

## 財產保險公司檢查手冊(異動版)

### 一、財務狀況之查核(共 3 項)

| 項目編號                     | 查核事項  |   | 法令規章   | 說明      |
|--------------------------|---|---|--|---------|
|                          | 修正後   | 修正前   |  |         |
| 1.2.4.4                  | ④保險公司辦理強制汽車責任保險是否依主管機關規定之格式編製各種準備金計算表及相關報表，並經相關法令查核簽證後，於會計年度結束日起三個月內報主管機關？  | ④保險公司辦理強制汽車責任保險是否依主管機關規定之格式編製各種準備金計算表及相關報表，並經相關法令查核簽證後，於會計年度結束日起三個月內報主管機關？  | 「 <u>強制汽車責任保險監理報表</u> 」  | 新增法令規章。 |
| 1.2.7<br>(自 115.1.1 起適用) | (7)準備金之查核<br>直接承保業務準備金之查核：是否依保險商品性質，分別依國際財務報導準則第 17 號、第 9 號及第 15 號公報所規定適用之衡量模型計算保險合約負債、金融負債、服務合約負債，以及基於業務屬性提存各項準備金。 | (7)準備金之查核<br>直接承保業務準備金之查核：是否依保險商品性質，分別依國際財務報導準則第 17 號、第 9 號及第 15 號公報所規定適用之衡量模型計算保險合約負債、金融負債、服務合約負債，以及基於業務屬性提存各項準備金。 | 1.保險法第 145 條<br>2.保險業各種準備金提存辦法第 3 及第 7 條<br>3.保險業簽證精算人員及外部複核精算人員管理辦法第 4 條<br>4.本會 104.6.22 金管保財字第 10402506871 號令<br>5.「 <u>強制汽車責任保險各種準備金提存方式</u> 」及「 <u>強制汽車責任保險監理報表</u> 」 | 新增法令規章。 |

| 項目編號 | 查核事項  |                                  | 法令規章   | 說明           |
|------|---|----------------------------------|--|--------------|
|      | 修正後   | 修正前                              |  |              |
| 3.5  | 5.各項自有資本、風險資本之計算公式及為強化財務結構而發行具資本性質之債券是否依本會保險局之規定辦理。 | 5.各項自有資本、風險資本之計算公式是否依本會保險局之規定辦理。 | 保險業資本適足性管理辦法第2條、第2-1條、第4條及「保險公司發行具資本性質債券應注意事項」 | 新增查核事項及法令規章。 |

## 二、保險業務之查核（共3項）

| 項目編號 | 查核事項   |   | 法令規章  | 說明      |
|------|--|---|---|---------|
|      | 修正後  | 修正前   |   |         |
| 1.10 | 10.除主管機關另有規定者外，業務員從事招攬，是否取得要保人及被保險人親簽之投保相關文件？招攬涉及人身保險之商品者，是否親晤要保人及被保險人？業務員招攬之保件，是否於要保書上簽章並記載其登錄字號？授權所屬業務員以帳號、密碼於要保文件簽名是否符合「保險業務員所屬公司授權其業務員以帳號、密碼於要保文件簽名」控管措施，並將控管措施納入內部控制及內部稽核項目辦理？是否有接受第三方業者之媒合或派遣與消費者洽訂保險契約？ | 10. 除主管機關另有規定者外，業務員從事招攬，是否取得要保人及被保險人親簽之投保相關文件？招攬涉及人身保險之商品者，是否親晤要保人及被保險人？業務員招攬之保件，是否於要保書上簽章並記載其登錄字號？授權所屬業務員以帳號、密碼於要保文件簽名是否符合「保險業務員所屬公司授權其業務員以帳號、密碼於要保文件簽名」控管措施，並將控管措施納入內部控制及內部稽核項目辦理？是否有接受第三方業者之媒合或派遣與消費者洽訂保險契約？ | 1.保險業務員管理規則第15條及本會113.10.23金管保壽字第11304936921號解釋令<br>2.本會105.4.8金管保壽字第10502540567號令<br>3.本會保險局108.7.22保局(產)字第10804163190號函<br>4.本會110.1.4金管保綜字第10904184633號函<br>5.「保險業務員所屬公司授權其業務員以帳號、密碼於要保文件簽名」控管措施 | 新增法令規章。 |

| 項目編號     | 查核事項  |   | 法令規章  | 說明      |
|----------|---|---|---|---------|
|          | 修正後   | 修正前   |   |         |
| 2.5      | 5.要保書是否經要保人或被保險人簽章？有無由業務人員代為簽章之情形？若屬「其他法令規定足資證明要保人投保意願之相關證據或填報內容」之情形，是否符合相關條件或已取具足資證明要保人投保意願之相關證據，及將配套措施及相關證明方式，納入內部控制作業？ | 5.要保書是否經要保人或被保險人簽章？有無由業務人員代為簽章之情形？若屬「其他法令規定足資證明要保人投保意願之相關證據或填報內容」之情形，是否符合相關條件或已取具足資證明要保人投保意願之相關證據，及將配套措施及相關證明方式，納入內部控制作業？ | 1.保險業招攬及核保理賠辦法第7條第1項第12款第4目及 <del>本會112.7.27金管保壽字第11204924231號解釋令</del> 本會113.9.9金管保壽字第11304928911號令<br>2.本會106.7.28金管保產字第10602524244號函轉本會106.7.28金管保產字第10602524241號令 | 修正法令規章。 |
| 8<br>8.1 | (八)對保經代業務往來管理之查核<br>1.保險公司對於與保經代業務往來之管理(包括法令規定保險業應要求保經代遵循事項之監督管理)是否妥適？  | (八)對保經代業務往來管理之查核<br>1.保險公司對於與保經代業務往來之管理(包括法令規定保險業應要求保經代遵循事項之監督管理)是否妥適？  | 1.本會109.12.28金管保壽字第10904947221號令<br>2.本會110.1.11金管保壽字第1100490103號函<br>3.「保險業與保險代理人合約範本」及附錄代理業務績效考核表<br>4.銀行、證券商、保險公司、保險代理人或保險經紀人合作推廣契約書範本                             | 新增法令規章  |

### 三、資金運用項目之查核（共14項）

| 項目編號  | 查核事項   |  | 法令規章                      | 說明         |
|---|--|--|---------------------------|------------|
|   | 修正後  | 修正前  |                           |            |
| 3.4<br><del>3.4.1</del><br><del>3.4.2</del><br><del>3.4.3</del><br><del>3.4.4</del><br><del>3.4.5</del><br><del>3.4.6</del> | 4.保險業購買國內公開發行但未在證券交易所上市（以下簡稱未上市）或證券商營業處所買賣（以下簡稱未上櫃）之有價證券種類是否以下列為限：<br>(1)股票。<br>(2)有擔保公司債。<br>(3)最近一年內經信用評等機構評等達一定等級以上公司發行之普通公司債、可轉換公司債或附認股權公司債。<br>(4)依證券投資信託及顧問法發行之證券投資信託基金受益憑證及依信託業法發行之共同信託基金受益憑證。<br>(5)依金融資產證券化條例或不動產證券化條例發行之受益證券及資產基礎證券。<br>(6)其他經主管機關核准購買之有價證券。 | 4.保險業購買國內公開發行但未在證券交易所上市（以下簡稱未上市）或證券商營業處所買賣（以下簡稱未上櫃）之有價證券種類是否以下列為限：<br>(1)股票。<br>(2)有擔保公司債。<br>(3)最近一年內經信用評等機構評等達一定等級以上公司發行之普通公司債、可轉換公司債或附認股權公司債。<br>(4)依證券投資信託及顧問法發行之證券投資信託基金受益憑證及依信託業法發行之共同信託基金受益憑證。<br>(5)依金融資產證券化條例或不動產證券化條例發行之受益證券及資產基礎證券。<br>(6)其他經主管機關核准購買之有價證券。 | 保險業投資未上市未上櫃及私募有價證券管理辦法第3條 | 修正項次。      |
| <u>3.4.1</u>  | (1)前述(1)及(3)之發行人須最近二期不同年度經會計師簽證之年化稅後淨利平均為正者。但符合下列情形之一者，不在此限：   | 前述(1)及(3)之發行人須最近二期不同年度經會計師簽證之年化稅後淨利平均為正者。但符合下列情形之一者，不在此限：  |                           | 修正查核事項及項次。 |

| 項目編號             | 查核事項   |   | 法令規章  | 說明    |
|------------------|--|---|---|-------|
|                  | 修正後  | 修正前   |   |       |
| 3.4.1.1          | ①保險業自有資本與風險資本之比率達法定標準一點五倍以上。   | (1)保險業自有資本與風險資本之比率達百分之三百以上。   |   |       |
| 3.4.1.2          | ②保險業自有資本與風險資本之比率達法定標準以上，經其董事會決議同意。   | (2)保險業自有資本與風險資本之比率達百分之二百以上，經其董事會決議同意。   |   |       |
| 3.4.2            | (2)保險人購買未上市櫃有擔保公司債之保證人及未上市櫃普通公司債、可轉換公司債或附認股權公司債之發行人須經信用評等機構評定，長期債務信用評等達 twBBB 一等級或相當等級以上者。 | 保險人購買未上市櫃有擔保公司債之保證人及未上市櫃普通公司債、可轉換公司債或附認股權公司債之發行人須經信用評等機構評定，長期債務信用評等達 twBBB 一等級或相當等級以上者。 |   | 修正項次。 |
| 3.5              | 5.保險業購買國內私募有價證券之種類是否以下列為限（若屬公開發行公司應注意是否洽請會計師出具交易價格合理性表示意見）：                                | 5.保險業購買國內私募有價證券之種類是否以下列為限（若屬公開發行公司應注意是否洽請會計師出具交易價格合理性表示意見）：                             | 1.保險業投資未上市未上市櫃及私募有價證券管理辦法第4條<br>2.公開發行公司取得或處分資產處理準則 | 修正項次。 |
| <del>3.5.1</del> | (1)公開發行股票公司之股票。  | (1)公開發行股票公司之股票。   |   |       |
| <del>3.5.2</del> | (2)公開發行股票公司之有擔保公司債。  | (2)公開發行股票公司之有擔保公司債。   |   |       |
| <del>3.5.3</del> | (3)最近一年內經信用評等機構評等達一定等級以上公開發行股票公司之普通公司債、可轉換公司債或附認股權公司債。                                     | (3)最近一年內經信用評等機構評等達一定等級以上公開發行股票公司之普通公司債、可轉換公司債或附認股權公司債。                                  |   |       |
| <del>3.5.4</del> | (4)證券投資信託事業依證券投資信託及顧問法私募之證券投資  | (4)證券投資信託事業依證券投資信託及顧問法私募之證券投資   |   |       |

| 項目編號                                   | 查核事項  |  | 法令規章 | 說明         |
|--|---|--|------|------------|
|  | 修正後   | 修正前  |      |            |
| <del>3.5.5</del><br><del>3.5.6</del>   | 信託基金受益憑證。<br>(5)依金融資產證券化條例或不動產證券化條例私募之受益證券或資產基礎證券。<br>(6)其他經主管機關核准購買之有價證券。  | 基金受益憑證。<br>(5)依金融資產證券化條例或不動產證券化條例私募之受益證券或資產基礎證券。<br>(6)其他經主管機關核准購買之有價證券。   |      |            |
| 3.5.1<br>3.5.1.1<br>3.5.1.2<br>3.5.1.3 | (1)前述(1)及(3)之發行人須最近二期不同年度經會計師簽證之年化稅後淨利平均為正者。但符合下列情形之一者，不在此限：<br>①發行人為上市公司或上櫃公司。<br>②保險業自有資本與風險資本之比率達法定標準一點五倍以上。<br>③保險業自有資本與風險資本之比率達法定標準以上，經其董事會決議同意。 | 前述(1)及(3)之發行人須最近二期不同年度經會計師簽證之年化稅後淨利平均為正者。但符合下列情形之一者，不在此限：<br>(1)發行人為上市公司或上櫃公司。<br>(2)保險業自有資本與風險資本之比率達百分之三百以上。<br>(3)保險業自有資本與風險資本之比率達百分之二百以上，經其董事會決議同意。 |      | 修正查核事項及項次。 |
| 3.5.2                                  | (2)保險業購買前述私募有擔保公司債之保證人及私募普通公司債、可轉換公司債或附認股權公司債之發行人須經信用評等機構評定，長期債務信用評等達 twBBB 一等級或相當等級以上者。  | 保險業購買前述私募有擔保公司債之保證人及私募普通公司債、可轉換公司債或附認股權公司債之發行人須經信用評等機構評定，長期債務信用評等達 twBBB 一等級或相當等級以上者。  |      | 修正項次。      |
| 3.6.4                                  | (4)保險業擔任不動產投資信託之發起人者，得依「受託機構募集或私  | (4)保險業擔任不動產投資信託之發起人者，得依「受託機構募集或私募  |      | 修正查核事項。    |

| 項目編號   | 查核事項   |   | 法令規章                                  | 說明      |
|--------|--|---|---------------------------------------|---------|
|        | 修正後  | 修正前   |                                       |         |
|        | 募不動產投資信託或資產信託受益證券處理辦法」第八條規定，購買該不動產投資信託所發行之不動產投資信託受益證券。   | 不動產投資信託或資產信託受益證券處理辦法」第六條規定，購買該不動產投資信託所發行之不動產投資信託受益證券。   |                                       |         |
| 3.7.3  | (3)以結構型債券或分割本金債券搭配外國有價證券為資產池所發行之受益證券或資產基礎證券，其外國有價證券之種類及債券信用評等等級，應符合「 <u>保險業辦理國外投資管理辦法</u> 」規定，且資產池內之國內有價證券全數到期後，保險業所持有之受益證券或資產基礎證券，應於到期日起三個月內併入國外投資額度計算。 | (3)以結構型債券或分割本金債券搭配外國有價證券為資產池所發行之受益證券或資產基礎證券，其外國有價證券之種類及債券信用評等等級，應符合「 <u>保險業辦理國外投資範圍及內容準則</u> 」規定，且資產池內之國內有價證券全數到期後，保險業所持有之受益證券或資產基礎證券，應於到期日起三個月內併入國外投資額度計算。 |                                       | 修正查核事項。 |
| 3.8    | 8.保險業自有資本與風險資本之比率未達法定標準者，其購買未上市、未上櫃及私募有價證券，是否遵守下列規定：   | 8. 保險業自有資本與風險資本之比率未達百分之二百者，其購買未上市、未上櫃及私募有價證券，是否遵守下列規定：  | 保險業投資未上市未上櫃及私募有價證券管理辦法第7條             | 修正查核事項。 |
| 6.5.8  | (8)其他主管機關指定之事項。  | (8)其他主管機關指定之事項。   | 本會 113.9.26 金管保財字第 11301451251 號解釋令   | 新增法令規章。 |
| 6.10.5 | (5)被投資對象為依促進民間參與公共建設逕為辦理投資之案件，是否符合法令規定之投資金額及條件（但保險業依「 <u>保險業資金專案運</u>  | (5)被投資對象為依促進民間參與公共建設逕為辦理投資之案件，是否符合法令規定之投資金額及條件（但保險業依「 <u>保險業資金專案運</u>   | 1.保險業辦理保險業資金辦理專案運用公共及社會福利事業投資管理辦法第10條 | 修正查核事項。 |

| 項目編號 | 查核事項  |   | 法令規章   | 說明      |
|------|---|---|--|---------|
|      | 修正後   | 修正前   |  |         |
|      | <p>用公共及社會福利投資管理辦法」第 3 條及第 4 條辦理投資時，被投資對象於開發階段依環境影響評估法應實施環境影響評估者，不在此限)？</p> <p>註:保險業辦理保險業資金辦理專案運用公共及社會福利事業投資管理辦法第 10 條第 1 項之投資，其最近一期之自有資本與風險資本之比率應符合<u>法定標準</u>。</p> | <p>用公共及社會福利投資管理辦法」第 3 條及第 4 條辦理投資時，被投資對象於開發階段依環境影響評估法應實施環境影響評估者，不在此限)？</p> <p>註:保險業辦理保險業資金辦理專案運用公共及社會福利事業投資管理辦法第 10 條第 1 項之投資，其最近一期之自有資本與風險資本比率應符合保險法第 143 條之 4 第 1 項規定(不得低於百分之二百)。</p> | <p>2.本會 111.1.28 金管保財字第 11004365983 號令</p> <p>3.本會 111.1.28 金管保財字第 11004365984 號令</p>                              |         |
| 7.4  | 4.保險業資金投資第 5 條第 1 款至第 7 款有價證券是否符合規定等級、條件及限額？  | 4.保險業資金投資第 5 條第 1 款至第 7 款有價證券是否符合規定等級、條件及限額？  | 「保險業辦理國外投資管理辦法」第 6 條及「 <u>保險業差異化管理獎勵措施提高資產配置彈性權利計算標準</u> 」   | 新增法令規章。 |
| 7.5  | 5.保險業資金投資第 5 條第 8 款所稱外國證券集中交易市場或店頭市場交易之股權或債權憑證種類是否符合規定種類、條件、等級及限額？  | 5.保險業資金投資第 5 條第 8 款所稱外國證券集中交易市場或店頭市場交易之股權或債權憑證種類是否符合規定種類、條件、等級及限額？  | <p>1.保險業辦理國外投資管理辦法第 7 條</p> <p>2.本會 108.2.1 金管保財字第 10701970070 號函</p> <p>3.「<u>保險業差異化管理獎勵措施提高資產配置彈性權利計算標準</u>」</p> | 新增法令規章。 |
| 7.6  | 6.保險業資金投資第 5 條第 9 款所稱   | 6.保險業資金投資第 5 條第 9 款所稱   | 1.保險業辦理國外投資管   | 新增法令規章。 |

| 項目編號 | 查核事項                         |                              | 法令規章   | 說明 |
|------|------------------------------|------------------------------|--|----|
|      | 修正後                          | 修正前                          |  |    |
|      | 國外表彰基金之有價證券種類是否符合規定種類、條件及限額? | 國外表彰基金之有價證券種類是否符合規定種類、條件及限額? | 理辦法第 8 條<br>2.本會 97.11.6.金管保一字第 09702506821 號公告<br>3.本會 106.3.31 金管保財字第 10602501090 號函<br>4.本會 111.1.28 金管保財字第 11104902762 號令<br>5.「 <u>保險業差異化管理獎勵措施提高資產配置彈性權利計算標準</u> 」 |    |

#### 四、資訊作業之查核(共 19 項)

| 項目編號    | 查核事項   |  | 法令規章                        | 說明            |
|---------|--|--|-----------------------------|---------------|
|         | 修正後  | 修正前  |                             |               |
| 1.1.5.2 | (2)是否 <u>定義人員角色及責任、區隔相互衝突的角色，並建立資訊人員代理制度，以及視實際需要建立輪調制度？</u>            | (2)是否建立資訊人員代理制度，並視實際需要建立輪調制度？                | <u>保險業辦理資訊安全防護自律規範第 4 條</u> | 修正查核事項及新增法令規章 |
| 1.2.2   | 2.前述規範有關操作、管理、查核等各方面之規定是否完整？ <u>是否每年檢討資訊安全政策及資訊作業相關管理與操作規範等，並於發生重大</u> | 2.前述規範有關操作、管理、查核等各方面之規定是否完整？是否付諸實施，並適時檢討、修訂？ | <u>保險業辦理資訊安全防護自律規範第 4 條</u> | 修正查核事項及新增法令規章 |

| 項目編號                  | 查核事項   |     | 法令規章                        | 說明          |
|-----------------------|--|-----|-----------------------------|-------------|
|                       | 修正後  | 修正前 |                             |             |
|                       | <u>變更(如新頒布法令法規)時審查,以持續確保其合宜性、適切性及有效性?</u>  |     |                             |             |
| 1.2.3.3               | <u>(3)是否依據作業流程,識別人員、表單、設備、軟體、系統等資產,建立資產清冊、網路架構圖、組織架構圖及負責人,並定期清點以維持其正確性?</u>  |     | <u>保險業辦理資訊安全防護自律規範第4條</u>   | 新增查核事項及法令規章 |
| 1.3.4                 | <u>4.對於足以影響保險業信譽、或危及保險業正常營運、或金融秩序情事之資通安全事件,是否依「保險業通報重大偶發事件之範圍申報程序及其他應遵循事項」規定辦理通報?</u>  |     | <u>保險業辦理資訊安全防護自律規範第13條</u>  | 新增查核事項及法令規章 |
| 1.4<br>1.4.1<br>1.4.2 | <u>(四)營運環境管理人員之遵循情形</u><br><u>1.是否建立人員之註冊、異動及撤銷註冊程序,並配置適當之存取權限,必要時得限定人員使用之機器及網路位置(IP),另人員離(調)職時是否已移除權限?</u><br><u>2.是否列管硬體設備、應用軟體、系統軟體之最高權限帳號,及具有程式異動與參數變更權限之帳號?</u> |     | <u>保險業辦理資訊安全防護自律規範第4條之1</u> | 新增查核事項及法令規章 |

| 項目編號    | 查核事項   |     | 法令規章 | 說明 |
|---------|--|-----|------|----|
|         | 修正後  | 修正前 |      |    |
| 1.4.3   | 3.人員超過一定時間未操作個人電腦時，是否有設定密碼啟動螢幕保護程式或登出系統？                       |     |      |    |
| 1.4.4   | 4.登入作業系統進行系統異動或資料庫存取時，是否留存操作紀錄，並於使用後變更密碼？如無法變更密碼者，是否建立監控及覆核機制？ |     |      |    |
| 1.4.5   | 5.帳號是否採一人一號管理？如有共同使用需求，是否有其他補強管控方式，並留存操作紀錄且可識別使用人員身分？          |     |      |    |
| 1.4.6   | 6.採用固定密碼進行身分確認時，是否符合下列要求：                                      |     |      |    |
| 1.4.6.1 | (1)訂定密碼檢核邏輯。   |     |      |    |
| 1.4.6.2 | (2)使用後三個月內應變更密碼。   |     |      |    |
| 1.4.6.3 | (3)提供給系統使用之帳號應採取適當之管控措施(如限制人工登入、監控告警)。                         |     |      |    |
| 1.4.7   | 7.是否列管並限制使用加解密程式、具變更權限之公用程式(如資料庫工具程式)，並保留稽核軌跡？                 |     |      |    |
| 1.4.8   | 8.最高權限帳號使用時，是否先取   |     |      |    |

| 項目編號                           | 查核事項   |                                     | 法令規章          | 說明                    |
|--------------------------------|--|-------------------------------------|---------------|-----------------------|
|                                | 修正後  | 修正前                                 |               |                       |
| 1.4.9                          | 得權責主管或授權人員同意，並保留稽核軌跡？  |                                     |               |                       |
| 1.4.10                         | 9.對於具最高權限帳號、特殊功能(如程式或軟體異動、參數或組態變更權限等)權限帳號，是否和日常維運用帳號區隔，並每月抽查使用結果？如為核心資通系統，是否於該等帳號使用後，覆核使用結果？ |                                     |               |                       |
| 1.4.11                         | 10.對於提供網際網路服務之伺服器 AD(網域服務)主機之最高權限帳號與特殊功能權限帳號，是否採雙因子認證或納入特權帳號管理系統？                            |                                     |               |                       |
|                                | 11.對於第一類及第二類電腦系統，是否依最小權限(least privilege)及僅知原則(need-to-know)配發權限予人員使用，並定期審查帳號、權限之合理性及異常存取紀錄？ |                                     |               |                       |
| 1.5<br><del>1.4</del><br>1.5.1 | (五)內部稽核辦理情形<br><br>1.辦理電子商務業務及行動投保業  | (四)內部稽核辦理情形<br><br>1.辦理電子商務業務及行動投保業 | 1.保險業經營電子商務自律 | 修正項目編號、查核事項項次，及新增法令規章 |

| 項目編號   | 查核事項   |  | 法令規章  | 說明     |
|--|--|--|---|--------|
|  | 修正後  | 修正前  |   |        |
| <del>1.4.1</del><br>1.5.2<br><del>1.4.2</del><br>1.5.3<br><del>1.4.3</del> | <p>務等是否已將其納入內部稽核及自行查核作業規範？是否確依內部稽核作業規範辦理內部稽核？</p> <p>2.內部稽核之範圍是否完整涵蓋各項業務需要之資訊安全控管機制、網路系統使用管理、病毒偵測及預防、委外廠商管理及各項安控作業規範之遵循等？</p> <p>3.內部稽核所發現資訊作業相關缺失事項，是否均送請相關單位辦理改善？並追蹤其改善情形？</p> | <p>務等是否已將其納入內部稽核及自行查核作業規範？是否確依內部稽核作業規範辦理內部稽核？</p> <p>2.內部稽核之範圍是否完整涵蓋各項業務需要之資訊安全控管機制、網路系統使用管理、病毒偵測及預防、委外廠商管理及各項安控作業規範之遵循等？</p> <p>3.內部稽核所發現資訊作業相關缺失事項，是否均送請相關單位辦理改善？並追蹤其改善情形？</p> | <p>規範第 31 條</p> <p><del>2.保險業經營行動服務自律</del></p> <p>規範第 13 條</p>           |        |
| 2  | 二、網路及系統安全控管  | 二、網路及系統安全控管  | <p><del>保險業辦理資訊安全防護</del></p> <p>自律規範</p>                                 | 新增法令規章 |
| 2.2.1  | 1.是否建置一適當之網路系統安全管理措施、關閉非必要之網路服務及限制非必要之連線，以控制網際網路與其內部網路或電腦系統間之活動？   | 1.是否建置一適當之網路系統安全管理措施、關閉非必要之網路服務及限制非必要之連線，以控制網際網路與其內部網路或電腦系統間之活動？   | <p><del>保險業辦理資訊安全防護</del></p> <p>自律規範第 19 條</p>                           | 新增法令規章 |
| 2.4.1.9  | (9)對核心資訊系統與第一類電腦系統中遠距服務、行動服務及電子商務資訊系統置換作業：   | (9)對核心資訊系統置換作業：  | <p>1.本會 108.11.21 金管保財字第 10804957681 號令</p> <p>2.保險業辦理資訊安全防護自律規範第 5 條</p> | 修正查核事項 |
| 2.5.2.1  | (1)端末機使用人員資料(如使用者代   | (1)端末機使用人員資料(如使用者代   | <del>1.保險業辦理資訊安全防護</del>  | 修正法令規章 |

| 項目編號    | 查核事項  |   | 法令規章                                     | 說明     |
|---------|---|---|--|--------|
|         | 修正後   | 修正前   |  |        |
|         | 號、密碼、授權使用範圍等資料)之建檔、變更、註銷是否經申請、核准程序並留存紀錄?是否定期審核資訊系統帳號?   | 號、密碼、授權使用範圍等資料)之建檔、變更、註銷是否經申請、核准程序並留存紀錄?是否定期審核資訊系統帳號?   | <del>自律規範第15條第2及3款</del><br>金融機構資訊系統安全基準 |        |
| 2.5.2.2 | (2)使用者密碼是否可由使用者自行變更?是否有限制最少字元(以超過 8 個字元為宜)?是否有控制密碼有效期限及不得變更為前幾次使用過之密碼?是否以亂碼儲存並控制不得以明碼輸出或顯示?                             | (2)使用者密碼是否可由使用者自行變更?是否有限制最少字元(以超過 7 個字元為宜)?是否有控制密碼有效期限及不得變更為前幾次使用過之密碼?是否以亂碼儲存並控制不得以明碼輸出或顯示?                             |  | 修正查核事項 |
| 2.5.4   | 4.第一類(可由外部 Internet 直接連線之網際網路應用系統及核心資訊系統)、第二類(存放大量客戶資料之系統)電腦系統日誌紀錄管理:   | 4.第一類(可由外部 Internet 直接連線之網際網路應用系統及核心資訊系統)、第二類(存放大量客戶資料之系統)電腦系統日誌紀錄管理:   | 保險業辦理資訊安全防護自律規範第 17 條                    | 修正查核事項 |
| 2.5.4.1 | (1)系統產生之事件日誌紀錄(內容包含但不限於事件類型、發生時間、發生位置、使用者身分識別等資訊)是否有保留機制?除相關法令規定外,日誌紀錄是否至少保留 180 天?如涉及個人資料之日誌紀錄者,保留期限是否依個人資料保護法等相關規定辦理? | (1)系統產生之事件日誌紀錄(內容包含但不限於事件類型、發生時間、發生位置、使用者身分識別等資訊)是否有保留機制?除相關法令規定外,日誌紀錄是否至少保留 180 天?如涉及個人資料之日誌紀錄者,保留期限是否依個人資料保護法等相關規定辦理? |  |        |
| 2.5.4.2 | (2)系統內部時間是否定期進行基準時間源進行同步?   | (2)系統內部時間是否定期進行基準時間源進行同步?   |  |        |

| 項目編號      | 查核事項  |   | 法令規章                   | 說明          |
|-----------|---|---|------------------------|-------------|
|           | 修正後   | 修正前   |                        |             |
| 2.5.4.3   | (3)事件日誌是否設有存取限制，並以適當方式確保完整性；另是否依據事件日誌紀錄之儲存需求，配置容量，且定期將日誌紀錄送至原系統外之其他系統進行集中管理；或建置日誌伺服器？ | (3)事件日誌是否設有存取限制，並以適當方式確保完整性；另是否依據事件日誌紀錄之儲存需求，配置容量，且定期備份日誌紀錄至原系統外之其他系統；或建置日誌伺服器？ |                        |             |
| 2.5.4.4   | (4)是否定期審查系統管理者活動以識別異常或潛在資安事件並保留紀錄，設定合適告警指標並定期檢討修訂；或將相關事件日誌納入資訊安全事件之監控管理機制範圍？          | (4)是否定期審查系統管理者活動以識別異常或潛在資安事件並保留紀錄；或將相關事件日誌納入資訊安全事件之監控管理機制範圍？                    |                        |             |
| 2.5.5     | 5.是否評估各系統產生之事件日誌紀錄（內容包含但不限於事件類型、發生時間、發生位置、使用者身分識別等資訊）之保留機制？                           |   | 保險業辦理資訊安全防護自律規範第 17 條  | 新增查核事項及法令規章 |
| 2.6.5.1.1 | A.是否制定雲端服務管理政策，並定期檢視？   | A.是否制定雲端服務管理政策，並定期檢視？   | 保險業作業委託他人處理應注意事項第 18 條 | 新增法令規章      |
| 2.6.5.1.3 | C.傳輸及儲存客戶資料至雲端服務業者，是否採行客戶資料加密或代碼化等有效保護措施？是否訂定妥適之加密金鑰管理機制？                             | C.傳輸及儲存客戶資料至雲端服務業者，是否採行客戶資料加密或代碼化等有效保護措施？是否訂定妥適之加密金鑰管理機制？                       | 保險業作業委託他人處理應注意事項第 18 條 | 新增法令規章      |
| 2.6.5.1.8 | H.是否具專業技術及資源監督雲端服務業者執行受託作業，或委託專業  |   | 保險業作業委託他人處理應注意事項第 18 條 | 新增查核事項及法令規章 |

| 項目編號         | 查核事項   |     | 法令規章                   | 說明          |
|--------------|--|-----|------------------------|-------------|
|              | 修正後  | 修正前 |                        |             |
|              | <u>第三人輔助監督作業？</u>  |     |                        |             |
| 2.6.5.1.9    | I. <u>對於自行委託，或與委託同一雲端服務業者之金融機構聯合委託具資訊專業之獨立第三人查核雲端服務業者，是否符合下列要求：</u>          |     | 保險業作業委託他人處理應注意事項第 18 條 | 新增查核事項及法令規章 |
| 2.6.5.1.9.1  | a. <u>確認其查核範圍，是否涵蓋雲端服務業者受託處理作業相關之重要系統及控制環節。</u>                              |     |                        |             |
| 2.6.5.1.9.2  | b. <u>評估第三人之適格性，以及其所出具查核報告內容之妥適性。</u>  |     |                        |             |
| 2.6.5.1.9.3  | c. <u>對所委託作業範圍進行查核並出具報告。</u>   |     |                        |             |
| 2.6.5.1.10   | J. <u>對於委託雲端服務業者處理之客戶資料及其儲存地，是否符合下列要求：</u>                                   |     | 保險業作業委託他人處理應注意事項第 18 條 | 新增查核事項及法令規章 |
| 2.6.5.1.10.1 | a. <u>保有指定資料處理及儲存地之權利。</u>   |     |                        |             |
| 2.6.5.1.10.2 | b. <u>境外當地資料保護法規不得低於我國要求。</u>  |     |                        |             |
| 2.6.5.1.10.3 | c. <u>涉及重大性自然人客戶業務資訊系統之客戶資料儲存地以位於我國境內為原則。如位於境外，除經主管機關核准外，客戶重要資料應在我國留存備份。</u> |     |                        |             |

| 項目編號       | 查核事項  |   | 法令規章 | 說明     |
|------------|---|---|------|--------|
|            | 修正後   | 修正前   |      |        |
| 2.6.11.1.5 | E.金融 Fast-ID 是否遵循國際 FIDO 聯盟所訂定之產業技術標準，並符合我國金融行動身分識別聯盟所制訂之相關標準及規範？ | E.FIDO 是否遵循國際 FIDO 聯盟所訂定之產業技術標準，並符合我國金融行動身分識別聯盟所制訂之相關標準及規範？ |      | 修正查核事項 |

### 五、其他事項之查核(共 5 項)

| 項目編號             | 查核事項  |  | 法令規章                  | 說明      |
|------------------|---|--|-----------------------|---------|
|                  | 修正後   | 修正前  |                       |         |
| 5.5              | 5.客戶身分確認程序： <u>國際保險業務分公司是否遵循洗錢防制法、資恐防制法、主管機關所定應取得或驗證之文件、資料或資訊、產壽險公會所定保險業防制洗錢及打擊資恐注意事項範本等規定，確實辦理確認客戶身分程序，並納入內部控制及內部稽核項目？</u> | 6.客戶身分確認程序：  | 國際保險業務分公司管理辦法第 16-1 條 | 整併查核事項。 |
| <del>5.5.1</del> | (刪除)  | (1)國際保險業務分公司是否遵循洗錢防制法、資恐防制法、主管機關所定應取得或驗證之文件、資料或資訊、中華民國產物保險商業同業公會及中華民國人壽保險商業同業公會所定保險業防制洗錢及打擊資恐注意事項範本等規定，確實辦理確認客戶身分程序，並納入內 |                       | 刪除查核事項。 |

| 項目編號             | 查核事項   |  | 法令規章                                  | 說明           |
|------------------|--|--|---------------------------------------|--------------|
|                  | 修正後  | 修正前  |                                       |              |
|                  |  | 部控制及內部稽核項目?  |                                       |              |
| <del>5.5.2</del> | (刪除)   | (2)對本辦法中華民國一百零六年八月十八日發布之條文施行前既有客戶，是否於一百零六年十二月三十一日前重新辦理確認客戶身分程序並檢討其風險程度等級?                                    |                                       | 刪除查核事項。      |
| <del>5.5.3</del> | (刪除)   | (3)就有下列情形者是否立刻辦理上開確認客戶身分程序並檢討其風險程度等級：<br>①對客戶資訊之真實性有所懷疑，如發現該客戶涉及疑似洗錢交易，或客戶之業務往來模式出現重大變動時。<br>②客戶身分資訊定期更新屆至時。 |                                       | 刪除查核事項。      |
| 9.4              | 4.保險業透過「金融行動身分識別(金融 Fast-ID)」辦理資料共享，是否確實依相關規定辦理?應將本業務之人員管理、資料傳輸過程、資訊交換作業、資料儲存作業、紀錄保存及爭議處理機制等安全控管機制，納入保險業內部控制及稽核項目。 |  | 保險業透過「金融行動身分識別(金融 Fast-ID)」辦理資料共享自律規範 | 新增查核事項及法令規章。 |