出國報告（出國類別：其他）

參加印尼央行
「央行與公共機構風險管理」
國際工作研討會報告

服務機關：中央銀行
姓名職稱：蔡美芬(研究員)、陳娟娟(一等專員)
派赴地區：印尼雅加達
出國期間：107 年 10 月 21 日至 10 月 27 日
報告日期：108 年 1 月 23 日

摘要

「風險」係指損失的發生與何時會發生是無法確定，且損失發生之結果亦無法預料。根據美國反舞弊性財務報告委員會所屬發起組織委員會(Committee of Sponsoring Organizations of the Treadway Commission，簡稱 COSO)的定義，可能帶來負面影響的事項，代表風險。風險管理之目的並不是消除風險，而是管理風險，藉以提高企業創造價值的能力。

中央銀行執行貨幣及外匯政策，承擔各種風險—包括財務風險及非財務風險，尤其金融危機期間，承擔更多風險，財務風險管理(如控管交易對手及擔保品風險及融通條件)有助中央銀行實現政策目標，保護中央銀行的聲譽、可信度及自主權。此外，網路傳播已擴大聲譽風險及營運中斷風險的負面影響，天災及人為事故等帶來的風險對營運中斷的損害亦更加頻繁，宜預先制定並健全營運不中斷及復原計畫，提升面臨營運中斷時的韌性；而近年他國金融監理機關因應網路風險對金融體系之衝擊，發布相關網路風險管理規範，亦可供參。

由於天災與人為攻擊(如恐怖攻擊、資安攻擊等)事件頻傳，印尼央行極為重視風險管理，並分享其經驗，除訂定風險管理相關規範外，並強化三道防線機制，整合風險管理與內部稽核作業。

研習心得：(一)各國中央銀行逐漸重視內部風險管理；(二)整合中央銀行風險管理、危機處理及營運不中斷等計畫，俾能採行妥善措施因應，降低衝擊；(三)資安防護有賴資訊分享。

建議事項：(一)本行風險管理、危機處理及營運不中斷等計畫或人員應相互交流並支援；(二)加強國際合作以強化資安事件之資訊分享與分析。

關鍵詞：中央銀行、風險管理、COSO、最後融通者

目次

壹、前言

一、目的與過程

台灣經濟高度依賴對外貿易，與國際金融市場的連動性亦高，因而深受國際經濟金融情勢及風險的影響。2008 年全球金融危機爆發，各國無一倖免，顯示在金融自由化及全球化下，風險透過外溢效果進一步蔓延，擴大其嚴重性。另一方面，資訊科技推陳出新，企業營運高度仰賴資訊化，惟也因此面臨網路攻擊的威脅，網路媒體的運用更加大了聲譽風險的衝擊。此外，台灣與日本、印尼同位於環太平洋地震帶，地震頻繁，2011 年 3 月 11 日日本福島第一核電廠因強烈地震引發海嘯，造成核電廠反應爐冷卻系統失靈，輻射外洩；本次研討會前一個月，印尼蘇拉威西島發生強震及海嘯，造成二千多人罹難、數千人失蹤，在在提醒人們必須隨時做好風險管理及防災準備。

印尼央行於 2018 年 10 月 22 日至 26 日，在雅加達舉辦為期 5 天之「央行與公共機構風險管理」國際工作研討會，與會者包括印尼、台灣、南韓、中國大陸、馬來西亞、越南、斯里蘭卡、尼泊爾、土耳其、約旦、哈薩克、馬爾地夫及巴布亞紐幾內亞等 13 國央行及存保機構人員等，約 50 人與會。

印尼央行為因應經濟金融快速變遷、科技發展及地震海嘯等天然災害之風險，加強政策有效性及人力資源品質，由所屬之 Bank Indonesia Institute 舉辦研討會，邀請 IMF 及印尼央行等學者專家擔任講師，除了介紹 IMF 提供會員國融資時之保障評估(Safeguard Assessments within IMF Lending Activities)，且廣泛討論央行面臨之財務及非財務等各類風險的評估及管理機制，以及資安防護等議題；並於會中分享印尼央行風險管理的經驗，提供與會者研析參考。

二、本文架構

本報告共分為六部分;除此前言外,第貳節說明風險及風險管理架構;第參節介紹中央銀行財務風險與非財務風險的管理;鑒於網路安全已成為現階段金融體系內最重要課題，且可能擴大聲譽風險及營運中斷風險的衝擊，另以第肆節說明網路風險管理；第伍節闡述印尼央行風險管理的經驗;第陸節則為心得與建議。

貳、風險與風險管理

一、風險的定義

「風險」係指損失的發生與何時會發生是無法確定，且損失發生之結果亦無法預料。根據美國反舞弊性財務報告委員會所屬發起組織委員會(COSO[1])的定義，在一特定時間內，一特定地點發生的事項可能帶來正面影響，也可能帶來負面影響，抑或兩者兼具。有負面影響之事項，代表風險，風險將阻礙價值之創造或侵蝕現有價值；具有正面影響之事項，代表機會，機會係一個事項發生對目標達成產生正面影響的可能性，可協助價值之創造或保持，或抵銷負面之影響。

由於世界情勢快速變遷，使得企業面臨日益複雜的不確定性，部分不確定性可創造機會，部分不確定性則成為風險，企業的價值可能因為這些不確定性而減損或提升，而企業風險管理讓管理階層能有效處理不確定性及其相關的風險與機會,使企業創造價值之能力提高。

[1] 1985 年美國會計協會(American Accounting Association, AAA)、美國財務主管協會(Financial Executives International, FEI)、美國會計師公會(American Institute of Certified Public Accountants, AICPA)、美國管理會計學會(Institute of Management Accountants, IMA)與國際內部稽核協會(The Institute of Internal Auditors, IIA)共同成立「不實財務報導全國調查委員會」(National Commission on Fraudulent Financial Reporting，通常簡稱為 Treadway Commission)，旨在解決當時日益嚴重的不實財務報導問題。嗣後，基於 Treadway Commission 的建議，由其贊助機構另外成立 COSO，整合各種不同的內部控制的概念及定義，處理 3 個相互關連的主題(企業風險管理、內部控制與嚇阻舞弊)。

二、COSO 風險管理架構

(一) 2004 年版「企業風險管理—整合架構」

2001、2002 年美國陸續爆發安隆(Enron)、世界通訊(WorldCom)、泰科(Tyco)、全錄(Xerox)及默克藥廠(Merck)等重大公司財報不實及管理失當的醜聞，2002 年 7 月美國國會通過沙氏法案[2](Sarbanes-Oxley Act of 2002)，強化財務報告資訊之揭露，並加重公司管理階層在財務報表與公司資訊揭露的責任。因應沙氏法案，2004 年 COSO 提出「企業風險管理—整合架構」(Enterprise Risk Management — Integrated Framework)，關注焦點擴大至風險管理的範疇，並逐漸成為各國政府及企業內部控制及風險管理參採應用的重要指引。

1. 風險管理的內容

風險管理之目的並不是消除風險，而是管理風險。管理階層為使企業創造最大的價值，應在謀企業之成長、報酬及相關風險間，取得最適平衡下，訂定策略及目標，並有效率分配資源。根據 COSO「企業風險管理—整合架構」，企業風險管理包括：

(1) 協調風險胃納(risk appetite)與策略：管理階層於評估策略方案、訂定相關目標及訂定管理相關風險之機制時，需考量風險胃納。

(2) 強化風險因應決策：企業風險管理能提供辨認及選擇各種風險因應方案之嚴格規範。風險因應方案包括：風險規避、風險降低、風險分擔及風險承受。

(3) 降低營運的非預期風險及損失：企業得以強化辨認潛在事項與決定如何因應的能力，降低非預期的營運風險及相關成本或損失。

(4) 確認並管理貫穿於企業之多重風險：所有企業的各個單位均面臨多重風險，出

[2] 美國參眾兩院於 2002 年 7 月底通過沙氏法案，由布希總統簽署生效。該法案係美國自 1930 年代制定證券交易法案以來，監督該國證券市場最重要的立法。此法案又稱「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.強化資訊揭露；3.提高對會計及審計之規範；4.提高對違法行為的處罰。

現相互關連的後果。企業風險管理能促使企業對該等後果作出有效及整合性的因應。

(5) 掌握機會：管理階層透過全面考量潛在事項，辨識機會並積極掌握。

(6) 改善資金配置：取得強而有力的風險資訊，使管理階層能有效評估整體資金需求，並改善資金配置。

因此，企業風險管理是一個遍及企業各層面的過程，該過程受企業董事會、管理階層或其他人士所影響。透過此一過程，企業制定經營策略，辨認可能影響企業價值的潛在因素，並管理企業面臨的風險，使其不超過企業所能接受或忍受的風險，以合理保證企業目標之達成。

2．企業風險管理之組成要素

企業風險管理包含下列 8 個相互關連組成要素，這些組成要素係管理階層經營企業之方式而發展出來，並與管理之過程相結合：

(1) 內部環境：包含形塑組織基調，並建立企業人員看待及處理風險的基礎，包括風險管理哲學、風險胃納、操守及價值觀等。

(2) 目標設定：必須先有目標，才能辨認影響目標達成的潛在事項。管理階層應設立制訂目標的流程，且選定的目標必須能支持企業的使命，並與企業的風險胃納一致。

(3) 事項辨認：企業必須辨認可能影響目標達成的內外部事項是屬於風險或機會，如為機會，則應設法導回制訂策略或目標的流程中。

(4) 風險評估：企業分析風險，考量其發生之可能性及影響，並藉以決定風險應如何加以管理。

(5) 風險回應：管理階層依據企業的風險胃納、風險回應的成本效益、可能性與衝

擊的降低幅度等，評估選用適當的風險回應方案(規避、承受、降低及分擔)。

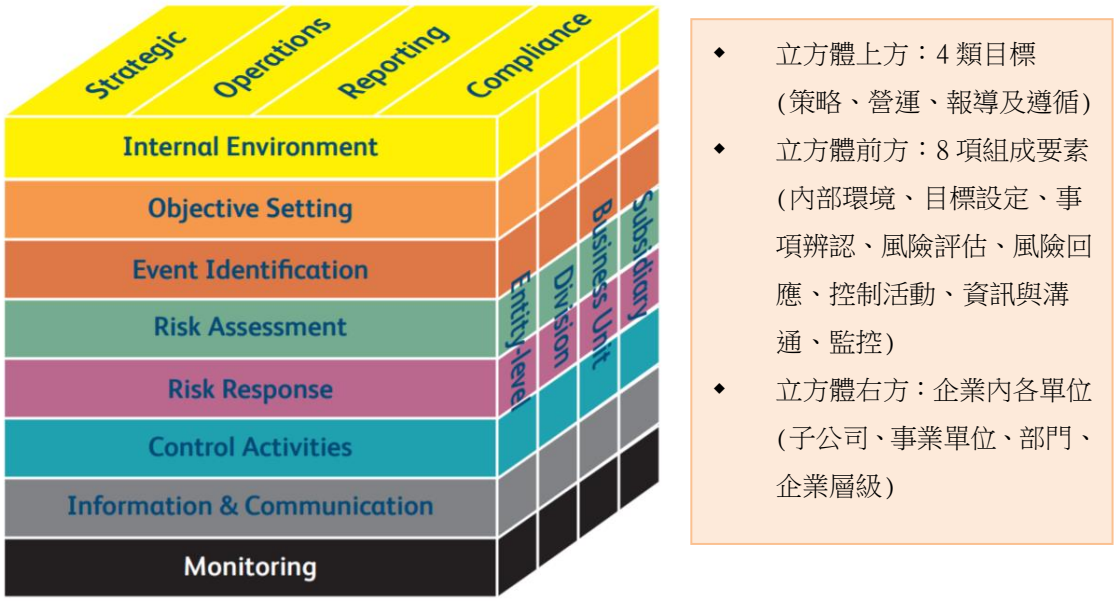
(6) 控制活動：用以協助企業確保風險回應及其他指示事項能有效執行的政策與程序，包含相關資訊技術控制措施。

(7) 資訊與溝通：攸關之資訊在一定的形式和期限內，予以辨認、蒐集並溝通，以確保相關人員能夠履行其職責。有效的溝通應該包含上下垂直及水平橫向等，以不同角度進行。

(8) 監控：企業風險管理各組成要素的有效性，可以藉由持續的監督活動、獨立的評估或二者並用的方式進行監督。

企業風險管理架構的組成要素是企業致力達成目標的必要因素。COSO 以立方體說明企業 4 類目標、8 項組成要素及組織單位等 3 個構面的企業風險管理架構(圖 1)。一個組成要素並不只是影響下一個組成要素，而是一個多方向，透過企業內各單位，且反覆進行的過程，彼此會相互影響。

圖 1　COSO 之 ERM 架構 (2004 年版)



- 立方體上方：4 類目標(策略、營運、報導及遵循)
- 立方體前方：8 項組成要素(內部環境、目標設定、事項辨認、風險評估、風險回應、控制活動、資訊與溝通、監控)
- 立方體右方：企業內各單位(子公司、事業單位、部門、企業層級)

資料來源：Institute of Risk Management (2018)

2. 2017 年版「企業風險管理—整合策略與績效」

2004 年迄今，由於業務與營運環境更加複雜、科技進步、利害關係人擴大參與及尋求更高層次的透明度與課責性，COSO 於 2017 年推出「企業風險管理—整合策略與績效」(Enterprise Risk Management—Integrating with Strategy and Performance，簡稱「新版 ERM」)，不再僅強調風險視角下的企業治理及管理要素，而是直接從企業治理和管理的角度提出將風險管理內容嵌入，試圖讓風險管理者從被動防禦轉變為主動出擊(管理)，使風險管理與價值創造的過程融為一體。

新版 ERM 核心內容由原有的 8 要素(圖 1)調整為 5 要素(治理與文化、策略與目標設定、執行風險管理、檢討與修正，以及資訊、溝通與報告)，並結合 20 項原則(圖 2)。

圖 2　COSO 新版 ERM 架構 (2017 年版)

資料來源：COSO (2018)

三、IMF 提供會員國融資時之保障評估

自 2000 年起，IMF 對其會員國提供融資時，採行保障評估措施，以確保取得 IMF 資源的央行能夠妥適管理資金並提供可靠資訊，降低 IMF 資源遭到濫用(Misuse)或提交錯誤資料(Misreporting)之潛在風險，維護其他會員國的資源可用性。

IMF 保障評估措施之治理架構涉及五大關鍵領域(ELRIC)，包含外部稽核機制(External Audit)、法律結構與獨立性(Legal Structure and Autonomy)、財務報告(Financial Reporting)、內部稽核(Internal Audit)與內部控制系統(System of Internal Controls)。若一國於 IMF 融資案的關鍵領域評估結果屬允當，且該國央行同意並適當執行 IMF 評估報告中相關強化措施的建議，則可辦理該筆融資協定。

自從 2000 年 3 月保障評估措施推出以來，截至 2018 年 8 月底，IMF 已完成涵蓋 96 個中央銀行的 307 項評估。IMF 認為，根據採行的保障評估經驗顯示，透過強化治理、控制及報告機制，已對央行運作產生正面影響。

參、中央銀行風險管理

中央銀行為金融機構，其風險管理與商業銀行等其他金融機構相近，在討論風險時，宜以一般銀行的風險管理標準及技術為起點，採取整合性的風險管理；然而，中央銀行屬決策機關，其地位及目標與以營利為基礎的機構不同，權責更為廣泛，其風險管理目標係建立一個架構，用於識別、監測及管理貨幣與金融機構政策執行時產生的風險，並促進外匯資產的最佳配置；中央銀行風險管理架構通常根據最佳市場慣例制定，採行企業風險管理，惟因其風險管理著重於目標的達成及公共服務的落實，旨在降低因執行政策操作所面臨之風險，避免聲譽受損，故與企業以保持競爭力及營業能力為風險管理核心不同。

中央銀行執行政策，承擔各種風險—包括財務風險(Financial risks)及非財務風險。各項財務風險與非財務風險可能彼此相互影響，例如，倘若政策及決策不當、作業失誤或財務損失，可能造成傷害中央銀行聲譽的風險。

一、財務風險管理

(一) 財務風險的範圍及管理目標

財務風險係與投資相關，即與金融資產負債管理有關的風險，包含市場風險[3] (Market risks)、信用風險[4] (Credit risks)、流動性風險[5] (Liquidity risks)及其他財務風險[6]等。由於金融創新，此類風險更為複雜，甚至呈現非線性特質，惟大部分關於財務風險的衡量方法已較成熟，中央銀行多可據以採行及管理相關風險。

財務風險管理的主要目標如下：

1. 促進財務可持續政策，維護中央銀行的可信度；

2. 保持足夠的財務實力，以執行核心業務及維持足夠的政策選擇，維護實現政策目標的能力；

3. 提高對公共資金的審慎及有效運用，保護中央銀行聲譽；

4. 提高內部及外部透明度，維持中央銀行自主性及政策溝通效果。

財務風險管理對中央銀行實現政策目標至關重要，同時保護中央銀行的聲譽、可信度及自主權。做為投資者，中央銀行傳統上趨於保守，在面臨風險與收益之間的權衡時，中央銀行傾向於持有信用風險較低、流動性較高的資產；然而，由於貨幣政策操作、確保金融穩定、維持安全有效率的支付制度等職責，以及外匯交易及投資活動(如外匯存底的運用)等業務，中央銀行仍須承擔多種風險。

[3] 因利率、匯率、股票及商品價格變動，造成財務部位暴險，導致遭受損失的風險。
[4] 因交易對手未能履行約定契約中的義務而造成經濟損失的風險。
[5] 指交易之一方因流動資金的不足，造成合約到期時，無法以合理成本及時獲得充足資金履行支付義務，造成損失的風險。
[6] 例如，因外幣部位暴險，導致預期鉅額匯率兌換損失等。

(二) 金融危機後，全球中央銀行財務風險評估與管理更為重要

金融危機期間，相對於民營企業減少暴險，中央銀行則在危機情況下承擔更多風險，造成資產負債表擴增，使其對財務風險的評估、控制及管理較以往更加重要：

1. 2008 年全球金融危機後，先進國家採行量化寬鬆貨幣政策(QE)，挹注市場資金，央行資產負債規模大幅擴增，結構亦發生變化。例如，金融危機前，美國 Fed 資產以美國公債為主；2008 至 2014 年因採行大規模資產購買計畫，增持美國公債及房貸抵押債券，並進行債券到期年限展延計畫，致面臨的信用風險及利率風險均上升。而負債方面，金融危機前，流通中的貨幣為美國 Fed 最大的負債項目；金融危機後，銀行準備金大增，反映 QE 政策效果及銀行體系投資不確定性上升。

2. 若干新興市場國家央行因應先進國家 QE 政策的外溢效果及匯率政策操作，外匯存底大幅擴增，故受國外利率及匯率波動的影響明顯增加；負債面則因沖銷操作，使得金融機構轉存款及債券發行增加，若國內利率相對較高，將造成央行國外投資所得收入不敷支應沖銷操作的利息支出。

而透過中央銀行資產負債表的分析，將有助了解其財務風險及財務實力。此外，獲利雖非衡量中央銀行表現的指標，惟營運損失恐導致外界質疑中央銀行履行政策目標的能力，並可能使其面臨政治壓力，影響中央銀行的自主性。

(三) 貨幣政策之財務風險控制

1. 中央銀行貨幣政策融通與商業銀行貸款之主要差異

中央銀行對金融機構融通所需採行之風險控制，與商業銀行辦理貸款類似，惟仍有部分差異，說明如下：

(1) 中央銀行融通利率之訂定，需考量政策因素，無法如商業銀行評估貸放利率係依交易對手與擔保品之品質而定。

(2) 基於貨幣政策操作規模龐大，須備妥完善之風險控制架構，以確保將風險降至最低。

2．風險控制架構，分為交易對手架構與擔保品架構，分述如下：

(1) 交易對手架構：主要關注交易對手信用風險，內容涵蓋融通對象之範圍、財務健全性(適足資本)、監管要求，以及基於審慎前提，限制某交易對手資格等。

(2) 擔保品架構：須關注擔保品之信用、市場及流動性風險等。

3．擔保品之風險減緩措施

中央銀行進行融通操作時，為降低可能承受的風險，須先決定本身可承受之最大風險容忍度，做為風險控制之基準，且由於風險高低取決於所接受之擔保品類型，相關風險減緩措施(risk mitigation measures)，可依據風險容忍度進行規劃，說明如下：

(1) 選擇合格擔保品：需考量擔保品市場性(即變現能力)、發行機構(公營或民營)、保證機構(公營或民營)或信評等級等因素。

(2) 定期估值並追加保證：定期依據市價或理論價格等資料，評估擔保品價值，確保融通金額不致高於擔保品價值，且為因應不同時期擔保品價值之變化，此項評估須經常(多為按日)進行，並於估值不足時追加徵提擔保品。

(3) 折扣率(haircuts)：訂定擔保品之折扣率，須考量擔保品本身之價格波動度，以及因交易對手違約，擔保品變現需時，可能對該等擔保品價格產生負面衝擊等影響因素，核給各項擔保品折扣率。此外，尚需額外追加折扣率，以因應估值不確定性或錯誤所衍生之風險。

(4) 集中度限制：為避免風險過度集中，針對個別交易對手之暴險額度，或由個別交易對手所提供之擔保品額度，應予設限。

前述針對擔保品之風險減緩措施，係基於避免中央銀行因融通操作而遭致風險，惟

中央銀行做為主管機關，亦需兼顧風險減緩措施可能對市場造成之後續效應，例如對該等擔保品之市場價值與供需情況等。

(四) 中央銀行做為最後融通者之財務風險控制

最後融通者操作係在市場發生系統性衝擊時，中央銀行須以較高利率計息，並徵提較佳之擔保品，向金融機構提供流動性；其目的在避免具償債能力，惟暫時欠缺流動性之金融機構陷入違約處境，進而對市場造成損害。

最後融通者之架構，須先定義合格之融通對象(如銀行等金融機構)、擔保品、融通標準、利率等，並強化對接受融通者之監視，以及申請緊急流動性支援之程序等；此外，提前演練亦為重要一環。

另為確保不致因執行政策而遭受財務風險，中央銀行內部決策架構須謹慎為之。因此，相關決策層級須提高至高階主管(另為合乎適法性、申報要求及降低風險，需納入財務風險管理與法律部門，本次研討會講師 Matevz Zbasnik 建議透過工作小組或委員會形式運作)，並由貨幣政策執行部門進行操作。

二、非財務風險管理

(一) 非財務風險的範圍

非財務風險包括策略風險[7](Strategic risks)、聲譽風險[8](Reputation risks)及營運風險(Operational risks，或稱「作業風險」，以下稱「作業風險」)等。其中，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的風險」。例如，IT 中斷、數據外洩、擔保品管理疏失、人員舞弊、未經授權的交易、恐怖攻擊、天災等因素所造成的風險。

由於作業風險常涉及內部問題，若控管不當，可能導致財產及機關聲譽嚴重損傷。

[7] 係因政策設計或執行的無效率，所產生不利影響的風險。
[8] 係指因外界負面評價而造成損失的風險。

最著名的例子為1995年英國霸菱銀行尼克李森(Nick Lesson)因操作衍生商品失利及內部控管不當，造成約8.6億英鎊的虧損，為整個集團淨值3.36億英鎊的2倍多，最後霸菱以1英鎊的象徵性價格，被荷蘭國際集團(ING)收購；2018年12月摩根大通亦因不當處理預發行美國存託憑證(ADR)，與美國證券交易委員會(SEC)達成須支付超過1.35億美元的和解協議[9]。

(二) 網路傳播已擴大聲譽風險及營運中斷風險的負面影響

全球金融危機後，財務風險管理對中央銀行益加重要的同時，非財務風險的管理更不容忽視。事實上，根據世界經濟論壇(World Economic Forum)發布之2018年全球風險報告，極端氣候、自然災害、網路攻擊等風險的發生機率及影響力均為最受關注之所在，而資料詐欺或竊取的發生機率亦不容忽視(圖3)。

另根據Aon Risk Services全球風險管理調查[10]，品牌與聲譽受損已連續兩次成為調查中排名第一的新興風險，數位科技風險亦愈來愈受重視(圖4)，而營運中斷則持續維持在前10大風險之列。對政府部門而言，前3大風險依序為：1.聲譽受損；2.網路犯罪、駭客攻擊、資訊病毒、惡意代碼；3.未能吸引或留住頂尖人才。

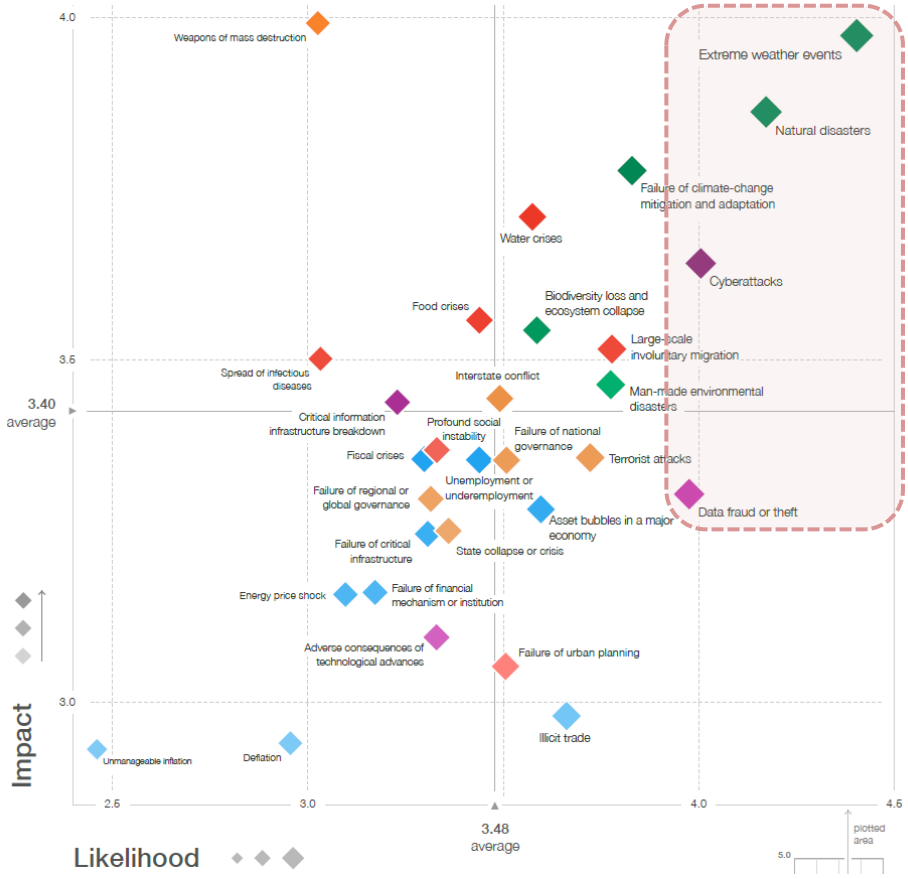
值得注意的是，儘管過去幾年間，產品缺陷、詐欺性商業手法或腐敗仍為商譽毀壞的主要因素，但在網路傳播的推波助瀾之下，已使得聲譽風險造成的負面影響被進一步擴大，使得企業更易遭受聲譽風險的衝擊。同時，網路犯罪也不再只是盜取個資或信用卡資料，其威脅已擴大至生產線中斷、阻止客戶下訂單等營運中斷的損害。

---

[9] 包括超過7,100萬美元的非法獲利、1,440萬美元的判決前利息及4,970萬美元的罰款，支付總額超過1.35億美元。詳U.S. Securities and Exchange Commission (2018)。

[10] 本報告每兩年發布一次，蒐集全球60個國家、33類產業，大、中、小型公司共1,843位風險決策者之意見，以洞悉各地區及各行業風險管理之觀念與做法。

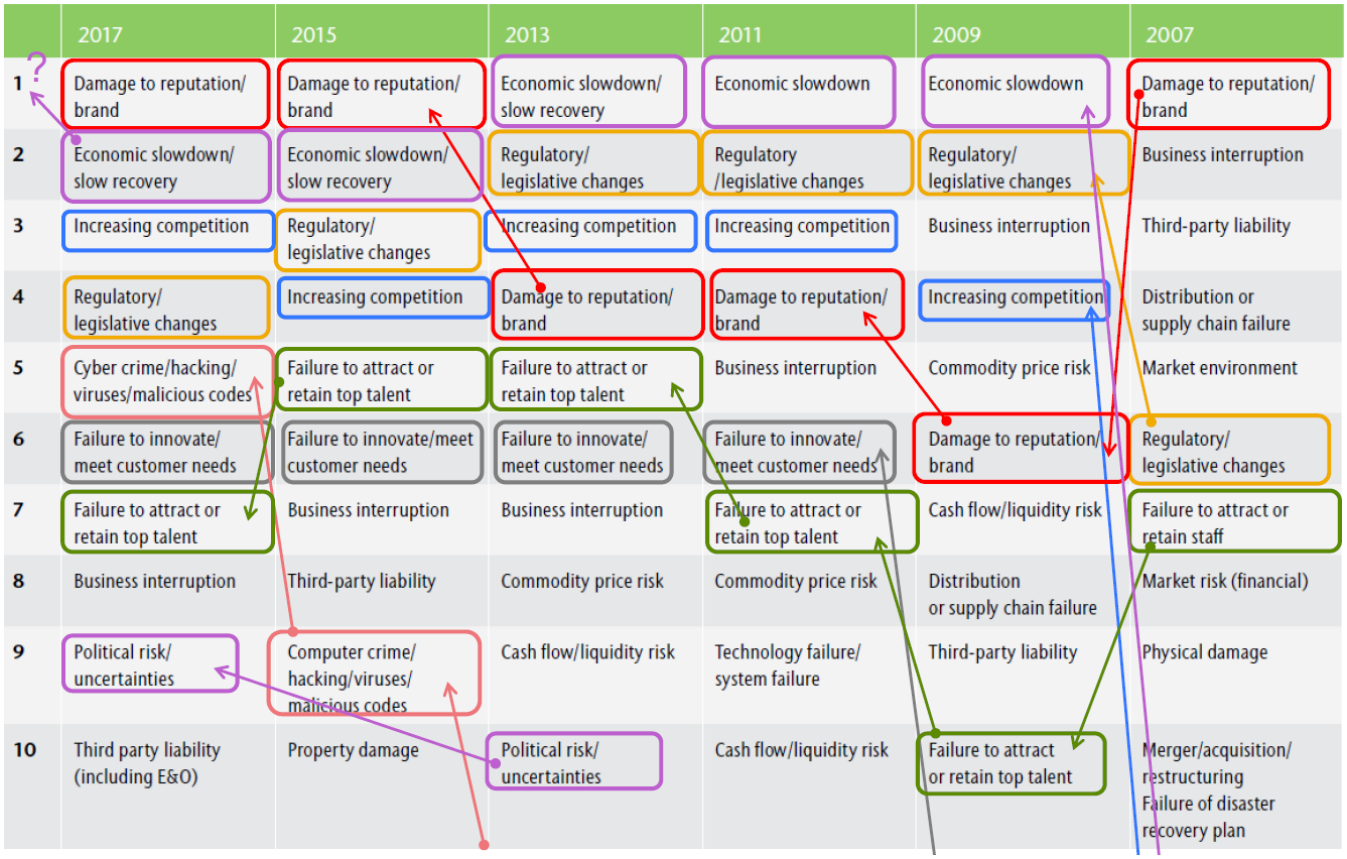
圖 3　2018 年全球風險概況



資料來源：World Economic Forum (2018)

全球化及網路無遠弗屆之下，許多新驅動因素，特別是網路風險及網路攻擊，正在改變傳統風險，賦予舊有挑戰全新的緊迫性及複雜性，本報告將於第肆章節進一步說明。

圖 4　全球前 10 大風險趨勢



	2017	2015	2013	2011	2009	2007
1	Damage to reputation/ brand	Damage to reputation/ brand	Economic slowdown/ slow recovery	Economic slowdown	Economic slowdown	Damage to reputation/ brand
2	Economic slowdown/ slow recovery	Economic slowdown/ slow recovery	Regulatory/ legislative changes	Regulatory /legislative changes	Regulatory/ legislative changes	Business interruption
3	Increasing competition	Regulatory/ legislative changes	Increasing competition	Increasing competition	Business interruption	Third-party liability
4	Regulatory/ legislative changes	Increasing competition	Damage to reputation/ brand	Damage to reputation/ brand	Increasing competition	Distribution or supply chain failure
5	Cyber crime/hacking/ viruses/malicious codes	Failure to attract or retain top talent	Failure to attract or retain top talent	Business interruption	Commodity price risk	Market environment
6	Failure to innovate/ meet customer needs	Failure to innovate/meet customer needs	Failure to innovate/ meet customer needs	Failure to innovate/ meet customer needs	Damage to reputation/ brand	Regulatory/ legislative changes
7	Failure to attract or retain top talent	Business interruption	Business interruption	Failure to attract or retain top talent	Cash flow/liquidity risk	Failure to attract or retain staff
8	Business interruption	Third-party liability	Commodity price risk	Commodity price risk	Distribution or supply chain failure	Market risk (financial)
9	Political risk/ uncertainties	Computer crime/ hacking/viruses/ malicious codes	Cash flow/liquidity risk	Technology failure/ system failure	Third-party liability	Physical damage
10	Third party liability (including E&O)	Property damage	Political risk/ uncertainties	Cash flow/liquidity risk	Failure to attract or retain top talent	Merger/acquisition/ restructuring Failure of disaster recovery plan

資料來源：林高輝 (2017)

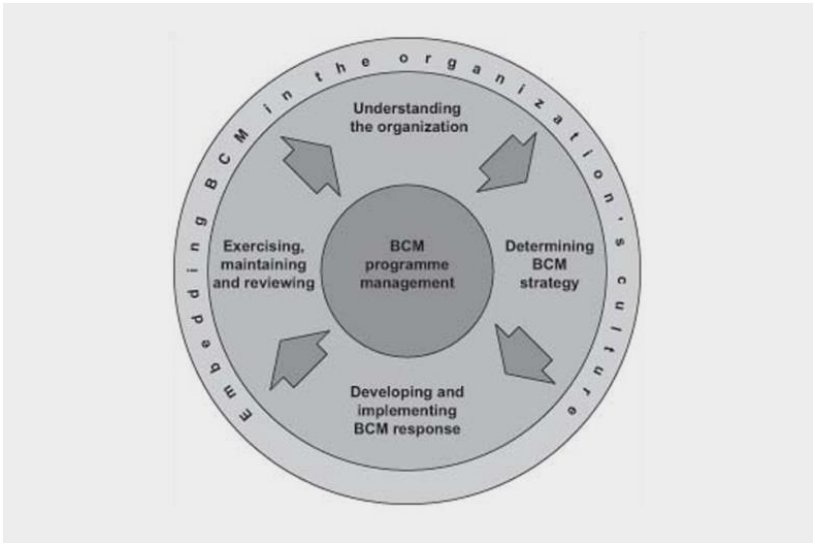
(三) 天災人禍頻仍，營運不中斷的風險管理持續受重視

歷經 SARS 疫情、美國 911 恐怖攻擊事件、日本 311 震災、印尼蘇拉維西島大海嘯等重大災害，以及人類對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，造成政府或企業營運的不確定性大幅提高，致使災害防治、營運不中斷管理(Business Continuity Management，簡稱 BCM)益受重視。

中央銀行提供並維護支付清算系統等重要的基礎建設施，處理金融市場交易及零售支付交易所涉及之銀行間資金之移轉，且促進金融穩定、健全銀行業務亦多為其經營目標，因此營運不中斷風險的管理與規劃有其重要性，避免一旦主要業務發生營運中斷，無法迅速有效應變處理，將損及形象與聲譽。

BCM 為持續性、週期性的管理工作，每一週期包含 4 個步驟：(1)了解組織，(2)決定營運持續管理策略，(3)發展與實行營運持續管理，以及(4)營運持續管理演練、維護與稽核(圖 5)，並將 BCM 深植於組織文化中，其目標係避免企業組織營運活動的中斷，透過實施營運持續計畫，並結合各項預防及復原的控制措施與程序，增長企業的復原能力。其方式為：辨識可能造成企業營運中斷的潛在衝擊、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。

圖 5　BCM 週期



資料來源：U.K. Cabinet Office (2012)

- **了解組織**
  - ✓ 分析營運上的衝擊
  - ✓ 風險判斷與控制
- **決定 BCM 策略**
  - ✓ 組織決策
  - ✓ 包括復原時程目標的復原活動
  - ✓ 與主要股東與外部機構的關係管理
- **發展與實施 BCM**
  - ✓ 事故回應架構
  - ✓ 事故與復原的管理計畫
  - ✓ 溝通
  - ✓ 公共及媒體關係
- **演練、維護和審查**
  - ✓ 計畫驗證
  - ✓ 目的導向及隨時更新
  - ✓ 持續改善
  - ✓ 修正計畫
  - ✓ 預防行動

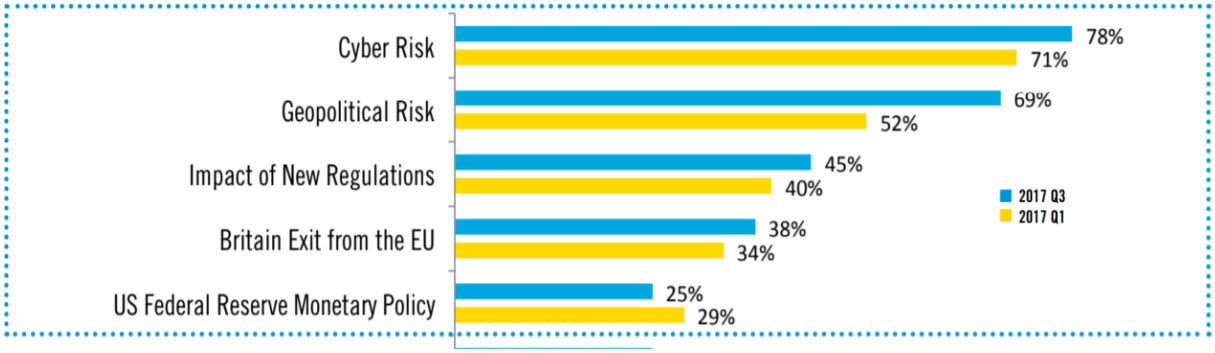
氣候變遷、地震、海嘯及人為事故等帶來的風險對營運中斷的損害已更加頻繁，因此，若可預先制定並健全營運不中斷及復原計畫，將可提升面臨營運中斷時的韌性。

肆、網路風險管理

2017 年 3 月，20 國集團(G20)財長與中央銀行總裁會議後表示，「資通訊技術(ICT)之惡意使用，可能破壞各國國內與國際金融體系中之重要金融服務，削弱安全防護與信

心，進而危及金融穩定」[11]。此外，美國集中保管結算公司(Depository Trust & Clearing Corporation, DTCC)針對系統性風險所進行之問卷調查結果[12]認為，網路風險(cyber risk)為 2018 年最主要風險(78%)，其次為地緣政治風險(69%)、新規範衝擊(52%)、英國脫歐(38%)及美國貨幣政策(25%)等(圖 6)。顯見網路安全已成為現階段金融體系內最重要課題。

圖 6 DTCC 系統性風險問卷調查結果



資料來源：DTCC（2018）

一、網路風險及網路攻擊

網路風險係指因資訊系統遭到破壞或攻擊而造成的傷害或損失；更廣泛的定義為組織內因技術性基礎設施或技術應用，所導致之可能損失或損害。其風險來源可分類如下：

(一) 內部惡意：員工或其他內部人員蓄意破壞、盜竊或其他瀆職行為。

(二) 內部無意：員工或其他內部人員因人為疏失，導致損害或損失。

(三) 外部惡意：係來自外部(如犯罪集團或駭客等)之計劃性攻擊，為最常見之網路風險來源。

(四) 外部無意：因外部非故意所導致之業務損失或損壞。例如，第三方合作夥伴遭遇技術問題，或是天然災害，均可能影響系統可用性。

近期針對中央銀行之網路攻擊事件(屬外部惡意)，主要集中於歐美與新興國家。其

[11] G20 (2017)。
[12] DTCC (2018)。

中，歐美等國中央銀行面臨之網路攻擊型態，包括資料外洩(如美國與義大利)與營運中斷(如挪威、瑞典)等事件；新興國家部分則多為詐騙事件(表 1)。

表 1　近年各國中央銀行面臨之網路攻擊案件

機關名稱	年度	型態	說明
Fed Cleveland	2010	資料外洩	遭盜 122,000 張信用卡資料。
Fed New York	2012	資料外洩	私有軟體密碼遭盜，損失 950 萬美元。
瑞典央行	2012	營運中斷	分散式阻斷服務(DDoS)攻擊*，網站中斷 5 小時。
厄瓜多爾央行	2013	詐騙	設於該行之帳戶遭盜 1,330 萬美元。
Fed Saint Louis	2013	資料外洩	4,000 名美國銀行高級主管資料遭到匿名公布。
史瓦濟蘭央行	2014	詐騙	遭盜 68.8 萬美元。
歐洲央行	2014	資料外洩	20,000 個電子郵件地址與聯繫資料外洩。
挪威央行	2014	營運中斷	DDoS 攻擊 7 家大型金融機構，導致服務中斷 1 天。
亞賽拜然央行	2015	資料外洩	數千名銀行客戶資料外洩。
孟加拉央行	2016	詐騙	透過 SWIFT 自該行設於 Fed New York 之帳戶轉出 8,100 萬美元。
俄羅斯央行	2016	詐騙	21 次網路攻擊，目的為自該行之代理行帳戶竊取 5,000 萬美元，最終損失 2,200 萬美元。
義大利央行	2017	資料外洩	兩名前高級主管之電子郵件帳號遭駭。

註：*係透過大量合法或偽造的請求，占用大量網路及器材資源，以達到癱瘓網路及系統之目的。

資料來源：Bouveret (2018)

二、網路風險控制

國際上對於網路風險控制，尤其是資訊安全控制，尚無一致性作法可供參考，另根據 BCBS(2018)提及有關網路風險控制範例，應可供作相關作業之參考(表 2)。

表 2　網路風險控制範例

控制目的	控制項目說明	控制措施範例	測試方法範例
進入(access)與存取權限僅限已取得授權之人員	基於工作角色與最低權限原則授權	用戶身分識別與驗證、人員控管與訓練	社交工程測試
	身分驗證(強度與資訊敏感性相當)	密碼政策、系統驗證控制	查核使用者進入情況
	未經授權者不得進入	防火牆、路由器、分隔網路	滲透性測試[1]
	保護系統不受惡意攻擊	反惡意軟體、網站及電子郵件過濾	非功能性測試[2]
	未授權者不得進入與使用系統間聯繫管道	加密、關鍵項目管理	審查關鍵項目管理
偵測未授權之進入與使用情況	適時偵測未經授權進入與使用系統之情況	日誌、安全防護訊息與事件管理、監控攝影機、侵入偵測、事件分析及作業程序升級等	滲透性測試、紅隊測試[3]
對未授權進入與使用之回應	有序回應資安事件	資安事件回應指南、危機處理、營運不中斷計畫	桌上(tabletop)演練、公私共同演練
最大限度延長正常運作時間之系統設計	系統能夠處理個別組件(component)失靈問題	沙盒解決方案、零信任架構[4]	Chaos Monkey testing[5]、架構審查、failover testing[6]
盡可能恢復運作	以備份(不會受到同一網絡事件影響的方式存儲)恢復運作	復原計畫、安排及測試	技術性恢復運作測試
透過極小化新脆弱性(或安全漏洞)，並採取措施減緩相關風險，以降低脆弱性	實施控制措施，以盡量降低因系統變更產生的新脆弱性	安全軟體開發，非功能性測試、變更控制、系統強化	控制變更審核、代碼掃描、架構審核
	及時找出新脆弱性並修復	修補(patching)	脆弱性掃描、滲透性測試、模糊測試[7]

控制目的	控制項目說明	控制措施範例	測試方法範例
	及時找出新威脅並修復	網路情報、資安策略	個別性能審查
監管與監督(治理)網路安全	決策者充分瞭解網路風險控制，並適度監督業務	報告、治理會議、內部審計、確保獨立性、諮詢審查	治理審查

註：1.係以駭客思維試圖入侵網站、資訊系統及設備等，以找出各種可能的漏洞進行驗證，並評估資訊系統與硬體安全性。

2.用於驗證系統(例如內存資料及性能)之測試技術。

3.從攻擊者角度出發，找出各種可以入侵企業管道的作法。

4.指安全概念與威脅模型，即任何嘗試連接到系統者應先經過驗證。

5.係模擬測試軟體工具。

6.此類測試用以驗證系統分配額外資源，並將操作移動到備份系統的能力。

7.用於檢測軟體或電腦系統安全漏洞(脆弱性)之軟體測試技術。

資料來源：BCBS（2018）

三、網路風險管理規範

近年來由於網路風險持續升高，各國金融監理機關為減緩該等風險對金融體系之衝擊，相繼發布金融機構之網路風險管理相關規範。為瞭解前述規範之發展趨勢，以下概述有關美國與香港等地金融監理機關新近發布之金融機構網路風險管理規範(或草案)及相關措施，以供本行與國內金融監理機關擬訂相關政策參考。

(一) 美國聯準會、貨幣監理署及聯邦存款保險公司[13]

2016 年 10 月共同發布「強化網路風險管理標準」(Enhanced Cyber Risk Management Standards)草案[14]，規範對象為具一定規模以上之國內外金融機構與相關第三方業者，有關網路風險管理之重點整理如下：

1. 網路風險治理：本項管理重點在於，網路風險管理應整合為公司治理之一部分。

[13] Board of Governors of the Federal Reserve System、Office of the Comptroller of the Currency 及 Federal Deposit Insurance Corporation。

[14] 本草案公開徵求業者意見之期限(2017 年 2 月 17 日)已屆，惟尚未發布最終版本。

因此，要求適用機構應訂定涵蓋機構整體營運範圍之網路風險管理策略，並經理事會通過。再者，要求該等機構之網路風險管理架構，應納入政策與通報單位，以及獨立之風險管理單位與內部稽核單位，以協助並執行前述策略；另亦須在前述架構內，納入有關辨識與回應網路事件之機制，並進行測試，且視情況適時更新。

2. 網路風險管理：網路風險管理整合為業務部門(定期評估風險並報告)、獨立風險管理(以企業整體為範圍進行偵測並回報)，以及內稽單位(於稽核業務內納入網路風險管理策略之有效性評估)等 3 類。

3. 內部依存管理：內部依存係指適用機構賴以提供服務、資訊交流與聯繫之資產(包括勞動力、資訊、技術及設施)。內部依存管理要求以機構整體做為管理基準，確保持續評估並提升與內部依存有關之網路風險管理。再者，為對內部依存有最新且全面性的認識，適用機構須就內部資產及其業務功能列表並持續追蹤，進而建立並採行適當的控制措施；有關列表追蹤之作業程序說明如下：

   (1) 先行評估資產及其作業環境的網路風險(使用該項資產之前)。

   (2) 資產生命週期內持續監控資產及其作業環境。

   (3) 評估資產相關網路風險。

4. 外部依存管理：外部依存係指適用機構與賣方、供應業者、客戶及公用事業(如電力與電信)等外部組織或服務提供者(該適用機構賴以提供服務、資訊交流與聯繫者)間之關係。外部依存管理相關策略與前述內部依存管理類似，均需以適用機構整體考量，並持續評估相關風險管理。此外，須具備辨識與即時監控相關網路風險之能力，並就各關係業者採行適切之控制措施，例如審視外部關係、定期測試替代解決方案等。

5. 事件回應、網路防禦及情況認知：此項管理目的在確保適用機構針對網路事件

所引發之營運中斷，已備妥相關回應計畫，以減緩衝擊並自事件中快速恢復運作，進而強化本身及金融部門之網路復原能力。據此，要求該等機構須訂定機制，以因應營運中斷事件(尤其指同時發生多起事件、廣泛性中斷，或網路攻擊重大基礎設施事件等)。再者，對於關鍵資料之保存，應訂定相關規範，以確保該等資料之機密性、不可竄改及離線保存等。

(二) 香港金管局

2016 年 5 月公布網路防衛計畫(Cybersecurity Fortification Initiative, CFI)，內容主要為三大支柱，包含網路防衛評估架構 (Cyber Resilience Assessment Framework, C-RAF)、專業培訓計畫(Professional Development Programme, PDP)及網路風險資訊共享平台(Cyber Intelligence Sharing Platform, CISP)。其中 PDP 及 CISP 已陸續於 2016 年底開始實施，而網路防衛評估架構則分階段實施(最晚須於 2018 年底前完成)。

1. C-RAF：旨在評估機構之網路風險概況及防範網路攻擊所需具備之能力，並供金管局瞭解個別機構及銀行體系之應變準備概況。相關評估架構說明如下：

   (1) 自身風險程度評估(Inherent Risk Assessment)：根據所使用之科技、服務管道、提供之商品與服務、組織特性及歷史紀錄(防禦網路攻擊)等因素，評估本身之網路風險狀況，並以「高」、「中」、「低」3 種級別顯示風險程度。

   (2) 成熟度評估(Maturity Assessment)：根據自身風險程度之評估結果，訂定成熟度目標，並評估實際成熟度，其間差距則擬定改進計畫以提升成熟度。

   (3) 風險資訊主導之網路攻擊模擬測試(Intelligence-led Cyber Attack Simulation Testing)：根據最新或特定的網路攻擊風險資訊，實地模擬網路攻擊，以測試機構之網路防禦能力；凡自身風險程度評估等級屬「中」或「高」之機構，需進行本項模擬測試。

2. PDP：係金管局與香港銀行學會及香港應用科技研究院合作，推出網路安全從業人員之認證計畫與專業培訓課程。

3. CISP：金管局與香港銀行學會及香港應用科技研究院合作成立該平台，經由蒐集資訊提供分析(網路風險分析報告與建議)，並分享相關資訊予參加機構，以強化機構間之合作，提升全體銀行業之網路防衛能力。

伍、印尼央行之風險管理

由於印尼天災與人為攻擊(如恐怖攻擊、資安攻擊等)事件頻傳，印尼央行極為重視風險管理，除訂定風險管理相關規範外，並為強化三道防線機制，自 2016 年起整合風險管理與內部稽核作業，且以風險圖像(risk profile)與風險控制矩陣(risk control matrix)等形式，進行風險評估。

一、發展概況

印尼央行風險管理業務相關之發展概況與未來規劃藍圖說明如下：

(一) 1994-2002：成立風險管理單位(risk management unit)，以評估所面臨之市場風險、信用風險、流動性風險及經營績效，並對交易對手績效與信用風險進行評估；於公開市場操作科(Money Market Operation Division)下設置風險管理組(Risk Management Group)。

(二) 2003-2011：將企業風險管理(Enterprise Risk Management, ERM)概念[15]導入風險管理業務，並透過 SIMROIS[16]通報相關風險樣貌。

(三) 2012-2015：成立風險管理處(Risk Management Department)，其職責包括提出風險評估與建議、針對採購作業採行四眼原則(four eyes principle)[17]、

[15] 係結合企業策略設定與執行，且供企業用以管理風險，進而創造、保存及實現價值之企業文化、技能及實務；而非僅指某項功能、部門或檢核清單。
[16] 為該行 ERM 資訊系統。
[17] 四眼原則係指某項交易需經由 2 人以上之核准。

審視法遵與投資績效、控管作業風險、執行營運不中斷管理與內部控制，以及評估有關貨幣與準備金管理之新興金融工具等；成立宗旨在整合 ERM、貨幣政策、外匯準備相關之風險管理業務，並強化法規架構，實施三道防線機制。

(四) 2016-2018：擬訂風險胃納聲明，並成為 International Operational Risk Working Group(IORWG)會員。

(五) 2019-2024：提升風險管理成熟度評級(maturity level)，並達到國際風險管理最佳等級(如 COSO2017、ISO22301 等)。

二、風險管理準則

為使內部各層級於執行風險管理時能取得一致性，該行訂定以下 5 項風險管理準則(表 3)，做為內部執行之參考。

表 3　印尼央行風險管理準則

目標	須具獨立性，排除利益衝突，並輔以明確的任務、組織、系統及職責。
衡量	以系統化方式，預估風險之不確定性(透過可得之最適資訊及成本效益分析)。
動態	對任何環境或事件變化隨時做出回應，並有能力配合改善。
整合	制定及執行印尼央行之策略性政策、營運政策及營運活動時，應與風險管理進行整合。
附加價值	風險管理應有助於達成印尼央行之願景與任務(保障該行與社會大眾之利益)。

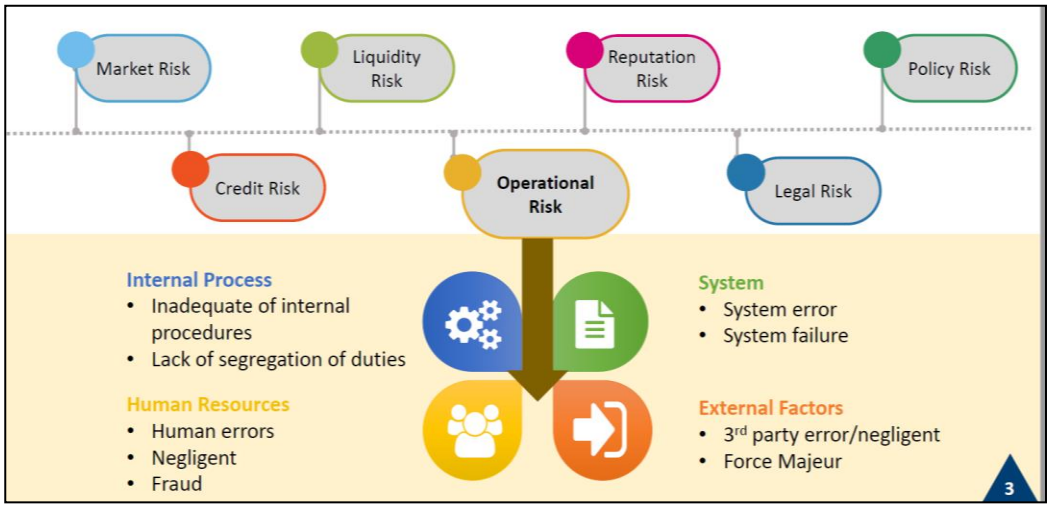
資料來源：本次研討會簡報資料

三、風險範疇

印尼央行風險範疇包含財務風險(市場風險、信用風險及流動性風險)與非財務風險

(作業風險、聲譽風險、法規風險及政策風險)；其中，作業風險可能源自內部作業程序(不合適之內部程序、責任劃分不夠明確等)、人力資源問題(人為疏失、忽視、瀆職等)、系統(系統錯誤、失靈等)及外部因素(第三方錯誤/忽視、不可抗力事件)等(圖 7)。

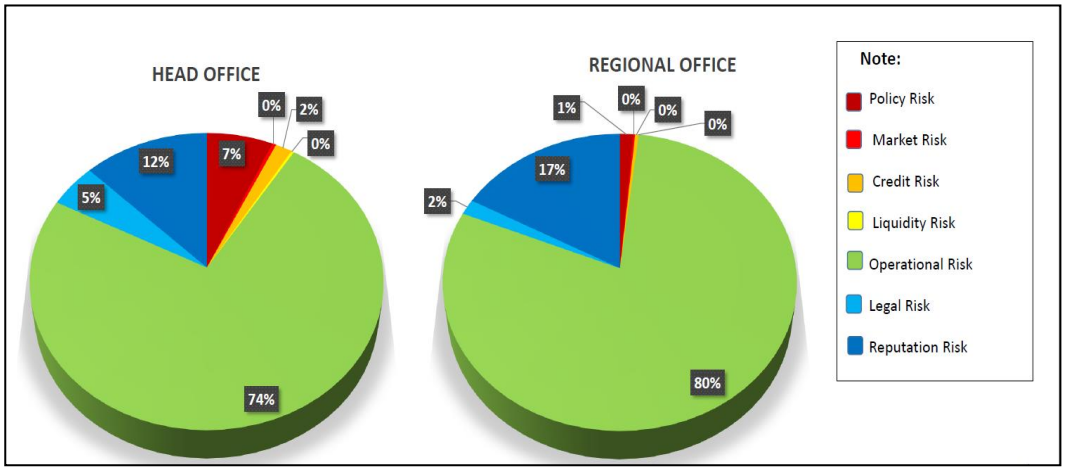
圖 7　印尼央行風險範疇



資料來源：本次研討會簡報資料

另觀察該行 2018 年之風險圖像，其中影響最大之風險類別為作業風險(占總行 74%，占地區分行 80%)，其次為聲譽風險(圖 8)。

圖 8　印尼央行風險類別



資料來源：本次研討會簡報資料

四、風險管理架構

印尼央行之風險管理架構，係由該行理事會主導政策方向，再由各業務單位共同參與風險管理會議(Risk Management Forum)，就相關業務提出建議，俾憑執行三道防線機制，其風險管理項目如表 4，相關架構說明如後：

表 4 印尼央行風險管理項目

項目	內容	說明
策略性政策	風險偏好聲明	該聲明須經理事會核可，再據以訂定各業務部門之營運風險指引
營運政策	風險限制與容忍度	設定風險上限與容忍度，供各業務部門遵循
風險管理實務	三道防線	包括風險辨識、衡量、回應與控制、監視及報告等5道程序
事件處理與營運不中斷	未遂事件、復原目標時程、營運不中斷計畫	須確保營運活動(尤指核心業務)能持續運作

資料來源：本次研討會簡報資料

(一) 理事會：為該行 ERM 訂定方向與政策，發布風險胃納聲明，並承諾支持該行企業風險管理任務，以及強化風險意識。

(二) 風險管理會議：各業務單位共同參與討論，並就理事會通過之 ERM 策略議題，提出相關建議。

(三) 三道防線機制

藉由三道防線機制(流程詳如圖 9)，提高各風險管理層級之對話並深化分析，以監視各種可能風險，促進整體風險管理之有效性。

1. 第一道防線

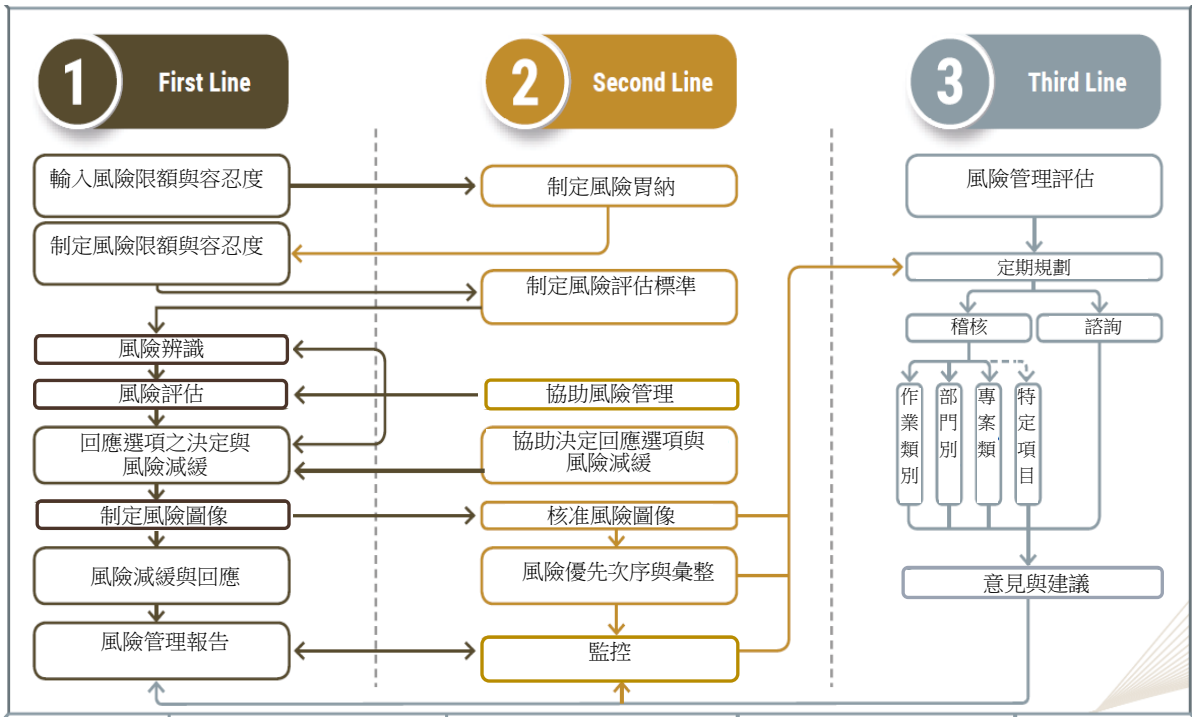
由各營運單位負責執行，任務包括擬定風險限額與風險容忍度、風險辨識、評估、

選擇風險控制之回應措施、監控及報告風險樣貌等；另為提升風險管理之有效性，須由內控人員(Internal Control Officer, ICO)[18]進行監控並提供諮詢，協助營運單位落實本階段風險管理任務。

2. 第二道防線

係由獨立運作之風險管理單位負責執行，並透過協調、核准及整合風險管理作業，形成第二道防線。主要任務在擬定風險胃納聲明與風險評估標準及核准風險圖像等。在財務風險方面，需監控有關外匯準備投資與貨幣政策操作等業務，並提供諮詢與評估；非財務風險方面，需進行作業風險評估；此外，亦須遵循「四眼原則」機制運作；在營運不中斷管理方面，研擬營運衝擊分析(business impact analysis)與危機應變作業，並進行模擬演練，另亦須為相關基礎設施備妥所需資源(如人員、設施等)。

圖 9　印尼央行三道防線機制



資料來源：Bank Indonesia (2018)

[18] ICO 扮演之角色與職責包括(1)風險管理諮詢、(2)促進各營業單位之風險管理、(3)與風險管理處協調、(4)監控單位內部自我評估作業。

3. 第三道防線

由定期評估風險控制有效性之稽核單位負責執行,包括對營運作業之風險控制作業進行測試，以及規劃與執行風險基礎之內部稽核制度(Risk Based Internal Audit, RBIA)[19]。

(四) 風險管理程序

印尼央行的風險管理程序分為風險辨識、衡量、回應與控制、監視及報告等 5 道程序如表 5。

表 5 印尼央行風險管理程序

程序	說明
辨識	風險識別是自上而下(top down)與自下而上(bottom up)之過程，用於偵測、識別及描述影響目標達成之風險性質、來源及成因。
衡量	風險衡量決定風險發生之可能性、衝擊程度與速度，並檢視所需的控制作業。
回應與控制	風險處置，以及透過自我衡量控制與自我衡量風險等作業，進行風險評估。
監視	檢視風險容忍度與限制，控制相關計畫，以及對未遂事件與損失事件建檔。
報告	風險圖像報告、風險控制矩陣、未遂事件與損失事件說明等。

資料來源：本次研討會簡報資料

五、營運不中斷管理

印尼央行遵循 ISO 22301[20]國際標準，執行營運不中斷管理，並於理事會下設立營

[19] RBIA 係有關治理、風險管理及控制的稽核方法，用以確保風險不致超出所設定之目標。
[20] ISO 22301 係以營運不中斷管理(Business Continuity Management, BCM)為主題之國際標準。

運不中斷管理工作小組，負責聯繫及推動相關工作。該行營運不中斷管理之目標，在於對可能造成重要工作中斷之事件，提高認知、警覺及準備，並在優先考量重要工作場所人身安全之前提下，建立該行服務的復原能力，以避免或降低事故發生時之衝擊。營運不中斷管理涵蓋範疇包括人員救援、確保關鍵任務之持續運作，以及尋求可用之資源(場所、設備、人員及技術等)，其基本運作原則及營運不中斷計畫(Business Continuity Plan, BCP)概述如下：

(一) 營運不中斷管理之基本運作原則

1. 優先考量人員安全防護。

2. 理事會與員工積極參與。

3. 確保一致性與持續性。

4. 因應須迅速、適當、整合及協調。

5. 優先復原關鍵工作。

6. 整合為該行風險管理之一環。

7. 備妥所需資源。

(二) 擬訂執行營運不中斷管理之 BCP

1. 計畫內容

(1) 關鍵任務：如關鍵營運單位、支援性質之業務單位(負責危機發生時之聯繫工作)，以及執行 BCP 與啟動關鍵任務人員。

(2) 關鍵設施：包括關鍵資訊系統之業務單位與災難復原計畫(disaster recovery plan)等。

(3) 人員安全與維安：包括人力資源與後勤單位，以及緊急應變計畫(emergency response plan)等。

2. BCP 擬訂後須經由實地測試、演練、檢討及改善，以確保屆時相關作業之順行，測試項目包括針對重要營運場所進行消防演練、模擬地震疏散作業，以及關鍵應用服務、理事會會議之基礎設施、替代營運場所之測試演練等。

陸、心得與建議

一、心得

(一) 各國中央銀行逐漸重視內部風險管理

經詢問此次與會之央行學員，部分表示近年其機構已針對內部風險管理成立專責單位或人員，以因應現階段快速變化之外部環境(天災、經濟金融環境變化、恐攻與資安攻擊事件等)與內部管理需求(避免人為作業誤失、瀆職等)。尤其近年資安事件頻傳，其攻擊規模與速度與日俱增，為避免受到相關事件之影響，各國中央銀行有必要維護業務運作及本身聲譽，進而維持金融穩定，因此，內部風險管理之重要性已逐漸升高。

(二) 整合中央銀行風險管理、危機處理及營運不中斷等計畫，俾能採行妥善措施因應，降低衝擊

風險管理屬事前預防，而危機處理與營運不中斷計畫係供事件發生之因應處置，三者宜相互配合呼應。透過關注重大危機事件之因應與發展，配合優化相關風險管理與緊急應變機制，以及模擬各種危機情境，進行衝擊分析與後續處置，加以營運不中斷計畫之補強與演練，方能於危機事件發生時，及時有效因應，降低所受衝擊。

(三) 資安防護有賴資訊分享

網路科技傳播的推波助瀾，已加大網路風險對聲譽風險的負面影響，且網路攻擊及電腦病毒亦擴大營運中斷的風險。為防止資安攻擊事件發生並降低衝擊，建立全面性或依個別產業或部門別之資訊分享中心，有其必要性；且基於個別機構/公司於遭遇攻擊時不願暴露本身弱點，將有礙資訊分享，爰建置國家層級資訊分享與分析中心，應可有效促進資訊交流，並強化資訊分析能力，減緩事件之衝擊程度。

二、建議事項

(一) 本行風險管理、危機處理及營運不中斷等計畫或人員應相互交流並支援

本行於 2005 年設立風險管理推動小組，整合本行風險管理架構及運作事宜，並自 2012 年起將該小組併入內部控制小組，每年檢討並作成風險管理報告。鑒於國內外環境變化快速，為防患未然，並及時應變，建議本行內部控制小組除就風險管理提出年度報告外，亦可將風險管理、危機處理及營運不中斷等計畫或人員相互交流並支援，以提高綜效。

(二) 加強國際合作以強化資安事件之資訊分享與分析

金管會於 2017 年 12 月成立「金融資安資訊分享與分析中心」(F-ISAC)，由財金資訊公司負責營運，將銀行業、證券期貨業及保險業納入聯防體系，旨在提供資安預警、應變及聯防，並提升整體應變與防護能力。由於資安事件不受國境限制，跨國攻擊可能成為常態，建議國內資安防護宜多方尋求國際合作，以強化防護機制。

參考資料

1. 林高輝 (2017), 「企業風險管理趨勢—威脅與機會並存的新思維」, Aon Benfield，7 月.
2. 許焦桃(2011)，「SEACEN 研訓中心 Operational Risk Management and Business Continuity Management 中央銀行作業風險管理及營運持續管理出國報告」，8 月 15 日。
3. AON (2017), “Global Risk Management Survey 2017”.
4. Bank Indonesia (2018), “2017 Annual Report,” August.
5. BCBS (2018), “Cyber-Resilience: Range of Practices,” Basel Committee on Banking Supervision, Bank for International Settlement, December.
6. Bouveret, Antoine (2018), “Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment,” International Monetary Fund, June.
7. COSO (2018), “An Executive Summary of Enterprise Risk Management-Applying Enterprise Risk Management to Environmental, Social and Governance-Related Risks,” October.
8. DTCC (2018), “Systemic Risk Barometer－2018 Risk Forecast,” Depository Trust & Clearing Corporation, November.
9. G20 (2017), “Communiqué,” G20 Finance Ministers and Central Bank Governors Meeting, Baden-Baden, Germany, March.
10. Institute of Risk Management (2018), “From the Cube to the Rainbow Double Helix: A Risk Practitioner’s Guide to the COSO ERM Frameworks”.
11. Manzanera, Antonio (2018), “Safeguards Assessments Findings in Central Banks’ Risk Management Practices,” October.
12. U.S. Securities and Exchange Commission (2018), “JPMorgan to Pay More Than $135 Million for Improper Handling of ADRs,” December
13. U.K. Cabinet Office (2012), “Business Continuity Management － Revision to

Emergency Preparedness," Emergency planning and preparedness: exercises and training, March.

14. World Economic Forum (2018), "The Global Risks Report 2018, 13th Edition", January.
15. Zbasnik, Matevz (2018), "Managing Financial Risk from Monetary Policy and Lender of Last Resort (LOLR) Operations," October.