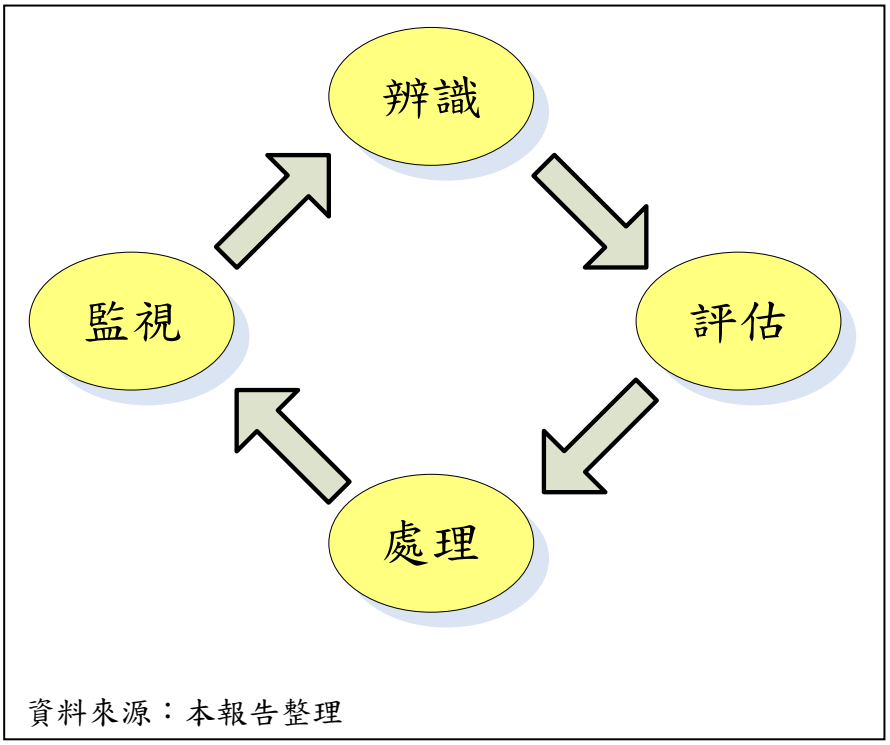
4. 外部事件:由於第三者行為所導致之作業風險事件；包含外部詐欺、實質資產毀損，以及各類法令改變而影響某項業務持續營運之能力；例如恐怖活動、政治因素、稅賦、法規變動、經濟環境、同業競爭、天災等。

作業風險造成損失型態則包含內部詐欺、外部詐欺、僱用慣例/工作場所安全、客戶/產品/營業行為、人員或資產損失、營運中斷與系統當機、執行/運送及作業流程之管理等，詳如附錄 2。

作業風險管理的目的，是藉由建立及有效執行作業風險管理架構與機制，以降低組織的作業風險，並達成營運及管理目標。組織可依本身業務規模、性質及複雜度訂定作業風

險管理準則及程序，基本上作業風險管理流程可分為辨識風險、評估風險、處理風險、監視/審查(如圖 4)。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組織具備完善的作業風險管理。

圖 4：作業風險管理流程



資料來源：本報告整理

作業風險是可以被測量及以量化的方式進行風險分析，以下簡述風險控制與自我評估方式：

一、風險控制與自我評估

風險控制與自我評估(RCSA：Risk-Control Self Assessment)是一種結構化風險自評之工具，此工具主要目標在識別組織內部主要業務流程之潛在風險，及現存控制機制是否有效。實務中，自我風險評估過程不但花費最多人力時間，也最易遭受業務單位抗拒。完成業務流程檢視並辨識營運過程中可能發生之作業風險點後，則可將大部分作業風險事件進行全面性的定位及歸類，

以便對事件發生之影響程度與發生機率做進一步的分析作業。

(一)風險影響度分析

影響程度分析方式可分為質化或量化，質化分析通常將影響程度分類為低、中、高、非常高及災難性的等幾個等級(如表 1)，若組織針對內部風險資訊或外部事件有完整建檔紀錄時，則可參考歷史紀錄或損失金額將影響程度進行量化估計。

表 1：風險影響矩陣

	層級	說明
影響	災難性的	發生非常嚴重的影響，重大的財務損失(如：大於 500 萬的財務損失)
	非常高	發生非常嚴重的影響，重要的財務損失(如：大於 100 萬的財務損失)
	高	發生嚴重的影響，高度財務損失(如：介於 100~500 萬的財務損失)
	中	發生中度的影響，可以及時處理並控制，中度財物損失(如：介於 10~50 萬的財務損失)
	低	發生輕微的影響，低財物損失(如：約 10 萬的財務損失)

資料來源：課程講義

(二)風險發生機率分析

針對事件發生機率分析亦同樣可採質化或量化方式，質化分析通常將發生機率分類為低、中、高、非常高及災難性的等數個等級，組織亦可參考歷史經驗或紀錄將交易次數及風險發生機率予以量化，設定各級分類標準(如表 2)。

表 2：風險機率矩陣

	層級	說明
機率	災難性的	在大部分的情況下，預期會發生
	非常高	在大部分的情況下，有發生的機率
	高	偶爾會發生
	中	偶爾可能發生
	低	在未預期的情況下，可能發生

資料來源：課程講義

(三)風險等級評量(風險地圖)

依據風險事件給予不同影響程度及發生機率後，即可透過風險比對的步驟，得出各風險事件之風險高低程度，亦即表示在未採取任何管理措施前，先行界定各風險事件之屬性。

表 3：風險等級矩陣

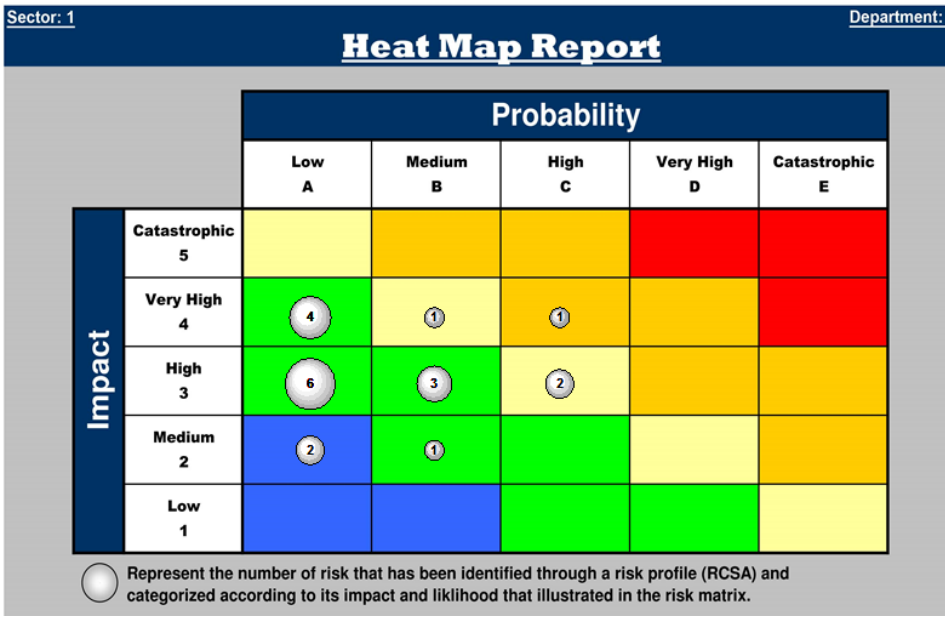
		機率				
		低	中	高	非常高	災難性的
風險	災難性的	Major	Massive	Massive	Catastrophic	Catastrophic
	非常高	Minor	Major	Massive	Massive	Catastrophic
	高	Minor	Minor	Major	Massive	Massive
	中	Insignificant	Minor	Minor	Major	Massive
	低	Insignificant	Insignificant	Minor	Minor	Major

說明：Catastrophic：極度高風險，必須立即採取行動。
Massive：高風險，高階管理階層必須注意。
Major：中度風險，管理階層有責任將之列入管理。
Minor：低度風險，納入例行性管理。
Insignificant：極度低風險，無需管理。

風險評量的結果是挑出一些需要進一步優先處理的風險。組織應該考慮營運目標以及冒險可能會帶來的機會。如果評量的結果顯示風險的危險性低或為

可接受的程度，則這些風險將接受程度最小的風險處理。組織應監督並定期檢討這些低危險或可接受的風險，以確定這些風險仍維持可接受的程度。如果風險沒有被列為低危險或可接受的風險，則應使用風險對策來處理。

圖 5：風險地圖



資料來源：課程講義

(四)RCSA 的附加價值

一個設計良好的 RCSA 可協助辨識出銀行的風險及有效的控制措施，它提供的好處包含：

- 一致性的語言及衡量標準：為了促進風險評估、處理及報告的一致性，各部門(單位)應使用共同的語言，定義分類作業風險，以作為風險處理措施/控制的依據。
- 清楚且明確的風險所有權。
- 定義可降低風險的行動方案。
- 同仁與管理層之間對於風險和控制方法公開討論，從而更了解銀行的作業風險及可能造成的影響。

- 組織文化變革，使作業風險管理流程落實到組織的各項營運活動中。
- 提供預警信號。

二、作業風險管理組織

作業風險管理是組織內全體人員的職責，因此應要清楚定義每個管理階層的職掌，以確定組織具備完善作業風險管理機制。原則上，風險管理部門及業務支援部門皆應獨立於風險承擔單位；稽核單位亦需完全獨立於風險承擔單位，才能對風險管理機制進行客觀審視。

(一)董事會

1. 應瞭解銀行內所承擔的各項風險，並負擔起整體風險管理之最終責任。
2. 應建立適當的風險管理策略、政策、架構及全行的風險管理文化，並將資源做有效的配置。
3. 定期檢視風險管理策略、風險組織、風險流程及風險管理資訊，以確保其妥適性並掌握全行風險狀況。

(二)高階管理階層

1. 高階管理階層應執行董事會所核准之風險管理策略，及風險管理架構。
2. 監督檢視管理流程的適當性，並明確指派必要之專業人員。
3. 確認從事銀行各項風險管理之員工，具備專業的條件及能力。
4. 確保能有效地溝通與協調相關風險管理功能及跨

部門間之各項風險。

(三)獨立風險管理之機制

1. 針對經董事會核准之各項風險管理政策，監督其後續執行狀況。
2. 建立銀行衡量、監控及評估風險之整體架構，及相關項目之後續執行細則。
3. 確實瞭解各業務單位之風險限額及使用狀況，並於發現業務單位所承受的風險超出設定限額時，督促採取相關改正措施。
4. 進行業務單位風險調整後之績效衡量(或提供其他部門風險調整後績效之相關資訊) 。
5. 確認採用適當的方法，進行模型有效性之評估與回顧測試，以驗證各項估計結果之正確。
6. 適時且完整的提出風險管理相關報告。
7. 溝通與協調銀行內風險管理相關事宜。

(四)稽核

1. 稽核單位應建立適當之稽核計畫及程序，以檢視銀行內各單位風險管理之實際執行狀況。
2. 對於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。
3. 應具備適當獨立性之地位，以確保管理階層對於稽核報告內之建議內容，已及時採取適當之改善措施。

4. 銀行應聘任具備相關專業知識及經驗的稽核人員，以瞭解行內所採行之風險管理執行程序及風險衡量工具的模型或方法。

5. 內部稽核人員應評估內部控制制度在組織內部執行的情形，且在其獨立功能下，向管理高層報告，以促使內部控制持續有效。稽核工作在「消極上」是防止弊端，在「積極上」是協助管理階層，以精進企業之管理體質。

三、作業風險管理成功要素

1. 董事會及高階管理階層的支持與承諾。

2. 清楚明確訂定各事業單位的職責職掌。

3. 要與現行決策制定結構結合。

4. 要動員組織全體。

5. 初期應以教育訓練優先。

6. 需發展好的實例、手冊、技巧。

7. 要不斷學習與檢討改進。

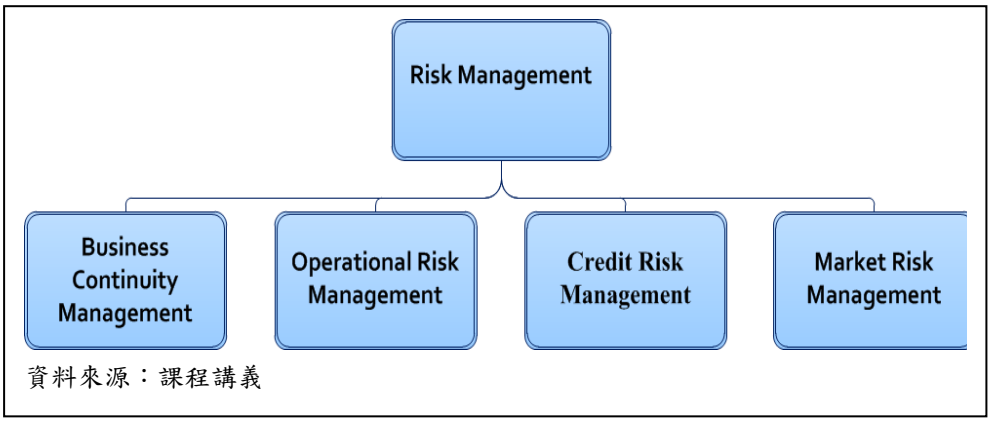
肆、營運持續管理

一、營運持續管理方法

營運持續管理(Business Continuity Management ：BCM)是一個整體的管理過程，目的是確定一個組織的潛在威脅，及這些威脅對業務營運可能造成的影響，並建立組織有效應對的能力，以保障利害關係人、組織聲譽，品牌與利益。

講師分享埃及央行的風險管理部門的組織架構，包含營運持續管理、作業風險管理、信用風險管理、市場風險管理均設有專門的管理單位(如圖 6)。

圖 6：埃及央行風險管理組織架構



資料來源：課程講義

(一)營運持續管理的目標

1. 防止業務活動中斷，確保重要業務流程不受重大故障和災難的影響。
2. 結合預防和復原措施，將風險造成的影響降低到可以接受的等級。
3. 分析災難、安全缺失和服務損失的後果。制訂和實施應變計畫，確保在要求的時間內恢復業務流程。
4. 選用控制措施降低風險，限制破壞性事件造成的後果，確保重要作業能及時復原。

(二)營運持續管理的方法

埃及中央銀行將營運持續管理分為三個階段(如圖 7)，分述如下：

1. 計畫階段

- 確認 BCM 需求
- 獲得管理階層同意
- 定義關鍵業務
- 進行營運衝擊分析
- 全行營運衝擊分析驗證
- 確認業務需求(包括復原目標時間及回復目標時間點等)
- 發展 BC 策略

2. 實施階段
   - 選擇營運回復場所地點
   - 獲得管理階層對營運回復場所的支持
   - 營運回復場所基礎設施的準備
   - 發展 BC 計畫
   - 執行 BC 計畫
   - 修正 BC 計畫
3. 改善階段
   - BCP 的定期測試
   - BCP 的修正與改善

圖 7：埃及央行的 BCM 架構

資料來源：課程講義

二、營運持續運作計畫

營運持續運作計畫(Business Continuity Planning：BCP)是針對各種可能災害事故風險，包括天然災害、營運策略錯誤、機密外洩、爆炸、傳染病(如 SARS)、電力中斷、石油危機、政治暴動、恐怖份子等等，擬定應變與復原計畫，以應付可能對組織所造成之營運與財務狀況。

相較於 BCM 是營運持續管理的過程(Process)，BCP 則是達成營運持續的計畫(Plans)，巴基斯坦講師為 BCP 下了一個註解--BCP 像是保險，你會希望永遠不要用到它，但當需要時，你會很慶幸你擁有它。

央行為維持國家整體金融穩定，除發展本身的營運持續運作計畫，對於同為金融體系一分子的其他銀行也有責任，這是央行面對的挑戰。巴基斯坦由於地理位置及政治因素，常遭受天然災害及人為的破壞，為確保營運的正常，對於緊急應變(BCP)及與金融機構間的聯絡管道等特別的重視，除本身訂定內部營運持續運作計畫外，並提供商業銀行相關參考指引，定期彙整商業銀行異地備援中心辦理情形、更新相關聯絡資訊等，確保央行及其他商業銀行都有營運持續運作的能力。講師以巴基斯坦央行實行 BCP 的經驗與大家分享：

(一)巴基斯坦央行於 2004 年發布金融機構的 BCP 指導方針，並於 2007 年進行修正。

(二)要求所有銀行定期提供資料，包括重要業務項目、測試頻率、測試的內容以及 BCP 演練的模擬情境。

(三)發行央行與各金融機構的 BCP(含備援中心)通訊

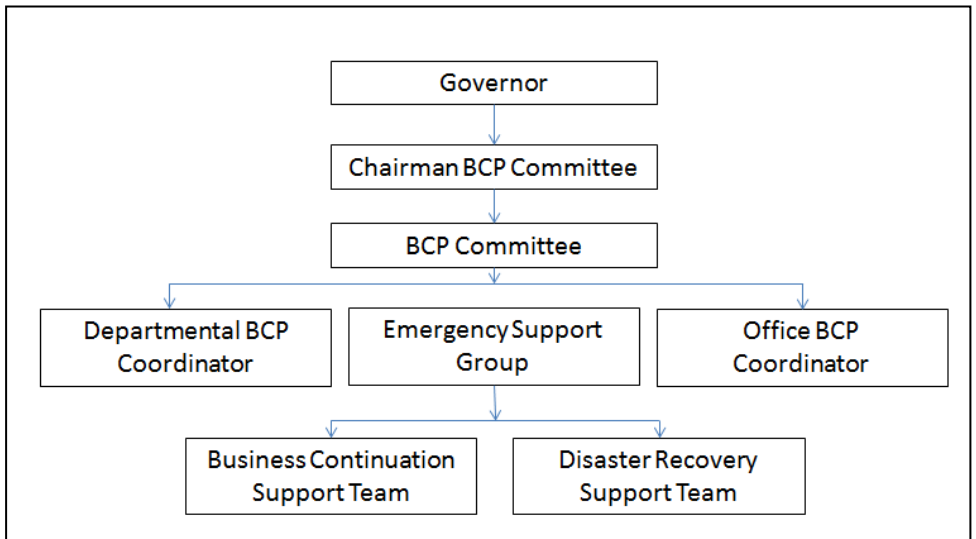
錄。

(四)定期與金融機構 BCP 聯絡員進行會議，以掌握各金融機構 BCP 執行情況。

(五)BCP 啟用/事件紀錄

1. 2005 年因地震造成 Muzaffarabad 地區的商業銀行都遭到破壞，最後使用巴基斯坦央行的辦公室作為該地區商業銀行的緊急備援場所。
2. Hyderabad 地區辦公室因暴民縱火導致 600 家商業銀行分行遭破壞。
3. 2007 年與 2014 年的選舉暴力。
4. 2014 年 11 月發生颶風威脅。
5. 2014 年 8 月發生罷工及靜坐抗議事件等。

圖 8：巴基斯坦央行 BCP 治理架構



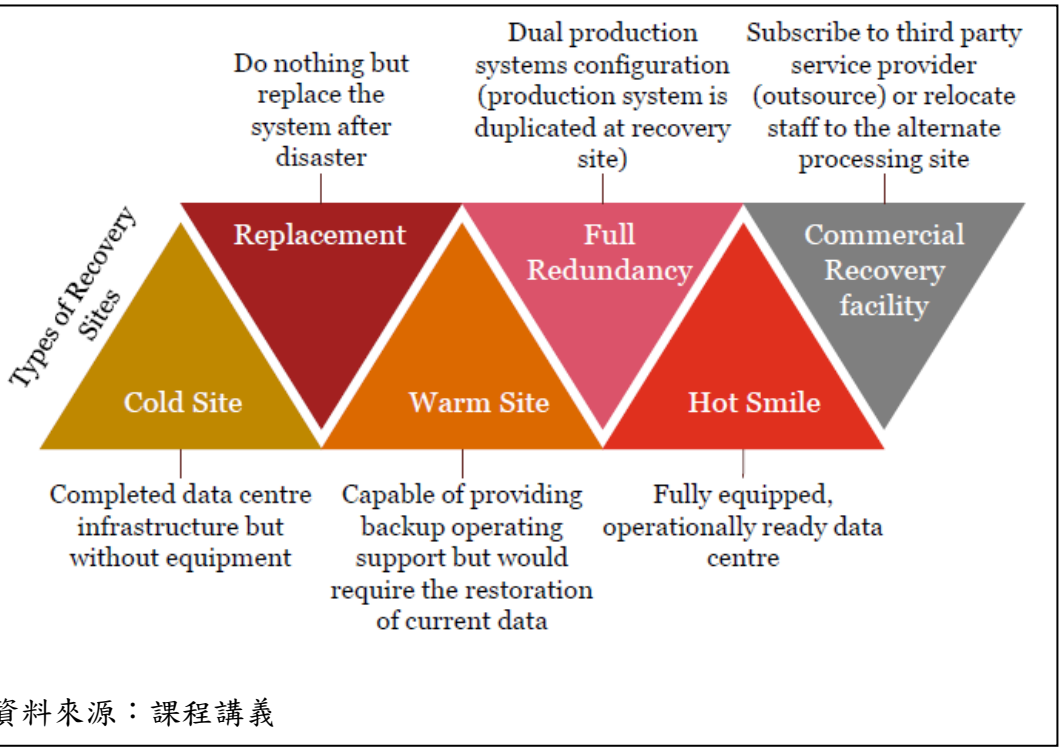
資料來源：課程講義

三、業務恢復基礎設施

在設計 BCP 時，備援中心的規模、地點及硬體設施配置等應該如何設計，可能是管理者實際面臨到的問題，營運衝擊分析(Business Impact Analysis,BIA)及關鍵業務的目標回復時間(Recovery Time Objective,RTO)、資料回復時間(Recovery Point Objective,RPO)兩項指標，可以作為評估依據。

RTO 指的是當災難發生時，回復企業資料所需的時間，亦即企業要花多少時間才能重新上線。而 RPO 指的是當災難發生時，企業可以忍受多少資料遺失，例如 A 服務能忍受資料遺失 4 小時，而 B 服務則是不能忍受任何資料遺失的時間，因此 B 服務的備援機制要比 A 服務來得更為即時，甚至達到與備援中心同步的狀態。

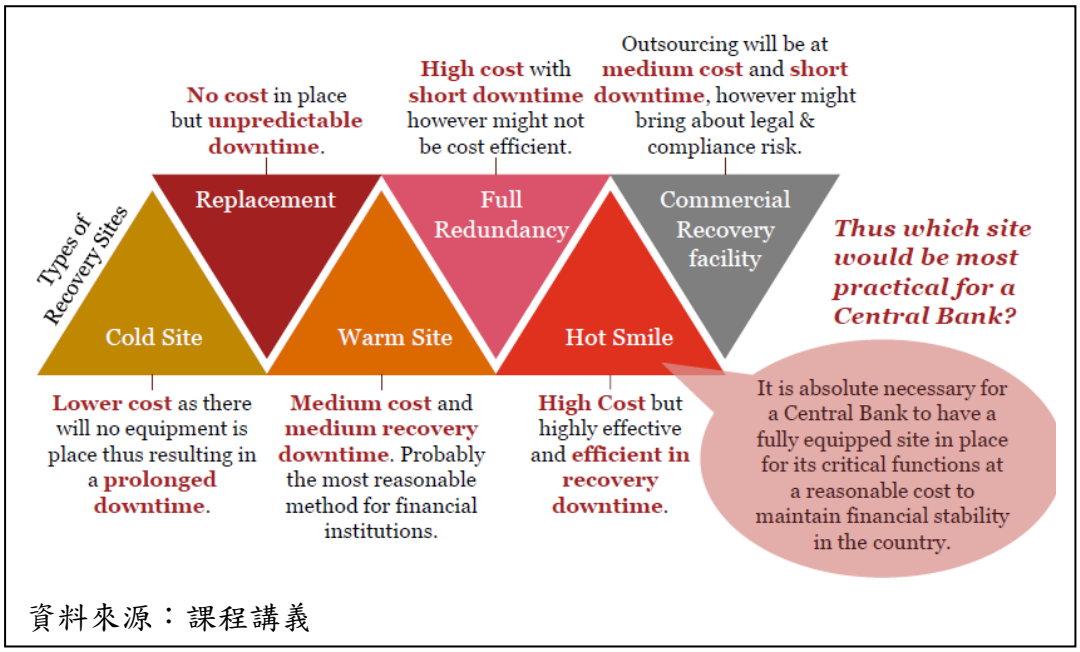
圖 9：備援中心類型



資料來源：課程講義

當 RPO 以及 RTO 的時間愈短，需要花費的成本就愈高。也因此，較不重要的周邊業務或許可以 24 小時以上才回復，而核心業務因為不能中斷，因此採取最高的保護策略，故企業在選擇備援中心時可依成本及效益進行評估(如圖 9、10)。

圖 10：備援中心之成本效益



資料來源：課程講義

除了上述幾種備援中心型態外，講師還分享選擇備援場所時考慮的項目(如表 4)：

表 4：營運復原場所選擇的參考

符合業務上的需求	可使用的辦公室環境
	適當的休息空間
	現金出納櫃台
地點	安全性
	資訊基礎設施是否已備妥
	與主中心間的距離
	無障礙的緊急服務
成本	設備成本
	管理成本
管理者的同意	BCM 預算
	營運復原場所的地點

資料來源：課程講義

四、危機管理及溝通

危機(Crisis)是指發生威脅到組織重大價值之事件，在處理時具有時間壓力，迫使決策者必須做出決策，該決策並可能有重大影響。危機是不可預測且變化快速的，並有下列幾項特性：

- 危機可能會帶來嚴重的威脅。
- 必須在時間壓力下明快、智慧的處理。
- 由不正確的決策引起。
- 危機吸引公眾及媒體的關注，消息可能未經證實但卻迅速傳播。
- 高度複雜且同時影響許多人。

危機管理(Crisis Management)則是指為避免或降低危機對組織之傷害，對危機情境維持一種持續性、動態性之監控及管理過程。危機管理與風險管理循環圖如附錄 3。

央行面對危機的處理方式會密切關係到金融市場、媒體和民眾，在關鍵時刻，錯誤的消息或語氣可能導致局勢惡化，因此在進行危機處理時，快速、誠實的溝通，可以降低危機可能造成的傷害。進行危機溝通要點如下：

- 儘速蒐集真相並儘快公布。
- 啟動危機處理小組，確立指揮系統、明確分工。
- 慎選發言人。
- 儘快澄清負面報導。
- 不斷的溝通，掌握議題建構的權利。

伍、研習心得

一、正視風險可能產生的危機，預防勝於治療

就如巴基斯坦講師說的，BCP 像是為企業的營運不中斷買份保險，央行身負穩定國家金融系統的重責大任，更應積極正視風險管理議題，不可心存僥倖心態，事前充分、完整的風險管理，有助於在危機發生時，明快、智慧地處理，並減少可能造成的衝擊。

二、高階管理階層的支持是成功關鍵

由於作業風險管理及營運持續管理都是全組織的活動，關係到組織的資源分配及預算編列等，因此首長的全力支持是必要的成功關鍵，應將持續營運融入日常營運的決策過程中；此外，明確的風險政策、堅強的推動組織、完善的計畫與執行步驟、單位間分享風險管理的經驗，都可以使風險管理及營運持續管理更容易成功。

三、BCP 應定期檢討，與時俱進

來自組織內部及外部的威脅不斷在改變，在進行營運持續管理時也應隨時注意環境的變遷，定期檢視營運衝擊分析與資安現況，進行檢討及調整改進，以確保在新型態危機發生時、在有壓力的情況下，組織業務仍能維持運作。

四、內部稽核人員素質影響風險管理成果

內部稽核是風險管理中重要的一環，稱職且專業的稽核人員可以協助檢核及驗證組織所採行的作業風險管理程序及風險衡量機制是否洽當，是風險管理成功要

素。一般組織內稽核人員常需兼任其他工作，較無法專注於稽核工作，且可能對業務不了解，無法充分掌握業務流程,導致內部稽核效果不彰或虛有其表。培養專業、專職的稽核人員及定期的內部輪調應是較佳的作法。

五、溝通與協商是風險管理很重要的一環

應確保組織內全體員工均能瞭解面對的風險與支持風險對策，進而提升對組織的信任。文件化可有助於溝通及達成共識，避免誤會或各說各話，且應將結果詳實紀錄與傳承。

陸、建議事項

一、強化營運持續運作管理，適時調整修正

為確保業務的持續運作，應設置跨單位的營運持續運作管理小組，負責監控、評估營運持續運作計畫的辦理情形，且應定期召開檢討會議，各單位依實務上遇到的問題或業務流程的改變提出修正意見，定期檢討改進營運持續運作計畫，經由不斷修正及經驗累積，以確保計畫的有效性、正確性及可用性。

二、加強緊急聯絡機制

事件發生時常十分緊急，處理時間非常有限而緊迫，需以最快速度處理以降低可能造成的作業影響，故找對的人，事情就解決了一半。易於隨身攜帶的緊急連絡卡有助於緊急事件發生時，很快取得相關人員的聯絡方式。緊急連絡卡內容應至少包含緊急事件發生時的聯絡人員名單、聯絡方式及異地備援中心的連絡資訊等。

三、辦理員工教育訓練，強化風險意識

風險管理是全組織的事，每個人對於所掌業務面對的風險都應有辨識、評估及處理的能力，持續教育訓練接收新知，可於事件發生時，不致因沒有準備而慌亂不知所措，訓練有素的員工是風險應變時堅強的後盾。

四、加強討論技巧及表達能力的訓練

本次參與國際性研討會議實為寶貴經驗，除可加強資訊專業之外的管理知識，並提供自我成長及強化溝通、表達能力的機會。建議除積極參與國際性會議吸取國外央行經驗外，內部訓練課程也可增加個案討論、情境分析等上課方式，加強同仁思考及問題討論的訓練，以提升溝通能力。

附錄 1　研討會議程

編號	授課者	課程名稱
103/12/2		
01	Fot Chyi Wong 新加坡金融管理局風險管理部門前執行長	中央銀行的作業風險
02	Ma Regina Fajardo 菲律賓央行風控長	定義中央銀行的作業風險
03		企業風險管理
04	Asif Mahmood、Shehzad Ali Sharif 巴基斯坦央行 BCP 部門副主管、專員	與私部門間的合作關係
103/12/3		
05	Hatem Ibrahim 埃及央行 風險管理部門主管	作業風險管理方法
06		制定營用持續計畫
07	Fot Chyi Wang	主題討論：大型傳染病的緊急應變計畫
08	Eckart Koerner PwC 金融風險管理部執行長	營運恢復的基礎架構
09	Fot Chyi Wong、Edmund Chong	主題討論：如何因應新型態網路安全威脅
103/12/4		
10	Ludek Niedermayer 捷克央行前副總裁	稽核與風險管理委員會的角色
11	Edmund Chong 新加坡大華銀行 BCM 部門負責人	危機管理

附錄 2　作業風險損失事件型態分類

損失事件型態（層級 1）	定　　義	類別（層級 2）	營業活動項目（層級 3）
內部詐欺	至少有一名公司內部人員參與，意圖詐取、侵占公司財產、規避法令或公司內部規範（不含多樣化/差別待遇事件）所導致之損失。	未經授權行為	刻意匿報交易、未授權交易造成之金錢損失、刻意錯誤評估部位。
		竊盜與詐欺	詐欺/信用詐欺/不實存款、偷竊/勒索/挪用公款/盜取、盜用資產、惡意毀損資產、偽造、支票騰挪、私運、假帳/虛偽交易、不實稅務/刻意逃稅、賄賂/回扣、非公司帳之內線交易。
外部詐欺	外部人員意圖詐取、侵占公司財產或規避法令所導致之損失。	竊盜與詐欺	偷竊/強盜、偽造、支票騰挪。
		系統安控	駭客攻擊、竊取資料造成之財物損失。
僱用慣例、工作場所安全	因違反僱用、健康或安全規定及協議、支付個人損害求償或差異性/歧視事件所導致之損失。	僱用關係	薪資、福利、終止雇用、工會活動。
		環境安全	一般性責任、員工健康及安全規定、勞方求償。
		差別待遇	所有歧視之行為。
客戶、產品、營業行為	非故意或疏忽而對特定客戶未盡專業義務（包括忠實及合適性要求）、或因產品特性及設計所導致之損失。	合適性、揭露及忠實義務	違反忠實義務/違反指導原則、適當/揭露事項、違反消費金融揭露規定、損及隱私、強制性行銷、帳務炒作、誤用機密資料、貸放者責任。
		不當營業或市場行為	反拖拉斯、不當營運/市場慣例、市場操縱、屬公司帳之內線交易、未獲核准營業項目、洗錢。
		產品瑕疵	產品瑕疵、模型錯誤。
		選擇、推介及暴險	未依規對客戶徵信、逾越客戶限額。
		諮詢服務	就諮詢服務績效所引發之爭執。
人員或資產損失	因天然災害或其他事件所導致之損失。	災害及其他事件	天然災害損失、因外力（恐怖活動、暴力行為）造成之損失。

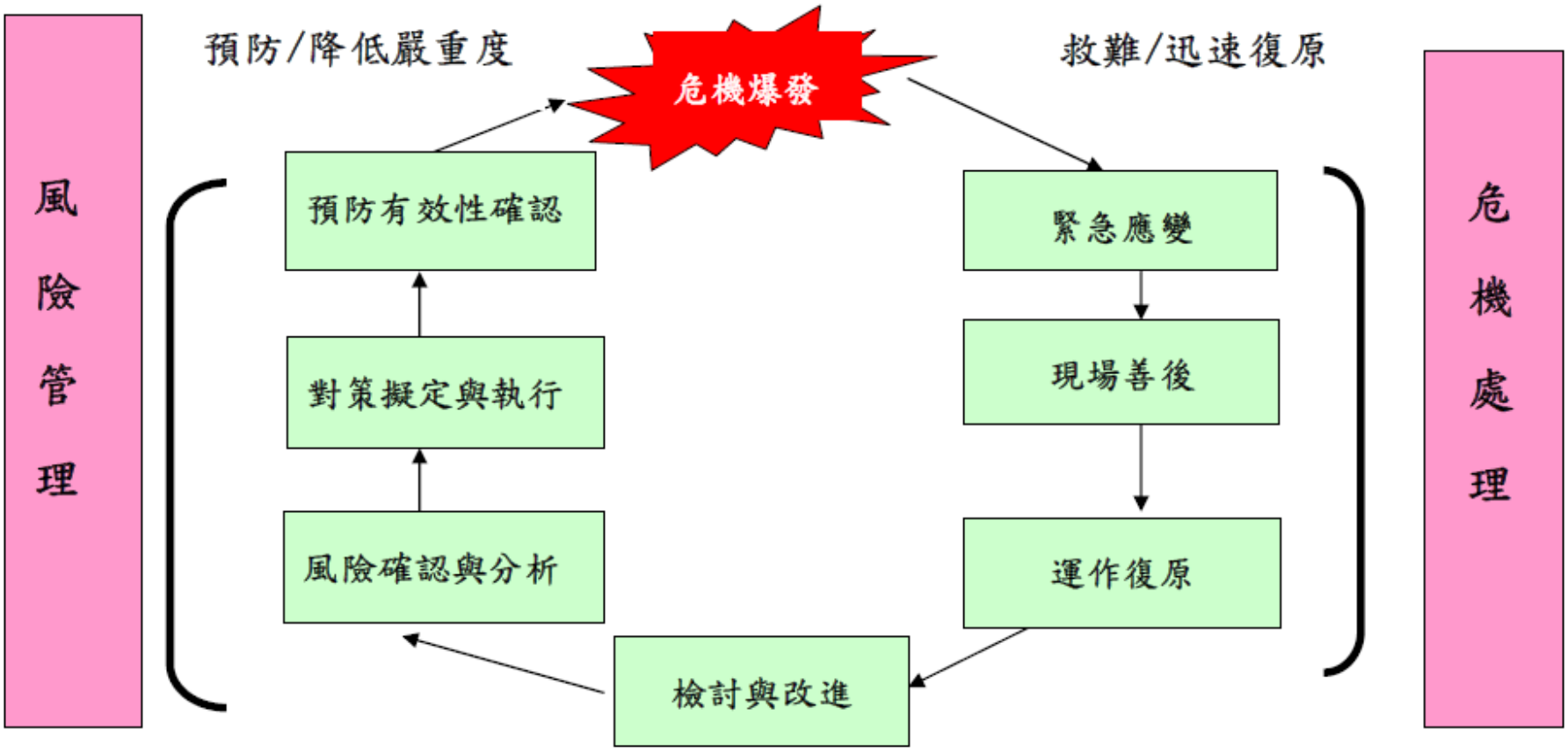
損失事件型態（層級1）	定　　義	類別（層級2）	營業活動項目（層級3）
營運中斷與系統當機	因營運中斷及系統當機所導致之損失。	資訊系統	硬體、軟體、通訊、水電或瓦斯供應中斷。
執行、運送及作業流程之管理	與交易對手或賣方交易之處理不當或過程管理疏失所導致之損失。	交易記錄、執行與維護	溝通不當、資料輸入、維護或記載錯誤、誤期、模型/系統失誤、帳務處理錯誤/交易歸屬錯誤、其他工作執行不當、交付失誤、擔保品管理疏失、註記資料維護。
		監控與報告	疏於必要之報告、不精確之外部報告所造成之損失。
		客戶吸收與文件資料	未徵提客戶同意書或棄權聲明書、相關法律文件遺漏或不完整。
		客戶/帳戶管理	未經授權接觸資料、因客戶資料錯誤所造成之損失、因疏忽造成客戶資產減損。
		交易對手	與同業交易處理不當、其他與同業交易之爭議。
		銷售商與供應商	委外、賣方爭議。

註：

1. 因天然災害或其他事件導致之損失：在七十二小時內發生之天然災害（地震、颱風、颶風、暴風、洪水等），除了發生在不同地點或非同時發生，於損失分類時，將被視為個別事件。
2. 營運中斷及系統當機：單一事件或連續性事件導因於相同原因（如機械故障發生於同樣部位、錯誤發生於特定程式），於損失分類時，將被視為個別事件。

資料來源：摘錄自銀行局-銀行自有資本與風險性資產計算方法說明及表格(2012)

附錄 3　危機管理與風險管理循環示意圖



資料來源：摘錄自風險管理及危機處理作業手冊

參考文獻

1. CentralBanking(2014)，「中央銀行營運持續計畫及作業風險管理」上課講義
2. Price Waterhouse and Coopers(2011)，「銀行風險管理實務範本-總論大綱及案例彙編」，銀行公會
3. Price Waterhouse and Coopers(2011)，「銀行風險管理實務範本-作業風險管理分論及案例彙編」，銀行公會
4. 行政院研究發展考核委員會(2009)，「風險管理及危機處理作業手冊」
5. 行政院(2008)，「行政院所屬各機關風險管理及危機處理作業基準」
6. 銀行局(2012)，「銀行自有資本與風險性資產計算方法說明及表格」
7. 新巴塞爾協定與我國券商之風險管理 http://nccur.lib.nccu.edu.tw/bitstream/140.119/35411/6/93260906.pdf
8. 古步鋼(2011)，「風險管理實務」
9. Michael E. Whitman, Herbert J. Mattord, Andrew Green(2009)，“Principles of Incident Response and Disaster Recovery”，Cengage Learning
10. Wei Ning Zechariah Wong,Jianping Shi(2014)，“Business Continuity Management System1”，Kogan Page
11. Susan Snedaker(2013)，“Business Continuity and Disaster Recovery Planning for IT Professionals”，Syngress Media