# 保險業內部控制及稽核制度實施辦法第六條之一、第六條之二修正草案總說明

保險業內部控制及稽核制度實施辦法（以下簡稱本辦法）自九十年十二月二十日發布施行後，歷經十三次修正，最近一次修正公布日期為一百十三年五月七日。鑒於近年保險業數位化程度加速，相應之資訊安全防護機制需予以強化，及配合金融監督管理委員會一百十一年十二月二十七日發布之金融資安行動方案二點零，爰修正本辦法第六條之一及第六條之二，其修正要點如下：

一、擴大資訊安全長與獨立行使職權之資訊安全專責單位之設置範圍，為前一年度經會計師查核簽證資產規模達新臺幣三千億元，或前一年度網路投保保費收入達新臺幣五億元者，並明定資訊安全長之權責。另增訂資訊人員每年應受訓時數。（修正條文第六條之一）

二、明定資訊安全專責單位之權責。（修正條文第六條之二）

# 保險業內部控制及稽核制度實施辦法第六條之一、第六條之二修正草案條文對照表

| 修正條文 | 現行條文 | 說明 |
| --- | --- | --- |
| 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。<br>保險業前一年度經會計師查核簽證之資產總額達新臺幣三千億元，或前一年度網路投保保費收入達新臺幣五億元者，應指派副總經理以上或職責相當之人兼任資訊安全長，綜理資訊安全政策推動及資源調度事務，且應設置獨立行使職權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。<br>保險業資訊安全長每年應向董(理)事會報告前一年度資訊安全整體執行情形，並及時報告重大資安問題。<br>保險業資訊安全專責單位每年應將前一年度資訊安全整體執行情形，由資訊安全長（無資訊安全長者，由資訊安全專責單位主管）與第二十五條第一項人員聯名出具內部控制制度聲明書，提報董 | 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。<br>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，應指派副總經理以上或職責相當之人兼任資訊安全長，綜理資訊安全政策推動及資源調度事務，且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。<br>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，由資訊安全長(無資訊安全長者，由資訊安全專責單位主管）與第二十五條第一項人員聯名出具內部控制制度聲明書，提報董(理)事會通過。<br>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 | 一、金融監督管理委員會於一百十一年十二月二十七日發布金融資安行動方案二點零，推動資產或資本達一定規模或電子交易達一定比例者，擴大其設置資訊安全長範圍。復考量近年保險業數位化程度加速，且外在資訊安全威脅日益增加，相應之資訊安全機制需予以強化，為確保保險業在快速數位化的環境中保持競爭力，爰修正第二項設置資訊安全長及獨立行使職權之資訊安全專責單位之標準，由前一年度經會計師查核簽證資產規模達新臺幣一兆元以上，調整為達新臺幣三千億元，或前一年度網路投保保費收入達新臺幣五億元，並酌作文字修正。<br>二、參考美國紐約州金融服務署(NYDFS)於於一百十二年十一月修正發布資安規範(SECOND AMENDMENT TO 23 NYCRR 500)，新增第三項規定，明定資訊安全長之權責。其餘項次順移。<br>三、現行第三項前段屬資訊安全專責單位之權責事 |

| | | |
|---|---|---|
| （理）事會通過。<br>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；其他資訊從業人員則每年至少應接受六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。<br>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。 | 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。<br>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。 | 項，移列至第六條之二規定。<br>四、考量資訊人員職責與資訊安全密切相關，爰修正第五項，增訂該等人員每年至少應接受六小時以上資訊安全專業課程訓練或職能訓練，並酌作文字修正。<br>五、第六項所指「符合適用條件起」，涵蓋如本次因法規修正以致符合適用條件之情形，併此敘明。 |
| 第六條之二　保險業資訊安全專責單位應辦理事項至少包括：<br>一、負責資訊安全管理制度之規劃、執行與監控，以控管資訊安全風險。<br>二、督導各單位落實資訊安全管理制度，並確保資通安全及資訊之機密性、完整性與可用性。<br>三、建立資通安全防護、資通安全情資之評估因應與資通安全事件通報及應變相關機制。<br>四、每年應將前一年度資訊安全整體執行情形，納入第二十五條第一項內部控制制度執行情形評估。 | 第六條之一第三項　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，由資訊安全長（無資訊安全長者，由資訊安全專責單位主管）與第二十五條第一項人員聯名出具內部控制制度聲明書，提報董（理）事會通過。 | 一、本條新增，由現行條文第六條之一移列規定。<br>二、明定資訊安全專責單位權責，涵蓋金融跨業或與第三方服務供應商間之安全控管，以及資安情資因應處理及資通安全事件之處置程序完整性。<br>三、現行第六條之一第三項所定資訊安全專責單位應辦事項，移列至第一款及第四款規範，並考量內部控制制度執行情形評估包含資訊安全執行情形，爰於第四款增訂後段規定，以符實際。 |