證券暨期貨市場各服務事業

資訊作業韌性參考指引

第一章 總則

第一條 （目的）

依據金融監督管理委員會「金融資安行動方案」，為強化證券商、期貨商及投信投顧業者之資訊作業韌性，確保組織於核心系統遭受中斷事故，可有效執行應變措施、將損害降低至可承受範圍，擬定資訊作業韌性參考指引。

第二條 （適用範圍與對象）

本指引適用之組織包含證券商、期貨商、證券投資信託事業及證券投資顧問事業。適用對象分為以下兩類說明:

一、第一類:

(一)依「證券暨期貨市場各服務事業建立內部控制制度處理準則」第三十六條之二條文指派資訊安全長之組織。

(二)「建立證券商資通安全檢查機制-分級防護應辦事項附表」所列第一級、第二級、第三級證券商。

(三)「建立期貨商資通安全檢查機制-分級防護應辦事項附表」所列第一級、第二級、第三級期貨商。

二、第二類:

非屬第一類範圍之組織。

三、外資集團在台子公司或分公司，其資安、營運持續或作業韌性管理政策由外國母公司或總公司控制與建置者，如其母公司或總公司已建置或設立相關控制措施，且有較佳之規範，則從其規範；若無，則應遵循本國法令法規規範。

四、以下參考指引如無特別說明，皆為第一類及第二類組織應遵循之事項。

第三條 （名詞定義）

一、營運持續：

資訊作業面臨損害、異常或中斷服務時的處理能力與應變彈性。

二、核心業務：

係指直接提供客戶交易或支持交易業務持續運作之必要業務。

三、核心系統：

係指直接提供客戶交易或支持交易業務持續運作之必要系統，其餘皆為非核心系統。

四、營運衝擊分析(Business Impact Analysis, BIA)：評估隨著核心業務中斷時間的增長，辨識出對組織所造成衝擊之分析方法。

五、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，應考量法令法規、營收損失與利害關係人要求等面向。

六、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)核心系統之 RTO：中斷事故發生後，核心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。

(三)核心系統之 RTO 應小於等於核心業務之 RTO。

七、資料復原點目標(Recovery Point Objective, RPO)：

(一)核心業務之 RPO：依據核心業務性質評估中斷事故發生時，核心業務可承受之資料損失量所訂之值，應依據營運衝擊分析之結果評估訂定。

(二)核心系統之 RPO：依據核心業務性質評估中斷事故發生時，核心系統可承受之資料損失量所訂之值。

(三)核心系統之 RPO 應小於等於核心業務之 RPO。

八、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)內回復之最低限度運作水準。

九、災害應變機制：當災害發生造成核心系統異常或中斷時，各系統相

關作業流程對應之應變、減災或復原措施。

第二章 國際營運持續管理標準

第四條 （營運持續管理）

國際標準組織已訂有以營運持續管理為主題之國際標準，組織導入ISO22301 國際營運持續管理標準及取得相關驗證，可有效協助組織參採最佳實務做法，強化組織營運持續管理。

一、證券商：「建立證券商資通安全檢查機制-分級防護應辦事項附表」所列第一級證券商(實收資本額 200 億以上)應取得國際營運持續管理標準；第二級證券商應導入國際營運持續管理標準。

二、期貨商、投信投顧業者：「證券暨期貨市場各服務事業建立內部控制制度處理準則」第三十六條之二條文指派資訊安全長之組織，應導入國際營運持續管理標準。

第三章 營運持續管理

第五條 （管理組織與權責）

一、組織應訂定營運持續管理權責單位，配置適當之人力、物力與財力資源，以負責推動、協調監督及審查營運持續管理事項。

二、組織應訂定營運持續相關管理、訓練、演練及應變復原等規範，並對所有核心業務與核心系統相關員工及供應商傳達適用之規範。

三、組織應依據權責及專業能力選擇適當人員擔任其角色並定期提供必要教育訓練。

第六條 （核心業務與核心系統）

一、組織應每年識別核心業務與核心系統。

二、外資集團在台子公司或分公司，若核心系統建置於外國母公司或總公司時，依外國母公司或總公司所制定資通安全規範機制為基準，提供相關文件後，可僅就本地實務可執行面進行核心系統評估。

第七條 （營運衝擊分析）

組織應每年定期執行營運衝擊分析，評估核心業務中斷所造成之衝擊程

度，並產出下列分析結果，以利評估核心系統復原策略：

一、組織應識別核心業務之業務性質及重要特性，依據識別結果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復原點目標(RPO)，以作為恢復核心系統之依據。

二、組織應訂定核心系統之復原時間目標(RTO)、資料復原點目標(RPO)，以作為備份備援規劃及執行復原作業之依據。

三、組織應依據核心業務之重要程度或復原時間目標(RTO)列出復原優先順序，並辨識滿足最小可接受服務水準所仰賴之資源分配(包含但不限於場地、基礎設施、網路、電話線路、資通系統、辦公用軟硬體、辦公設備、預備金、人員、文件與復原所需供應商)。

四、組織應依據經營策略、營運目標、組織規模及資源等，制定出災害發生後應迅速回復之最小可接受服務水準，以反映組織所願意接受之風險。

第八條 （備份備援機制）

組織應依據營運衝擊分析結果，制定核心系統之備份與備援機制：

一、組織應依據系統特性與資料復原點目標(RPO)，考量備份頻率、儲存媒體類型(光碟、外接硬碟、磁帶)、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)、備份方式(網路同步寫入、網路非同步寫入與離線備份)等，制定適當之資料備份機制。

二、組織於制定資料備份機制時，宜考量「3-2-1 備份原則」。

(一) 至少製作三份備份。

(二) 將備份分別存放在兩種不同儲存媒體。

(三) 至少一份放在異地保存。

三、組織應依據系統特性、業務單位需求與復原時間目標(RTO)，制定適當之系統備援架構，例如鏡像站(Mirror Site)、熱備援站(Hot Site)、暖備援站(Warm Site)或冷備援站(Cold Site)等。

四、組織規劃備份與備援機制時應考量網路流量、備援網路設備、備援

線路、備援電信營運商與備援資安防護設備等項目。

五、 組織應定期檢視核心系統之同異地系統備援機制與同異地資料備份機制是否符合需求。

第九條 （機房設置規劃）

一、組織規劃備援機房時應遵循政府建築及消防相關法令法規，考量支援設施包含電力供給、空調配置、環境監控與告警等配置。

二、第一類組織應設置異地備援機房。

三、第一類組織之主機房基礎設施應考量備援機制，例如配置雙饋線、機房專用不斷電系統(UPS)、機房專用發電機、二家以上電信營運商、二線以上對外網路線路等。

四、第一類組織之主機房與異地備援機房應有足夠營運使用之電力、供水、用油等供應措施，當發生供應措施中斷時，應至少維持七十二小時運作時間。

五、組織於評估搬移或新建機房設置地點時，應考量以下事項：

(一)組織應參考行政院「電腦機房異地備援機制參考指引」，主機房與異地備援機房之位置應避免遭受同一中斷風險事件影響(例如同一地震帶、同一電力供應區域等)或主機房與異地備援機房之距離達30公里以上。

(二)組織應考量該位置之地質條件、天然災害、人為災害(是否鄰近核電廠、處理化學製品或易爆材料的廠區、機場飛航航道的直接下方、繁忙的醫院、治安高風險區等)、公共設施(水、電、油、網等之供應)、交通便利、人員移動時間等因素。

(三)組織宜考量是否與同業間，有過度集中於相同機房之問題。

第十條 （災害應變機制）

組織應制定災害應變機制，以確保災害發生時，可有效降低人員傷亡、核心系統與各項資產損失情況。內容包含但不限於：

一、應設置災害應變與營運持續相關內部組織，並明訂其權責：

(一)應設置自衛消防編組。

(二)應設置緊急通報小組或緊急處理小組。

二、應辨識可能造成中斷之風險情境(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擬定如何避免、預防與應變之緊急應變措施。

三、應制定緊急處理程序，包括配合自衛消防編組指示進行避難、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、應制定緊急通報程序，並明訂通報之單位及權責。

(一)應訂定對組織內部之通報程序，包括自衛消防編組、緊急處理小組或相關權責單位。

(二)應訂定對外部警消機關（例如：警察、消防隊）之通報程序。

(三)應訂定資訊安全訊息通報機制(例如:正式之通報程序及資安事件通報聯絡人)，針對與資訊系統有關之資訊安全或服務異常事件應依「證券期貨市場資通安全事件通報應變作業注意事項」辦理，並採取適當矯正程序，留存紀錄。

(四)其他法令法規規範應通報主管機關或公會等外部單位者，應訂定相關通報程序。

第十一條（營運持續計畫）

組織應制定營運持續計畫，以確保災害發生時，可於復原時間目標(RTO)內回復至最小可接受服務水準。內容包含但不限於：

一、啟動條件。

二、參與人員及職責說明。

(一)應設置營運持續管理小組或營運持續管理委員會。

(二)應盤點核心業務復原所需之執行人員及支援人員。

(三)應指派核心系統復原負責人員及其代理人。

三、緊急處理程序及緊急通報程序。

四、核心業務之復原程序、同異地系統復原程序（例如：電腦設備、通訊設備、電力系統、資料庫、電腦作業系統等備援及回復計畫）。

五、營運持續計畫之維護頻率。

六、營運持續相關教育訓練之規範。

七、往來外單位之應變規劃及合約適當性。

第十二條（營運持續計畫演練）

組織應針對各情境、各業務狀況進行演練，以達到演練及測試程序之有效運作。

一、組織應針對已辨識可能造成核心業務中斷之風險情境(包含天然災害、人為災害與資通訊安全事件)設計演練情境。

二、組織應進行模擬災害或意外發生時之情境操作，考量納入核心系統操作人員、核心業務執行人員與復原所需供應商；並規劃演練之系統數量、規模與層次(實體機、虛擬機與中介層等)。

三、組織應於演練前，辨識可能造成之風險(例如：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、演練可能損害之客戶權益等)，並事先擬定保護措施。

四、演練內容應驗證各項核心系統所制定之標準作業程序(內容包含但不限於監控、分級分類、通報、應變與復原)。

五、組織應每年定期演練並驗證其核心系統可用性，依需求規劃為同異地系統備援演練、同異地系統重建演練(針對無備援之系統)或同異地資料備份回存測試，以確保人員熟悉程度與程序有效性，並應留存相關演練紀錄。

六、第一類組織應於異地系統備援演練時，納入實際業務運作驗證，以實證最小可接受服務水準所仰賴之內部資源配置及人力調度、外部夥伴之協同作業及資訊網路調整介接等作業，於關鍵時刻皆能有效運作。並鼓勵第二類組織執行。

七、組織應於演練後召開檢討會議，確認復原機制與演練結果是否符合組織所制定的復原時間目標(RTO)及資料復原點目標(RPO)要求，並檢視核心系統現有同異地系統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。

第十三條（認知及能力訓練）

一、組織應確保核心系統復原負責人員及其代理人有能力適任並授予充足訓練。訓練面向與內容可包含但不限於認知訓練、營運持續、

相關最新趨勢、備份備援技術面訓練、演練之經驗傳承、近期內外部營運持續相關案例、資通系統架構變更等。

二、組織應完整記錄人員之受訓結果並每年定期檢視同仁之認知程度、能力與訓練內容妥適性。

第十四條（核心系統委外之管理）

一、核心系統委外時，組織應依委外服務範圍及特性確保於災害發生後，核心系統之復原水準、系統復原時間目標(RTO)、資料復原點目標(RPO)能支持核心業務回復至最小可接受服務水準，以及每年定期演練並驗證其核心系統可用性。

二、組織應將上述營運持續管理相關要求納入委外契約。

第四章 參考文獻

一、行政院(107 年 6 月)，資通安全管理法，
資通安全管理法-全國法規資料庫 (moj.gov.tw)

二、ISO 國際標準組織(108 年 10 月)，ISO 22301:2019 Security and resilience — Business continuity management systems — Requirements
ISO - ISO 22301:2019 - Security and resilience — Business continuity management systems — Requirements

三、銀行公會(110 年 7 月)，金融機構資通安全防護基準，
(金管會函文)

四、壽險公會(110 年 10 月)，保險業資訊作業韌性參考規範草案，
(金管會函文)

五、美國聯邦金融機構檢查委員會 FFIEC(108 年 11 月)，FFIEC Information Technology Examination Handbook Business Continuity Management，
FFIEC Press Release

六、行政院國家資通安全會報(103 年 7 月)，電腦機房異地備援機制參考指引，
我國電腦機房異地備援機制參考指引 (行政院國家資通安全會報-作業規範) (ey.gov.tw)