# 「保險業資訊作業韌性參考原則」

金管會 111 年 7 月 4 日金管保綜字第 1110492600 號洽悉

| 條文 | 訂定說明 |
| --- | --- |
| 保險業資訊作業韌性參考原則 | 依金管會 109 年 9 月 17 日金管資字第 1090193408 號函及保險局 109 年 12 月 3 日保局(綜)字第 1090429495 號函訂定「保險業資訊作業韌性參考原則」(下稱本參考原則)。 |
| 第一點(目的)<br>為協助保險業資訊作業於發生意外事故、人為破壞或重大設備故障等事件造成核心業務之資通系統中斷時，能有效執行應變措施並將損害降低至可承受範圍，及在既定時間內重建並恢復系統，中華民國產物保險商業同業公會(以下簡稱產險公會)、中華民國人壽保險商業同業公會(以下簡稱壽險公會)爰共同訂定本參考原則，以資遵循。<br>保險業宜參照本參考原則相關規定辦理。 | 揭示本參考原則之訂定目的。 |
| 第二點(用詞定義)<br>本參考原則用詞，定義如下：<br>一、資訊作業韌性：資訊作業系統面臨損害時的處理能力與應變彈性。<br>二、核心資通系統：關鍵業務所需之必要系統，應包含「保險業辦理資訊安全防護自律規範」所列之核心資訊系統與涉及核心業務持續運作之重要資訊系統。<br>三、營運衝擊分析(Business Impact Analysis，BIA)：分析業務中斷對公司所造成影響運作之方法。<br>四、復原時間目標(Recovery Time Objective，RTO)：核心資通系統從事故發生到完成回復正常運作狀態之可接受時間。<br>五、資料復原點目標(Recovery Point Objective，RPO)：事故發生後，核心資通系統之業務流程資料可被回復的離事故發生時之最近時間點，保險業應依照營運衝擊分析之結果評估訂定資料復原點目標。<br>六、核心業務識別：依據保險業所提供之關鍵產品與服務，識別遭遇重大災變時公司需持續運作之業務作業流程。 | 1.明定本參考原則用詞定義。<br>2.增列用詞定義及說明，其相關參考條文或說明：<br>(1)核心資通系統：原用詞定義核心資訊系統由關鍵資訊系統組成，以參考資通安全管理法施行細則第七條(同金管會 109 年 5 月 26 日金管保綜字第 1090419516 號函准備查修正之保險業辦理資訊安全防護自律規範第五條第一項)及參照「行政院國家資通安全會報-關鍵資訊基礎設施資安防護建議內容」進行調整，符合保險業適用之定義。<br>(2)營運衝擊分析：參照「保險業風險管理實務守則__問答手冊 BCM 議題，其營運衝擊分析之步驟主要評估「業務中斷之衝擊」訂定。<br>(3)核心業務識別：依照各公司業務別之作業流程涉及到核心業務時，應識別遭受重大災變時要如何持續運作之流程。 |

# 「保險業資訊作業韌性參考原則」

金管會 111 年 7 月 4 日金管保綜字第 1110492600 號洽悉

| 條文 | 訂定說明 |
| --- | --- |
| 七、最大可容忍中斷時間(Maximum Tolerable Period of Disruption ,MTPD)：核心業務發生營運中斷事故時，組織可容忍營運中斷的最大時間值。<br>八、災害應變運作：當意外發生造成核心資通系統中斷時，各系統相關作業流程是否有其他因應或緊急應變措施，可在指定時間內回復至組織正常或可接受的營運水準。<br>九、演練測試：依保險業所訂定災害應變運作各項措施辦法及流程，納入情境模擬測試，確保在該情境災害下能夠正常運行或即時處理系統。<br>十、復原能力之實證：依保險業辦理演練測試，須與實際作業流程進行相關驗證，避免當發生天災人禍時，各項應變措施無法運行，而造成重大營運損失。 | (4)最大可容忍中斷時間：參考來源為國際標準 ISO 22301 之 MTPD 的定義，組織因可容忍最大中斷時間。<br>(5)災害應變運作：該定義以當意外發生時需達成災害復原之目的，擬訂持續保持系統營運水準之目標。<br>(6)演練測試：參照「保險業風險管理實務守則__問答手冊 BCM 議題，以 BCM 標準的演練及測試之定義。<br>(7)復原能力之實證：該定義以落實實際辦理演練，並與實際作業流程與環境進行驗證，以達到復原之有效性。 |
| 第三點(資訊作業韌性之管理權責與組織)<br>保險業資訊作業韌性之管理權責與組織，依保險業風險管理實務守則之規定辦理。<br>保險業之營運持續管理應遵循下列事項：<br>一、訂定核心資通系統之業務負責單位及系統營運單位，以確保職責之有效分配。<br>二、分配系統營運管理相關工作，包括但不限於資源取得、內部協調、指導系統營運管理之運作等。 | 明訂資訊作業韌性之管理權責與組織。<br>1. 第一項明訂資訊作業韌性之管理權責與組織，按營運持續管理係指監督和落實營運韌性，資訊作業韌性為營運持續管理之一環，考量保險業風險管理實務守則及保險業風險管理實務手冊問答手冊已規範保險業整體營運相關層級之管理權責與組織，故保險業之資訊作業韌性之管理權責與組織依保險業風險管理實務守則規範辦理。<br>2. 第二項明訂保險業之營運持續管理應符合之事項。 |
| 第四點(資訊作業韌性之參考原則項目)<br>資訊作業韌性之參考原則項目如下：<br>一、核心資通系統識別<br>保險業應視系統規模、架構及依賴程度，訂定範圍及作業流程，內容包括：<br>(一) 辨識所有核心資通系統之重要性與相依性。<br>(二) 盤點支持系統持續營運所需之重要支援資訊系統。<br>(三) 核心資通系統若建置於國外總公司時，依國外總公司所訂定資訊安全規範機制為基準，提供相關文件後予以排除豁免，並僅就本地實務可執行面進行資訊系統評估。 | 依保險局 109 年 12 月 3 日保局(綜)字第 1090429495 號函說明二(一)訂定相關指引，說明如下：<br>1. 核心業務雖配有專屬資訊系統加以輔助，然其資訊系統損毀並不會使業務實體遭致嚴重衝擊，可以其他作業方式因應之，另需辨識所有業務之功能與其重要性及分析各業務流程和各系統之間相互依賴關係併入之，故「核心業務之識別」更改為「核心資通系統識別」之參考指引。<br>另本條文參考保險業內部控制及稽核制度實施辦法第 37 條納入排除豁免有核心資訊系統為國外母公司之情況。 |

# 「保險業資訊作業韌性參考原則」

金管會 111 年 7 月 4 日金管保綜字第 1110492600 號洽悉

| 條文 | 訂定說明 |
| --- | --- |
| 二、最大可容忍中斷時間<br>保險業進行營運衝擊分析時，應評估核心資通系統中斷所造成影響及衝擊程度，並依核心業務識別之影響程度劃分最大可容忍中斷時間，以利評估核心資通系統復原策略，內容包括：<br>（一） 依據核心業務識別之業務性質及重要特性，妥善對營運持續管理之要求訂定核心資通系統可容忍中斷時間。<br>（二） 訂定復原時間目標及資料回復點目標，以作為恢復核心資通系統之依據。<br>（三） 依據核心業務識別之重要性程度及所仰賴之資源，列出復原優先順序。<br>（四） 依據保險業之經營策略、營運目標、公司規模及資源等，訂定適當營運水準目標及災害發生後應回復之可接受的最低服務水準，以反映公司所願意接受之風險。 | 2. 本款條文參考內政部消防署暨所屬機關業務持續運作程序規範及參照「保險業風險管理實務守則__問答手冊 BCM 議題其程序似與營運衝擊分析步驟一致，故訂定「最大可容忍中斷時間」之參考指引。 |
| 三、災害應變運作<br>保險業應訂定災害應變計劃與程序，以確保核心資通系統能於災害發生時，可滿足最低營運需求，內容包括：<br>（一） 訂定災害適用範圍及啟動應變運作時機。<br>（二） 為因應災害事件發生，保險業應明確定義災害應變組織。災害應變組織角色應包括但不限於災害事件應變指揮官、系統營運與協調指揮者、系統處理人員、災害事件調查人員、公關人員及系統之實務業務操作與客服人員等，並應訂定組織角色之職責。<br>（三） 訂定應變處理程序，程序應明確且具可操作性，內容包括：<br>1. 災害事件發生之通報管道、通報程序、判斷災害影響程度、進行通報等。<br>2. 視災害情況，召開災害事件應變處理會議。<br>3. 訂定溝通策略，包括與內外部相關利害關係人溝通策略，以降低營運中斷之衝擊。<br>4. 進行損害控制(包含跡證保存)。<br>5. 訂定復原程序，包括啟動復原作業的時機與流程，以及復原所需資源調度之計畫。 | 3. 本款條文參考內政部消防署暨所屬機關業務持續運作程序規範並訂定「災害應變運作」之參考指引。 |

| 條文 | 訂定說明 |
| --- | --- |
| 6.根據災害事件進行根因分析及依分析結果進行追蹤改善。<br>（四） 定期檢視核心資通系統異地災害備援機制。<br><br>四、核心資通系統復原計劃<br>保險業應針對擬訂之情境/各業務狀況進行演練或實體模擬操作，以達到演練及測試程序之有效運作。<br>（一）應落實核心資通系統演練階段所訂定標準作業程序。<br>（二）辨識風險及災害影響大小應包含但不限外部環境對核心資訊系統及業務流程運作，當意外發生可以降低對保險業的營運衝擊。<br>（三）應進行模擬災害或意外發生時之情境操作。<br>五、復原能力之實證<br>保險業應針對核心資通系統中斷可能之情境進行演練或實體模擬操作，並應確認復原機制是否完善，以確保演練情境測試結果有效性：<br>（一）核心資通系統復原計畫應每年至少演練一次，以確保復原計劃之有效性，並使相關人員確實瞭解與熟悉。<br>（二）演練範圍應納入重要支援資訊系統，演練人員應納入業務單位及相關人員。<br>（三）若採異地備援，演練時宜納入實際業務運作，以驗證異地備援之有效性。<br>（四）演練結束後，應檢討結果，並據以修正或調整應變處理程序及復原計畫之內容。<br>（五）確認復原機制是否符合保險業所訂定的復原時間目標及資料復原點目標要求。<br>（六）核心資通系統復原計畫進行演練時，須有記錄過程及演練記錄，並呈交管理層核可及留存記錄。 | 4.前述來函所稱「壓力測試」指 BCM 標準中資訊系統的演練及測試，在傳統資訊系統中的「壓力測試」意義與之不同，恐造成同業進行實務上執行時有名詞誤導，故配合同業執行狀況而改成「核心資通系統復原計劃」以符合資訊系統之 BCM 實務以避免混淆，故訂定該參考指引。<br><br>5.為呈現實際演練後之狀況並持續改善、驗證有效性及確認之水準及需持續改善之一環所訂定「復原能力之實證」之參考指引。 |
| 第五點(資訊作業韌性之認知及能力訓練)<br>保險業辦理資訊作業韌性之認知及能力訓練，應遵循下列事項：<br>一、應定期辦理核心資通系統之營運持續教育訓練並留存紀錄。<br>二、核心資通系統應規劃備援人力，備援人力依其業務及作業需要，應安排接受相關必要訓練，以確保可支援系統事故處理。 | 明訂各會員公司辦理資訊作業韌性之認知及能力訓練應辦理之事項。 |

# 「保險業資訊作業韌性參考原則」

金管會 111 年 7 月 4 日金管保綜字第 1110492600 號洽悉

| 條文 | 訂定說明 |
| --- | --- |
| 第六點(資訊作業韌性之有效量測與評估)<br>保險業依據所訂資訊作業之持續營運管理目標，決定適當量測標的、評估方法及分析方法，以確保評估資訊作業韌性管理之有效性。 | 明訂資訊作業韌性之有效量測與評估之方式。 |
| 第七點(施行程序)<br>本參考原則經產險公會與壽險公會理事會通過並陳報主管機關後施行；調整時，亦同。 | 明訂本參考原則之施行程序。 |