國際清算銀行 (BIS)「作業韌性原則」摘譯報告

本公司國關室摘譯

壹、前言

2007 至 2009 年爆發全球金融危機後，巴塞爾銀行監理委員會（Basel Committee on Banking Supervision, BCBS）針對審慎監理架構所進行的改革，已強化全球銀行體系之監理，這些改革亦導致一系列為增強金融韌性的結構性變更。儘管資本及流動性的大幅提高已改善銀行承受金融衝擊的能力，BCBS 認為仍有

本摘譯報告非巴塞爾銀行監理委員會之官方譯文。

必要進一步強化銀行降低相關事件作業風險的能力，前揭事件諸如疾病大規模流行、網路事件、技術失靈及自然災害等，可能導致金融市場重大運作失靈或大規模作業中斷情況。鑒於銀行在全球金融基礎建設運作所扮演的關鍵角色，強化銀行韌性可為金融體系帶來更多保障。

在新型冠狀病毒（COVID-19）疫情爆發前，BCBS 認為金融體系之重大作業中斷事件（disruptive events）將考驗全球金融危機以來金融體系韌性的改善成果。隨著 COVID-19 疫情的持續發展，BCBS 亦觀察到銀行快速變更其作業處理方式，因應組織內不同部門所產生之新風險或既有風險的變化。既知無法避免若干潛在風險，BCBS 相信以務實且彈性的方式提高銀行韌性，可強化銀行對潛在風險之承受、適應與復原能力，藉此降低潛在重大負面衝擊。

BCBS 於 2021 年 3 月發布本報告[註 1]，以推廣採用原則基礎之方法（principle-based approach）改善銀行作業韌性，該方法以 BCBS 更新之「作業風險健全管理原則（Principles for the Sound Management of Operational Risk, PSMOR）」[註 2]為基礎，並汲取 BCBS 先前發布之銀行公司治理、委外作業與營運持續等原則及相關風險管理準則內容。

BCBS 認可部分國家或地區及國際標準制定機構（standard-setting bodies, SSBs）為加強金融部門作業韌性所做的努力[註 3]，BCBS 計劃透過國際參與以強化作業韌性，並促進跨部門之合作。

貳、不斷演變之作業風險

儘管金融服務業運用科技技術帶來新的風險日益增加，銀行及其客戶實已受惠良多。近來銀行所面臨最主要的作業風險，係銀行為提供金融與中介服務，快速採用並加重依賴科技基礎建設，以及金融業越來越倚重第三方提供以科技技術為基礎的服務所致。COVID-19 大流行已使這類作業風險加劇，並增加經濟及業務之不確定性。科技技術及銀行與第三方的關係，可同時支援銀行持續提供客戶金融產品與服務，並提高銀行在疫情期間持續營運的能力。

疫情引起的營運中斷事件已影響銀行的資訊系統、人員、設施及與第三方服務提供業者與客戶的關係，亦使銀行加重倚賴線上工作的安排，導致網路威脅（勒

索軟體攻擊、網路釣魚等）事件激增、人員、流程與系統失靈引起的潛在作業風險事件增加。BCBS 將持續監控 COVID-19 疫情帶來的影響並汲取經驗，以修訂作業韌性指導準則。

參、作業韌性基本要素

有效的風險管理有益於銀行提升作業韌性。銀行風險管理活動，如風險辨識與評估、風險抵減（包括實施控制要項）、風險監控與有效性控制等活動共同發揮作用，可使作業中斷事件及其影響降至最低。此外，在銀行作業會失靈的前提下，管理階層著重銀行因應中斷事件並從中恢復的能力，將有助於作業韌性的提升。具作業韌性的銀行較不易在中斷事件發生時出現失誤並造成損失，從而減少事件對關鍵作業及相關服務、功能與系統的影響。某些諸如疾病大流行等作業風險雖無法避免，但可提高銀行對類等事件的回復能力。

同時，營運持續性、將服務外包給第三方，以及銀行所依賴的技術，是銀行強化作業韌性需考慮的重要因素。在這些領域上，無論是由 BCBS 單獨發布（註 4）的準則，抑或是與其他 SSB 聯合發布者（註 5），個別採用這些準則時，都無法充分涵蓋所有基本要素，但綜合運用之，確實可提高銀行作業韌性。

銀行必須確保現行風險管理架構、營運持續性計畫及第三方依存度管理，在組織內部一致性實施。銀行應考慮其作業韌性方法（operational resilience approach）是否與金融穩定委員會（Financial Stability Board, FSB）復原暨清理計畫架構（Recovery and Resolution Planning framework）所訂定的行動、組織定位相呼應（organizational mappings）、以及關鍵作業與關鍵共享服務之定義相互協調一致（註 6）。

本報告提及之作業韌性原則主要源自並改編自 BCBS 或各國監理機關多年來發布之現有準則。BCBS 認為許多銀行已建立適合其風險組合（risk profile）、作業結構、公司治理與文化之完善風險管理流程，且符合所屬國家或地區之明確風險管理要求。在現有準則與現行實務做法的基礎上，BCBS 發布以原則為基礎的作業韌性方法，有助於確保不同規模、作業複雜程度及所處不同地理位置的銀行相稱地實施（proportional implementation）。

肆、作業韌性定義

BCBS 將「作業韌性（operational resilience）」定義為銀行於中斷事件期間尚能進行關鍵作業的能力。這種能力可使銀行能夠發現潛在失靈狀況、加以自我保護免受潛在失靈的威脅與影響、予以因應並調整適應中斷事件，同時自中斷事件中恢復並汲取教訓，以盡最大努力減少中斷事件對銀行關鍵作業的影響。在擬定銀行作業韌性標準時，銀行應假設中斷事件是會發生的，並考量其整體風險偏好及對中斷事件的容忍程度。論及作業韌性，BCBS 將「中斷事件容忍度（tolerance for disruption）」定義為，銀行在一系列嚴重且擬真（plausible）的假設情境下，其所願意承受之任何種類作業風險造成的作業中斷程度。

「關鍵作業（critical operations）」一詞係源於 2006 年聯合論壇（Joint Forum）的營運持續性高階原則（high-level principles for business continuity）。其包含 FSB[註 7] 定義的「關鍵功能（critical functions）」，並擴展到因中斷事件對銀行持續營運或銀行在金融體系的角色造成重大影響之關鍵功能，包括活動、流程、服務及其相關支援資產[註 8]。判斷特定作業是否「關鍵」，取決於銀行的性質及其在金融體系所扮演的角色。銀行對中斷的容忍度應適用於關鍵作業層面。

報告使用之「個別職能（respective functions）」係 PSMOR 所指銀行三道防線內的適當職能，包括（1）業務單位管理；（2）獨立作業風險管理職能；（3）獨立稽核。依據銀行的性質，如其規模、複雜性及風險組合，三道防線的實施方式可能會有所不同。

伍、作業韌性原則

一、治理（Governance）

原則 1：

銀行運用其現有的治理架構建立、監督並實施有效的作業韌性方法，使能因應、適應中斷事件，並自事件中復原、從中學習，以減少中斷事件對銀行關鍵作業之影響。

(一)董事會檢視並核定銀行作業韌性方法，應考量銀行風險偏好及銀行對關鍵

作業中斷之容忍度。在制定銀行對作業中斷容忍度時，董事會應在所設定可能影響關鍵作業之嚴峻且擬真的廣泛情境下，考量銀行的作業能力，董事會應確保銀行政策能有效處理無法達到中斷容忍度等能力不足之情況。

(二)資深管理階層應在董事會監督下施行銀行作業韌性方法，並確保實施銀行整體作業韌性方法所需財務、技術及其他資源之有效分配。

(三)資深管理階層應及時提供銀行業務單位作業進行中之韌性報告，俾利董事會監督，尤其是發生可能影響銀行關鍵作業之重大缺失時。

(四)董事會應積極透過向所有相關人士（包括銀行人員、第三方及集團內部個體）明確傳達其目標，以確立銀行作業韌性方法獲廣泛瞭解。

二、 作業風險管理（Operational risk management）

原則 2：

銀行應發揮作業風險管理職能，持續辨識內外部威脅，以及來自人員、流程與系統方面的潛在失靈（potential failure），迅速評估關鍵作業之弱點，並依據作業韌性方法管理從而發生的風險。

(一)銀行作業風險管理職能應與其他相關職能相呼應，以管理並解決威脅關鍵作業之任何風險。銀行應協調其營運持續性計畫（business continuity planning）、第三方依存度管理、復原暨清理計畫（recovery and resolution planning）及其他相關風險管理架構，以強化銀行整體作業韌性。

(二)銀行應有足夠的控制要項與程序，俾及時辨識評估威脅、弱點及更普遍的作業風險，並儘可能避免風險影響關鍵作業。各職能單位應定期評估施行控制要項與程序的有效性，亦應在關鍵作業之任何基礎組成要素發生變化，以及事件發生後進行是類評估，汲取經驗教訓，並將導致事件的新威脅與弱點納入考量。

(三)銀行應依據整體作業風險管理之管理變更程序，發揮管理變更能力之功效，評估關鍵作業及其相互關聯與依存度之潛在影響。

三、營運持續計畫與測試（Business continuity planning and testing）

原則 3：

銀行應制定營運持續計畫，並在一系列嚴峻且擬真情境下進行營運持續之演練，以測試銀行在中斷事件下進行關鍵作業的能力。

(一)在評估潛在中斷事件影響時，有效的營運持續計畫應具有前瞻性。銀行應設定一系列包含中斷事件與事故之嚴峻且擬真之情境，進行營運持續之演練並加以驗證。

(二)有效營運持續計畫應可辨識關鍵作業，以及重要內外部依存度，以評估各種不同的中斷情境對關鍵作業之風險與潛在影響。這些計畫應包括營運影響分析、復原策略與測試計畫、訓練及認知計畫，以及溝通與危機管理計畫。

(三)營運持續計畫應研議、施行並定期進行涵蓋關鍵作業及作業間相互關聯與相互依存度之營運持續演練，演練對象包含但不限於第三方及集團內部個體。在其他營運持續性目標中，營運持續之演練應有助於員工對作業韌性之認知，此亦包括員工訓練，使能有效適應並因應事件的發生。

(四)營運持續計畫應就施行銀行災難復原架構提供詳細指引。這些計畫應確立作業中斷管理之角色與職責，並在發生影響關鍵人員之中斷事件時，就職權代理提供明確規範。此外，這些計畫應明確訂定內部決策過程，並定義啟動銀行營運持續計畫的觸發因子。

(五)銀行營運持續計畫之關鍵作業，與銀行復原暨清理計畫關鍵第三方服務的提供，應與銀行作業韌性方法一致。

四、關鍵作業關聯性與依存度之對映（Mapping interconnections and interdependencies）

原則 4：

一旦銀行識別確認其關鍵作業，銀行應依據其作業韌性方法，將提供關鍵作

業所需之內外部關聯性與依存關係予以對映。

(一)銀行各項工作應依據銀行提供關鍵作業所需之人員、技術、流程、資訊、設備，以及前者間之相互關聯與相互依存關係予以對映（即賦予定義並加以記錄），包括但不限於第三方或集團內之安排。

(二)銀行可視情況利用復原暨清理計畫來定義關鍵作業，並應考量其營運韌性方法，是否與其復原暨清理計畫臚列關鍵作業與關鍵第三方服務之組織協調一致（appropriately harmonised）。

(三)銀行之作業韌性方法及對映之粒度級別（level of granularity of mapping），在考量銀行風險偏好及關鍵作業中斷之容忍度後，應足以使銀行辨識其弱點，並可支持銀行進行如原則 3 所述測試其於中斷事件下進行關鍵作業之能力。

五、第三方依存度管理（Third party dependency management）

原則 5：

銀行應管理關鍵作業間之相互依存程度，包括但不限於第三方或集團內部個體之關係。

(一)銀行在與第三方或集團內個體（包含但不限於）達成協議之前，依據銀行作業風險管理架構、委外 / 第三方風險管理政策及作業韌性方法，進行風險評估與實地查核（due diligence）。在銀行達成這類協議之前，應查證協議之相關第三方或集團內個體是否至少具有相同標準的營運韌性，在正常及業務中斷情況下，確保銀行進行關鍵作業。

(二)銀行應制定適當的營運持續計畫、緊急應變計畫程序及退場策略，以便在第三方發生失靈或中斷事件影響關鍵作業之情況下，銀行能保持營運韌性。銀行營運持續計畫設定之情境，應評估第三方提供銀行關鍵作業服務之可替代性，以及其他在第三方中斷服務影響銀行作業韌性時的可行替代方案，例如，改由銀行內部自行提供服務。

六、事故管理（Incident management）

原則 6：

銀行應依據其風險偏好及對中斷事件的承受能力，制定並實施因應暨復原計畫，以管理可能影響銀行關鍵作業之事故（incidents）[註 9]。銀行應透過汲取過往事件之經驗教訓，持續改善其事故因應暨復原計畫。

（一）銀行應維護事件因應與復原、內部及第三方資源的清單，以支持銀行的因應與復原能力。

（二）事故管理的範疇應涵蓋事故的生命週期，通常包括但不限於下列各項：

1. 依據預先定義的標準（如恢復正常業務的預期時間）對事故的嚴重性進行分類，使銀行能夠對資源排列適當之優先順序，並妥善分配資源因應事故。
2. 事故因應及復原程序，包含其與銀行營運持續性、災難復原及其他相關管理計畫與程序之關聯。
3. 施行向內部及外部利害關係人（如監理機關）報告事故的溝通計畫，包括事故期間的績效指標及事故後經驗教訓的分析。

（三）應定期檢視、測試並更新事故因應暨復原程序，銀行應辨識並解決事故發生的根本原因，以防止事故或盡量減少事故之連續發生。

（四）在更新事故管理計畫時，應適當反映過往事故所汲取之教訓，包括他人經歷過的事故。銀行的事故管理計畫應管理影響銀行的所有事故，包括肇因於（但不限於）第三方及集團內部個體之事故。

七、含網路安全之資訊及通訊技術（Information and communication Technology（ICT）including cyber security）

原則 7：

銀行應確保資訊及通訊技術具有彈性，包括網路安全須符合保護、偵測、因應及復原計畫，前揭計畫則須定期測試，納入適當情境意識（situational awareness）並及時傳達相關資訊，以進行風險管理與決策流程，俾充分支持並促

進銀行關鍵作業。

(一)銀行應制定含網路安全之書面 ICT 政策，明訂治理及監督要求、風險所有權（risk ownership）與問責制（accountability）、ICT 安全措施（例如存取控制、關鍵資訊資產保護、身分管理）、網路安全控制的定期評估與監控、事故因應，以及營運持續性與災難復原計畫。

(二)銀行應確定其關鍵資訊資產及其所依賴的基礎設施，銀行亦應依據 ICT 風險評估及關鍵資訊資產對銀行關鍵作業的重要性，優先考量網路安全工作，同時監測與資料保護及保密所有相關之法律及監管要求。銀行應制定計畫並實施控制措施，以在發生網路事件時保持關鍵資訊的完整性，如針對支持關鍵作業所需之不可變動媒介資料的安全儲存與離線備份。銀行應定期評估其關鍵資訊資產的威脅狀況，進行弱點測試，並確保銀行對 ICT 相關風險的抵禦能力。

註釋

註 1： https://www.bis.org/bcbs/publ/d516.pdf.

註 2： *Revisions to the Principles for the Sound Management of Operational Risk*, March 2021, www.bis.org/bcbs/publ/d515.htm.

註 3： Bank of England and Financial Conduct Authority, Building the UK financial sector's operational resilience, December 2019; European Banking Authority, EBA guidelines on ICT and security risk management, November 2019; European Commission, Legislative proposal for an EU regulatory framework on digital operational resilience for the financial sector (DORA), September 2020; Monetary Authority of Singapore, Ensuring safe management and operational resilience of the financial sector, April 2020: International Organization of Securities Commissions (IOSCO), Principles on outsourcing, May 2020; and Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation and Office of the Comptroller of the Currency, Sound Practices to Strengthen Operational Resilience, October 2020.

註 4： BCBS, Risk management principles for electronic banking, July 2003, www.bis.org/

publ/bcbs98.pdf; and BCBS, Corporate governance principles for banks, July 2015, www.bis.org/publ/bcbs.pdf.

註 5： Joint Forum (BCBS-IOSCO-IAIS), Outsourcing in financial services, February 2005, www.bis.org/publ/joint12.pdf; and Joint Forum (BCBSIOSCO-IAIS), High-level principles for business continuity, August 2006, www.bis.org/publ/joint17.pdf.

註 6： 詳見 FSB, Key Attributes of Effective Resolution Regimes for Financial Institutions, October 2014 (http://www.fsb.org/wp-content/uploads/r_141015.pdf); relevant supporting guidance in Identification of Critical Functions and Critical Shared Services, July 2013 (http://www.fsb.org/wp-content/uploads/r_130716a.pdf); and Guidance on arrangements to support operational continuity in resolution, August 2016 (https://www.fsb.org/wp-content/uploads/Guidance-on-Arrangements-to-Support-Operational-Continuity-in-Resolution1.pdf).

註 7： FSB, Recovery and resolution planning for systemically important financial institutions: guidance on identification of critical functions and critical shared services, 2013. 依據 FSB，銀行關鍵功能 (critical functions) 定義為銀行為第三方進行的活動，這類活動若因銀行集團的規模或市場占有率、外部及內部相互關聯性、複雜度與跨境活動導致失靈，會對實體經濟功能及金融穩定造成重大服務中斷的現象。例如，支付、保管、商業或零售部門的借貸及存款收受活動、清算與結算、特定證券及高度集中專業貸款部門的造市等活動。

註 8： 支援資產 (supporting assets) 係指進行關鍵作業所需之人員、技術、資訊及設備。

註 9： 事故係指對銀行關鍵作業產生負面影響之現在或過去發生的中斷事件，事故管理為辨識、分析、改正、從事故中學習，並防止再次發生或因此降低其嚴重性的過程。事故管理的目標在於依據銀行對中斷事件的風險承受能力，限制中斷事件的影響，同時恢復銀行關鍵作業。