金融監督管理委員會令

中華民國 107 年 5 月 29 日
金管保財字第 10704502401 號

修正「保險業內部控制及稽核制度實施辦法」部分條文。

附修正「保險業內部控制及稽核制度實施辦法」部分條文

主任委員　顧立雄

保險業內部控制及稽核制度實施辦法部分條文修正條文

第　六　條　　保險業使用電腦化資訊系統處理者，其內部控制制度，除資訊部門與使用者部門應明確劃分權責外，至少應包括下列控制作業，並應依所屬商業同業公會訂定之自律規範辦理：

一、資訊處理部門之功能及職責劃分。

二、系統開發及程式修改之控制。

三、編製系統文書之控制。

四、程式及資料之存取控制。

五、資料輸出入之控制。

六、資料處理之控制。

七、電腦機房門禁之控制。

八、系統、檔案及電腦、通訊設備之安全控制。

九、硬體及系統軟體之購置、使用及維護之控制。

十、電腦病毒擴散及網路駭客入侵之防範控制。

十一、系統復原計畫、災變備援計畫及測試程序之控制。

十二、核心業務委外處理之控制。

十三、客戶及公司機密資料之保密及安全防範控制。

十四、電腦犯罪之防範控制。

中華民國人壽保險商業同業公會及中華民國產物保險商業同業公會應訂定並定期檢討資訊安全自律規範。

第六條之一　　保險業應設置資訊安全專責單位及主管，不得兼辦資訊或其他與職務有利益衝突之業務，並配置適當人力資源及設備。但主管機關對保險合作社另有規定者，依其規定。

保險業前一年度經會計師查核簽證之資產總額達新臺幣一兆元以上者，應設置具職權行使獨立性之資訊安全專責單位，並指派協理以上或職責相當之人擔任資訊安全專責單位主管。

保險業資訊安全專責單位負責規劃、監控及執行資訊安全管理作業，每年應將前一年度資訊安全整體執行情形，由資訊安全專責單位主管與董（理）事長（主席）、

總經理、總稽核聯名出具資訊安全整體執行情形聲明書（附表一），並於會計年度終了後三個月內提報董（理）事會。

保險業資訊安全專責單位人員，每年至少應接受十五小時以上資訊安全專業課程訓練或職能訓練。總機構、國內外營業單位、商品開發管理單位、資金運用單位、資訊單位、資產保管單位及其他管理單位之人員，每年至少須接受三小時以上資訊安全宣導課程。

適用第二項規定之保險業，應於符合適用條件起六個月內調整。

第二十五條　保險業總經理應督導各單位審慎評估檢討內部控制制度之執行情形，由董（理）事長及總經理、總稽核及總機構法令遵循主管聯名出具內部控制制度聲明書（附表二），並提報董（理）事會通過，於每年三月底前，依本法第一百四十八條之一規定併年度報表，報主管機關備查。

保險業應將內部控制制度聲明書內容揭露於保險業網站。

第 三十 條　保險業之總機構應依其規模、業務性質及組織特性，設立隸屬於總經理之法令遵循單位，負責法令遵循制度之規劃、管理及執行。

法令遵循單位應置總機構法令遵循主管一人，綜理法令遵循業務，至少每半年向董（理）事會及監察人（監事）或審計委員會報告，如發現有重大違反法令時，應即時通報董（理）事及監察人（監事），並就法令遵循事項，提報董（理）事會。

前二項法令遵循單位及總機構法令遵循主管之設置，規定如下：

一、保險業前一年度經會計師查核簽證之資產總額達新臺幣一兆元以上者，應設置專責之法令遵循單位，得兼辦防制洗錢及打擊資恐相關事項。但不得兼辦與法令遵循制度之規劃、管理及執行無關之法務或其他與職務有利益衝突之業務。其總機構法令遵循主管，得兼任防制洗錢及打擊資恐專責單位主管。但不得兼任法務單位主管或內部其他職務。

二、不適用前款規定之保險業，其總機構法令遵循主管除兼任法務單位主管與防制洗錢及打擊資恐專責單位主管外，不得兼任內部其他職務。

保險業之總機構法令遵循主管，職位應相當於副總經理，且具備領導及有效督導法令遵循工作之能力，其資格應符合保險業負責人應具備資格條件準則規定。

前項總機構法令遵循主管，於外國保險業在台分公司、再保險業及保險合作社得指派高階主管一人擔任總機構法令遵循主管，其中保險合作社得不受第三項不得兼任內部其他職務規定之限制。

總稽核、稽核單位主管及內部稽核人員，不得兼任第二項所定之總機構法令遵循主管。

保險業任免總機構法令遵循主管應經董（理）事會全體董（理）事二分之一以上同意，並報主管機關備查。

保險業總機構法令遵循主管、法令遵循單位主管及所屬人員，每年應至少參加主管機關或其認定機構所舉辦或所屬金融控股公司或保險業自行舉辦之在職教育訓練達二十小時以上，訓練內容應至少包括新修訂法令規章及新銷售保險商品。

保險業營業單位、商品開發管理單位、資金運用單位、資訊單位、資產保管單位及其他管理單位之法令遵循主管，每年應至少參加主管機關或其認定機構所舉辦或所屬金融控股公司或保險業自行舉辦之在職教育訓練達十五小時以上。

國外分公司之法令遵循主管，每年應至少參加由當地主管機關或相關單位舉辦之法令遵循在職教育訓練課程十五小時，或參加主管機關或其認定機構所舉辦或所屬金融控股公司或保險業自行舉辦之教育訓練課程。

前三項在職訓練為自行舉辦之訓練方式應提報董（理）事會通過，總機構需留存相關人員上課紀錄備查。

防制洗錢及打擊資恐專責單位設於法令遵循單位者，該專責單位人員充任前及每年應受之訓練，依防制洗錢及打擊資恐相關規定辦理，不受第八項及第三十三條第二項規定限制。

保險業應以網際網路資訊系統向主管機關申報總機構法令遵循主管、法令遵循單位主管及所屬人員名單、最近三年獎懲紀錄、資歷及受訓資料等。

第三十二條之一　適用第三十條第三項第一款之保險業應建立全公司之法令遵循風險管理及監督架構，其架構原則及權責規定如下：

一、法令遵循單位應建立辨識、評估、控制、衡量、監控及獨立陳報法令遵循風險之程序、計畫及機制，以全面控制、監督及支援國內外各部門、分支機構及子公司之個別營業單位、跨部門及跨境之相關法令遵循事項。

二、法令遵循單位應依據業務分類或法令遵循重點設置適當數量之專業單位，以負責該項業務或法令相關之國內外營業單位監督、法令遵循執行及支援事項。

三、法令遵循單位得依風險基礎方法評估各單位法令遵循主管之設置並強化法令遵循主管之獨立性，屬法令遵循風險較低之單位得不單獨設置法令遵循主管而由總機構法令遵循單位負責，不受第三十三條第一項前段規定之限制。

四、法令遵循單位應建立法令遵循風險警訊之獨立通報、評估及處理因應機制。

五、法令遵循單位應定期及不定期評估主要營運活動、商品及服務、資金運用或業務專案、有違反法令之虞之重大客訴等法令遵循風險管理情形，並建立與其他第二道防線之橫向溝通聯繫機制。

六、法令遵循單位為掌握全公司法令遵循風險情形，得向各單位要求提供相關資訊。

七、管理階層及各部門主管之考核，應納入法令遵循部門對其法令遵循執行程度之評估意見。

八、保險業及法令遵循單位應充分掌握國外營業單位應辦理之法令遵循事項及當地主管機關對法令遵循標準之要求，並提供充分資源及支援。

九、法令遵循單位依第三十條第二項至少每半年向董（理）事會及監察人或審計委員會報告之法令遵循事項，應針對全公司境內外營運情形，提出法令遵循風險管理之弱點事項及督導改善計畫及時程，董（理）事會應提供充分資源及對營業單位建立適當獎懲機制，以循序建立全公司法令遵循文化。

十、總稽核依第十一條第一項至少每半年向董（理）事會及監察人或審計委員會報告之稽核業務事項，應包括法令遵循單位辦理績效及全公司法令遵循程度之評估意見。

適用前項規定之保險業，應於符合適用條件起六個月內，依第三十條第三項第一款規定設置總機構專責之法令遵循單位及法令遵循主管，並調整全公司之法令遵循風險管理及監督架構報請主管機關備查後，且於每年四月底前，依本法第一百四十八條之一規定，將前項第五款及第九款評估報告函報主管機關。

第三十二條之二　保險業為促進健全經營，應建立檢舉制度，並於總機構指定具職權行使獨立性之單位負責檢舉案件之受理及調查。

保險業對檢舉人應為下列之保護：

一、檢舉人之身分資料應予保密，不得洩漏足以識別其身分之資訊。

二、不得因所檢舉案件而對檢舉人予以解僱、解任、降調、減薪、損害其依法令、契約或習慣上所應享有之權益，或其他不利處分。

檢舉案件之受理及調查過程，有利益衝突之人，應予迴避。

第一項檢舉制度，至少應包括下列事項，並提報董（理）事會通過：

一、揭示任何人發現有犯罪、舞弊或違反法令之虞時，均得提出檢舉。

二、受理之檢舉案件類型。

三、設置並公布檢舉之管道。

四、調查與配合調查之流程、迴避規定及後續處理機制之標準作業程序。

五、檢舉人保護措施。

六、檢舉案件受理、調查過程、調查結果與相關文件製作之紀錄及保存。

七、檢舉案件之處理情形，應適度以書面或其他方式通知檢舉人。

被檢舉人為董（理）事、監察人（監事）或職責相當於副總經理以上之管理階層者，調查報告應陳報至監察人（監事、監事會）或審計委員會複審。

保險業調查後發現為重大偶發事件或違法案件，應主動向相關機關通報或告發。

保險業應定期對所屬人員，辦理檢舉制度之宣導及教育訓練。

第三十三條　保險業總機構法令遵循單位、營業單位、商品開發管理單位、資金運用單位、資訊單位、資產保管單位、其他管理單位及國外分公司應指派人員擔任該單位法令遵循主管，負責辦理法令遵循業務。國外分公司法令遵循主管之設置應符合當地法令規定及當地主管機關之要求，除有下列情事者外，應為專任：

一、兼任防制洗錢及打擊資恐主管。

二、依當地法令明定得兼任無職務衝突之其他職務。

三、當地法令未明確規定，於與當地主管機關溝通並確認後，報經主管機關備查者，得兼任無職務衝突之其他職務。

保險業總機構法令遵循單位主管及所屬人員、營業單位、商品開發管理單位、資金運用單位、資訊單位、資產保管單位、其他管理單位及國外分公司之法令遵循主管，應於就任前或就任後半年內具下列資格條件之一：

一、曾任金融機構法令遵循人員或主管，合計滿五年者。

二、參加主管機關認定機構所舉辦三十小時以上課程，並經考試及格且取得結業證書。

三、國外分公司法令遵循主管係自當地聘任者，依董（理）事會通過之評估辦法自行評估，或經當地主管機關審查認可，足證其已具備熟知當地法令規定之相關能力。

四、營業單位、商品開發管理單位、資金運用單位、資訊單位、資產保管單位、其他管理單位之法令遵循主管得依保險業自行擬訂之具體訓練計畫，參加所屬金融控股公司或保險業自行舉辦三十小時以上相關訓練課程及測驗，足證其已具備熟知單位所需法令規定之相關能力。

各單位應擬訂法令遵循手冊，報經總機構法令遵循主管核可後，轉報總經理核定實施。

法令遵循手冊至少應包括：

一、各項業務應採行之法令遵循程序。

二、各項業務應遵循之法令規章。

三、違反法令規章之處理程序。

四、法令遵循業務之自行評估程序。

五、法令遵循主管名冊。

保險業設有國外分公司者，法令遵循單位應督導國外分公司辦理下列事項：

一、蒐集當地保險法規資料、落實執行法令遵循自行評估作業、確保法令遵循主管適任性及法令遵循資源（含人員、配備及訓練）是否適足等事項，以確保遵守其所在地國家之法令。

二、建立法令遵循風險之自行評估及監控機制，對於其中業務規模大、複雜度或風險程度高者，並應委請當地外部獨立專家驗證其法令遵循風險自行評估及監控機制之有效性。

第三十八條　保險業應於內部控制制度中，訂定對子公司必要之控制作業，並考量該子公司所在地政府法令規章之規定及實際營運之性質，督促其子公司建立內部控制制度。

保險業應建立集團整體性防制洗錢及打擊資恐計畫，包括在符合國外分公司（或子公司）當地法令下，以防制洗錢及打擊資恐為目的之集團內資訊分享政策及程序。

保險業應依子公司業務風險特性及其內部稽核執行情形，於年度稽核計畫中訂定對子公司之查核計畫。

保險業之子公司應向母公司陳報董（理）事會議紀錄、會計師查核報告、金融檢查機關檢查報告或其他有關資料，已設置內部稽核單位之子公司，並應將稽核計畫、內部稽核報告所提重大缺失事項及改善辦理情形併同陳報，由母公司予以審核，並督導子公司改善辦理。

總稽核應定期對子公司內部稽核作業之成效加以考核，經報告董（理）事會考核結果後，將其結果送子公司董（理）事會作為人事考評之依據。

第四十一條　本辦法自發布日施行。

中華民國一百零一年二月四日修正之第五條條文，除金融消費者保護之管理自一百年十二月三十日施行外，自發布後三個月施行。

中華民國一百零七年五月二十九日修正之第三十二條之二修正條文，自發布後六個月施行。

附表一

＿＿＿＿＿＿＿＿資訊安全整體執行情形聲明書

謹代表○○○○（保險業名稱）聲明本公司/合作社於○○年○○月○○日至○○年○○月○○日確實遵循「 保險業內部控制及稽核制度實施辦法」第 六條、第六條之一規定，及同業公會所訂資訊安全自律規範。經審慎評估，本年度資訊安全整體執行情形，除附表所列事項外，均能確實有效執行。如有虛偽，願負法律責任。

此致

金融監督管理委員會

聲明人

董（理）事長（主席）：　（簽章）

總經理：　（簽章）

總稽核：　（簽章）

資安專責單位主管：　（簽章）

中　華　民　國　年　月　日

資訊安全整體執行情形應加強事項及改善計畫

（基準日：　年　月　日）

應加強事項	改善措施	預定完成改善時間

附表二

○○○○保險股份有限公司
內部控制制度聲明書

本公司○○年○○月○○日至○○年○○月○○日之內部控制制度，依據自行檢查之結果，謹聲明如下：

一、本公司確知建立、實施和管理內部控制制度係董(理)事會及管理階層之責任，本公司業已建立此一制度。內部控制制度之目的係在對營運、財務報導及法令遵循等目標之達成，提供合理之確保。營運之目標係在追求營運之效果及效率，包括獲利、績效及保障資產安全等目標；財務之報導目標係在追求對外之財務報導為可靠；法令遵循之目標則在追求相關法令之遵循。法令遵循制度係達成法令遵循目標內部控制制度之一部分；財務紀錄及報表係依保險法及相關規定編製、編製基礎前後一致，且係財務報導內部控制制度之部分成果。

二、內部控制制度有其先天限制，不論設計如何完善，有效之內部控制制度亦僅能對上述三項目標之達成提供合理之確保；而且，由於環境、情況之改變，內部控制制度之有效性可能隨之改變。惟本公司之內部控制制度設有自我監督之機制，缺失一經辨認，本公司即採取更正之行動。

三、本公司係依據金融監督管理委員會訂頒保險業內部控制及稽核制度實施辦法(以下簡稱「實施辦法」)之規定判斷本公司內部控制制度之設計及執行是否有效，上項判斷之作成亦依據「實施辦法」規定之內部控制制度有效性之判斷項目。內部控制制度劃分為五個組成要素：1.控制環境，2.風險評估，3. 控制作業，4.資訊與溝通，及5.監督作業。每個組成要素又包括若干判斷項目，前述項目請參見「實施辦法」之規定。

四、本公司業已採用上述內部控制制度判斷項目，檢查內部控制制度設計及執行之有效性。

五、本公司基於前項檢查結果，認為上開期間之內部控制制度(包括

營運、財務報導及法令遵循)之設計及執行係屬有效，除附表所列事項外，能合理確保董(理)事會及經理人業已知悉營運目標達成之程度、財務報導及法令遵循目標業已達成；亦認為財務紀錄及報表係依保險法及有關規定編製，編製基礎前後一致，其正確性係允當。

六、屬股票公開發行公司者，應增列：本聲明書將成為本公司年報及公開說明書之主要內容，上述公開之內容如有虛偽、隱匿等不法情事，將涉及證券交易法第二十條、第三十二條、第一百七十一條、第一百七十四條或保險法等相關規定之法律責任。

七、本聲明書業經本公司○○年○○月○○日董(理)事會通過。

此致

金融監督管理委員會

聲明人：

董（理）事長（主席）：　（簽章）

總經理：　（簽章）

總稽核：　（簽章）

總機構法令遵循主管：　（簽章）

中　華　民　國　　年　　月　　日

_____內部控制制度應加強事項及改善計畫

（基準日：　年　月　日）

應加強事項	改善措施	預定完成改善時間

本則命令之總說明及對照表請參閱行政院公報資訊網（http://gazette.nat.gov.tw/）。