本會 112 年 10 月 20 日第 14 屆第 11 次理監事聯席會議核議通過
金管會 113 年 3 月 14 日金管銀國字第 1120236901 號函修正後洽悉

金融機構資訊作業韌性規範

第一條 中華民國銀行商業同業公會全國聯合會(以下簡稱本會)為確保金融機構核心資通系統因意外事故、人為破壞或重大設備故障等而出現服務中斷時，能有效執行應變措施，將損害降低至可承受範圍，並確保能在既定時間內恢復系統，特訂本規範。

第二條 本規範用詞定義如下：

一、資訊作業韌性：核心資通系統因意外事故、人為破壞或重大設備故障等而出現服務中斷時的處理能力與應變彈性。

二、核心業務：由銀行依業務運作中斷對客戶影響數等風險評估結果予以決定，評估範圍如：存款業務、放款業務、匯款業務、外匯業務等。

三、核心資通系統：支持核心業務持續運作必要之系統或設備。

四、重要支援資訊系統：支持核心資通系統持續營運所需之重要支援資訊系統。

五、營運衝擊分析(Business Impact Analysis, BIA)：評估核心業務中斷對金融機構所造成衝擊之分析方法。

六、最大可容忍中斷時間(Maximum Tolerable Period of Disruption, MTPD)：核心業務發生中斷事故之最大可容許中斷時間，應考量法規、利害關係人等面向予以決定。

七、復原時間目標(Recovery Time Objective, RTO)：

(一)核心業務之 RTO：中斷事故發生後，核心業務從中斷事故發生到回復至最小可接受服務水準之目標時間，應依據營運衝擊分析之結果評估訂定。

(二)核心資通系統之 RTO：中斷事故發生後，核心資通系統從中斷事故發生到回復至最小可接受服務水準之目標時間。

八、資料回復時點目標(Recovery Point Objective, RPO)：

(一)核心業務之 RPO：中斷事故發生時，核心業務可承受業務流程資料可被回復的最近時間點，應依據營運衝擊分析之結果評估訂定。

(二)核心資通系統之 RPO：中斷事故發生時，核心資通系統之業務流程資料可被回復的最近時間點(依照備份頻率及時間訂定)。

九、最小可接受服務水準：依據核心業務之復原目標，針對對應之核心業務所訂定期望於復原時間目標(RTO)內回復之最低服務水準。

十、核心資通系統供應商：係指提供銀行核心資通系統之軟硬體產品開發、建置或維運服務的組織或個人，包含其受託者與跨機構合作夥伴。

第三條 若為外國金融機構在臺子公司(或分公司)，應將其外國母公司(或總公司)所在國家(或地區)之資訊作業韌性相關規範與本規範進行比對，從嚴遵循。

第四條 應設置營運持續管理權責單位，配置適當之人力與資源，以負責推動、協調及審查營運持續管理事項。

第五條 應每年識別核心業務、核心資通系統與重要支援資訊系統。當發生影響核心業務及核心資通系統之重大變更時，宜評估是否需重新識別核心業務、核心資通系統與重要支援資訊系統。

第六條 應每年執行營運衝擊分析，並產出下列分析結果：

一、應依據核心業務之業務性質及重要性，訂定核心業務之最大可容忍中斷時間(MTPD)、復原時間目標(RTO)、最小可接受服務水準及資料回復點目標(RPO)，以作為恢復核心資通系統之依據。

二、各核心業務應配合最大可容忍中斷時間(MTPD)內設定復原時間目標(RTO)。

三、應訂定各核心資通系統之復原時間目標(RTO)、資料回復時點目標(RPO)，以作為備份備援規劃及執行復原作業之依據。

四、應依據核心業務之重要性程度或復原時間目標(RTO)列出核心業務之復原優先順序，並識別滿足最小可接受服務水準所需資源。

五、為能於復原時間目標(RTO)內回復至最小可接受服務水準，應擬定滿足最小可接受服務水準所需資源之解決方案。若資源無法於復原時間目標(RTO)內取得、準備完成，或系統備援能力不足者，應由營運持續管理權責單位督導主管或以上之核決層級，考量以下因素後，決定如何加強資源解決方案以補足資源落差，或選擇承擔未能於復原時間目標(RTO)內回復至最小可接受服務水準之風險：

(一)考慮組織可能承擔的風險的數量和類型；

(二)考慮相關的成本和利益。

六、如據第五條已重新識別核心業務、核心資通系統與重要支援資訊系統時，亦應重新執行營運衝擊分析。

第七條 應依據營運衝擊分析結果，制定各核心資通系統之備份與備援機制，並符合下列事項：

一、依據系統特性與資料回復時點目標(RPO)制定備份頻率及資料備份機制：

(一)考量備份媒體類型(磁帶與硬碟)、資料類型(虛擬機映像檔、系統源碼、資料庫與組態設定檔等)、備份類型(完整備份、增量備份與差異備份)、資料備份方式(網路同步寫入、網路非同步寫入與離線備份)等之妥適性。

(二)依需求將重要核心業務資料備份儲存於第三地或雲端。

(三)針對機密與敏感性資料，應實施妥善之防護措施。

二、依據系統特性與復原時間目標(RTO)制定系統備援機制：

(一)依需求規劃為不同等級之備援架構。

(二)主機房與異地備援機房之實體安全應符合金融機構資通安全防護基準第七條。

三、規劃備份與備援機制時應同時考量網路流量、備援網路設備、備援

線路、備援 ISP 與備援資安防護設備等項目。

四、應每年檢視核心資通系統之同地及異地系統備援機制與同地及異地資料備份機制是否符合需求。

第八條 應選擇適當人員擔任資訊作業韌性之角色並每年辦理資訊作業韌性相關教育訓練：

一、參與人員應包括但不限於：營運持續管理權責單位、核心資通系統復原負責人員、重要支援資訊系統復原負責人員、復原核心資通系統必要之供應商、核心業務執行人員，以及上述人員之代理人。

二、應記錄人員受訓結果並每年定期檢視其訓練內容妥適性，以培養具備執行資訊作業韌性相關之能力為目標。

第九條 應制定營運持續計畫，並符合下列事項：

一、應識別可能造成核心業務及核心資通系統中斷之風險情境(包含天然災害、人為災害與資通訊安全事件)，並針對各項風險情境制定營運持續計畫。內容應至少包含：

(一)參與人員及職責。

(二)營運持續計畫之啟動條件。

(三)預防與應變程序：應考量如何進行避難、減災與疏散等作業，並確認人員、辦公場所、通訊、資訊設備與各項資產受損狀況。

(四)復原程序：應考量核心業務之復原程序、同異地系統復原程序。並應依照營運衝擊分析結果，盤點執行復原程序時為滿足最小可接受服務水準所需資源。

(五)應明定與營運持續相關內外部之溝通、聯繫方式、程序、權責及負責單位(內、外對象包含如：客戶、大樓管理中心、警消單位、員工、交易對手、監管機構、委外廠商等)。

二、應每年檢視及測試計畫內容之適切性，視需要更新計畫內容，並於一個或多個異地位置保存計畫。

三、應確保相關人員能取得計畫並給予適當培訓以了解計畫內容。

第十條 應每年審查核心資通系統供應商與金融機構核心資通系統相關之營運持續計畫內容，並確保下列事項：

一、評估核心資通系統供應商若因下列原因而造成營運中斷，其營運持續計畫是否能滿足金融機構所訂之系統復原時間目標(RTO)、資料回復時點目標（RPO），以支持金融機構核心業務復原至最小可接受服務水準。

(一)因天然災害、人為災害與資通訊安全事件而中斷。

(二)未預期之設備故障或變更。

(三)與功能改進、維護、升級和現代化相關計劃性更換。

(四)產品生命週期結束且不再提供技術協助服務，或不具可用性。

二、若其營運持續計畫能滿足金融機構所訂之系統復原時間目標(RTO)、資料回復時點目標（RPO），以支持金融機構核心業務復原至最小可接受服務水準，應保存相關審查紀錄。

三、若其營運持續計畫不能滿足金融機構所訂之系統復原時間目標(RTO)、資料回復時點目標（RPO），以支持金融機構核心業務復原至最小可接受服務水準，應執行核心資通系統供應商營運中斷風險評估，依評估結果擬訂對應之風險處理措施或接受風險並取得營運持續管理權責單位核准。

第十一條 應執行營運持續計畫演練，並符合下列事項：

一、演練內容應驗證各項核心資通系統所制定之標準作業程序(內容至少包含監控、分級分類、通報、應變與復原)，以確保人員熟悉程度與程序有效性。

二、應每年依需求規劃為同地或異地系統備援演練、同地或異地資料備份回存測試；針對無備援之核心資通系統或重要支援資訊系統，得考量同地或異地系統重建演練。鼓勵異地備援演練時，納入對外實際運作驗證。

三、應針對已識別可能造成服務中斷之風險情境(包含天然災害、人為

災害與資通訊安全事件)設計演練情境。可規劃每年針對所有情境或輪流針對部分情境進行實操演練或桌面演練。

四、演練參與人員應包含核心資通系統復原負責人員、重要支援資訊系統復原負責人員、復原核心資通系統必要之供應商、核心業務執行人員。

五、演練測試前應識別可能造成之風險(如：因演練可能造成正式資料之錯誤或遺失、演練可能造成之資安防護水準下降、演練可能造成之客戶權益損害等)，並事先擬定保護措施。

六、應保留由管理階層核可之相關演練紀錄及召開檢討會議。檢討會議中需確認復原機制與演練結果是否符合 RTO 及 RPO 要求，並檢視核心資通系統之現有同異地災害備援機制與同異地資料備份機制是否符合核心業務之需求。

第十二條 本規範經本會理事會通過並函報金融監督管理委員會核備後實施，修正時亦同。