

財產保險公司檢查手冊(異動版)

一、財務狀況之查核(共 1 項)

項目編號	查核事項		法令規章	說明
	修正後	修正前		
1.3	3.投資性不動產後續衡量採用公允價值模式者，相關配套規範之查核	3 投資性不動產後續衡量採用公允價值模式者，相關配套規範之查核	保險業財務報告編製準則第 9 條第 3 項第 12 款	修訂查核事項及法令規章。
1.3.1	<u>(1) 公允價值之評價，應採收益法或成本法。但 109.5.11 修正發布前，原帳列投資性不動產之後續衡量已採用公允價值模式者，不在此限，並應以正常價格作為公允價值評估之依據，不得以限定價格、特定價格或特殊價格進行評估。</u>	(1) 於選用時之保險負債亦應採公允價值評估。公允價值評估方式則其計算方式由主管機關另定之，保險負債公允價值如大於帳列數，其差額應提列責任準備-保險合約負債公允，並調減保留盈餘。		
1.3.2	<u>(2) 投資性不動產已訂定超過一年以上之租賃契約者，應採收益法評價，並應依下列規定辦理：</u> <u>①現金流量：應依租賃契約為基礎評估，有期末價值者，得加計該期末價值之現值。</u> <u>②分析期間：收益無一定期限者，分析期間以不得逾物理耐用年限，收益有特定期限者，則應依剩餘期間估算。</u> <u>③折現率：限採風險溢酬法，以一定利率為基準，加計投資性不動產之個別特性估算。所稱一定利率</u>	(2) 自選定採用之時起，應就投資用不動產逐筆委託外部聯合估價師事務所進行評價、應於資產負債表日檢討評估公允價值之有效性，洽估價師檢視原估價報告，以決定是否重新出具估價報告，以及應至少每半年取具估價師出具之估價報告。 (3) 單筆評估金額達十億元以上者，應由二家以上之聯合估價師事務所進行估價。 (4) 不動產估價應以正常價格作為公允價值評估之依據，不得以限定價格、特定價格或特殊價格進行評估。		

項目編號	查核事項		法令規章	說明
	修正後	修正前		
1.3.3	<u>為基準，不得低於中華郵政股份有限公司牌告二年期郵政定期儲金小額存款機動利率加五碼。</u>	(5) 投資性不動產於取得後之首次委外鑑價報告不得由原取得不動產之不動產估價師及聯合估價師事務所辦理鑑價。		
1.3.4	<u>(3) 投資性不動產未訂定超過一年以上租賃契約或契約終止、解除、失效等已超過一年以上者，應採用成本法。</u>	(6) 不動產估價師及聯合估價師事務所每三年應更換一次，更換前後不得為同一估價師及聯合估價師事務所，且於更換後一年內不得再委任更換前之估價師及聯合估價師事務所。		
1.3.5	<u>(4) 保險負債之後續衡量應依本會每年指定之負債公允價值評估條件進行評估。保險負債公允價值超過帳列數者，應提具補強計畫，補強計畫列有準備金增提數者，應將該增提數列入責任準備金並調減保留盈餘。</u>	(7) 委外之聯合估價師事務所及其所屬不動產估價師應具備第 8 目所規定之條件。		
1.3.6	<u>(5) 自選定採用之時起，應就投資用不動產逐筆委託外部聯合估價師事務所進行評價、應於資產負債表日檢討評估公允價值之有效性，洽估價師檢視原估價報告，以決定是否重新出具估價報告，以及應至少每半年取具估價師出具之估價報告。</u>	(8) 保險業應建立不動產估價之作業流程並納入內部控制制度，包括應有委外聯合估價師事務所及估價人員之專業資格與條件、取得及分析資訊、評估價值、外部估價報告之適法性檢核及相關文件之保存。外部估價報告之檢核文件應列示所依據資訊及結論之理由，由權責主管簽章，其檢核內容至少應包括勘估標的之基本資料、估價基準日、標的物區域內不動產交易之比較實例、估價之假設及限制條件、估價方法、估價執行流程、估價結論是否允當及估價報告日等報告內容是否完備、估值計算是否錯		
	<u>(6) 單筆評估金額達十億元以上者，應由二家以上之聯合估價師事務所進行估價。</u>			

項目編號	查核事項		法令規章	說明
	修正後	修正前		
1.3.7	(7) <u>投資性不動產於取得後之首次委外鑑價報告不得由原取得不動產之不動產估價師及聯合估價師事務所辦理鑑價。</u>	誤。檢核文件應保存五年。	本會104.1.23金管保財字第10402501001號令	
1.3.8	(8) <u>不動產估價師及聯合估價師事務所每三年應更換一次，更換前後不得為同一估價師及聯合估價師事務所，且於更換後一年內不得再委任更換前之估價師及聯合估價師事務所。</u>	(9)會計師逐筆應複核保險業委任之聯合估價師事務所出具之估價報告，以確認獨立不動產估價師報告所採用方法及計算之合理性。 (10)保險業應依下列規範提列特別盈餘公積限制盈餘分配：		
1.3.9	(9) <u>委外之聯合估價師事務所及其所屬不動產估價師應具備第9目所規定之條件。</u>	①應就後續衡量採用公允價值模式之所有未實現利益淨額提列特別盈餘公積限制盈餘分配，嗣後因處分相關資產時，其各該投資性不動產因「後續衡量首次採用公允價值模式所生之影響淨額」所提列之特別盈餘公積，應由簽證精算人員依國際財務報導準則公報第四號「保險合約」第二階段內容發布之評價標準或原則評估準備金適足並報經本會核准後，始得依處分比例予以迴轉分配。		
1.3.10	(10) <u>不動產估價師應出具聲明書，內容至少應包括與要求估價之保險業並無實質上直接或間接利害關係，以及未遵循相關法令規範或未善盡專業應有之注意致應負之法律責任等。</u>	②保險業應於股東會上報告可分配盈餘之調整情形及所提列之特別盈餘公積數額，俾股東知悉影響情形。		
1.3.11	(11) <u>保險業應建立不動產估價之作業流程並納入內部控制制度，包括應有委外聯合估價師事務所及估價人員之專業資格與條件、取得及分析資訊、評估價值、外部估價報告之適法性檢核及相關文件之保存。外部估價報告之檢核文件應列示所依據資</u>			

項目編號	查核事項		法令規章	說明
	修正後	修正前		
1.3.12	訊及結論之理由，由權責主管簽章，其檢核內容至少應包括勘估標的之基本資料、估價基準日、標的物區域內不動產交易之比較實例、估價之假設及限制條件、估價方法、估價執行流程、估價結論是否允當及估價報告日等報告內容是否完備、估值計算是否錯誤，並應就其是否有鑑價假設條件或參考數值引用不當或錯誤等情事及對估價結果有重大影響之估價參數之合理性及正確性進行檢核。檢核文件應保存五年。 (12)會計師逐筆應複核保險業委任之聯合估價師事務所出具之估價報告，以確認獨立不動產估價師報告所採用方法及計算之合理性。			
1.3.13	(13)保險業有無依本會 109.5.11 金管保財字第 10904917647 號令提列特別盈餘公積限制盈餘分配： ① 應分別就投資性不動產「後續衡量首次採用公允價值模式之稅後影響淨額」及「後續各期公允價值變動之累積增值利益稅後淨額」提列特別盈餘公積，不得辦理盈餘分配。		本會 109.5.11 金管保財字第 10904917647 號令	

項目編號	查核事項		法令規章	說明
	修正後	修正前		
	② <u>依前款所提列之特別盈餘公積，僅得做為後續補足有效契約依國際財務報導準則公報第十七號「保險合約」、壽險業有效保險契約負債公允價值評估及其他本會指定評估方式等規定補足保險合約負債。</u> ③ <u>嗣後處分該投資性不動產者，如有依前款規定，以第一款提列之特別盈餘公積補足保險合約負債者，得經本會核准後，就原提列之特別盈餘公積之比例予以迴轉，人身保險業迴轉後，擬辦理盈餘分配者，仍應依本會一百零二年二月八日金管保財字第一〇二〇二五〇一九九二號函有關規定辦理。</u>			

二、保險業務之查核(共 5 項)

項目編號	查核事項		法令規章	說明
	修正後	修正前		
1.2	2. 招攬業務或徵員，有無以不實之文宣、廣告、以不同保險公司之契約內容做不當比較，或以不當管道或方式辦理人員招聘之情	2. 招攬業務或徵員，有無以不實之文宣、廣告、以不同保險公司之契約內容做不當比較，或以不當管道或方式辦理人員招	1.保險業招攬及核保理賠辦法第 6 條 2.保險業務員管理規則第 16 條 3.保險業招攬廣告自律規範第	修訂查核事項。

項目編號	查核事項		法令規章	說明
	修正後	修正前		
	事?內容是否經總公司或外商在台分公司核可?是否依規定揭露必要資訊? <u>是否有勸誘客戶解除或終止契約,或以貸款、保單借款繳交保險費之情事?</u>	聘之情事?內容是否經總公司或外商在台分公司核可?是否依規定揭露必要資訊?	4、4-2、5 條 4.財政部 85.9.18 台財保字第 852369361 號函 5.本會保險局 107.3.23 保局(壽)字第 10602110120 號函 6.本會保險局 107.3.23 保局(壽)字第 10704124102 號函	
1.26	26.是否有配合車商保代通路要求,強迫、引誘或限制要保人或被保險人締約或轉保之自由,且提供車商保代額外報酬或其他利益? <u>民眾透過車商保代業務員投保汽車保險,於首年投保或變更投保之保險公司時,是否填寫汽車保險調查表,並併同要保書留存建檔?</u>	26.是否有配合車商保代通路要求,強迫、引誘或限制要保人或被保險人締約或轉保之自由,且提供車商保代額外報酬或其他利益?	本會 108.2.22 保局(產)字第 10804520930 號函 本會 109.5.19 金管保綜字第 1090491857 號函	修訂查核事項及法令規章。
1.31	31.與異業合作推廣附屬性保險商品業務,是否依「保險業保險代理人保險經紀人與異業合作推廣附屬性保險商品業務應注意事項」規定辦理	31.與異業合作推廣附屬性保險商品業務,是否依「保險業保險代理人保險經紀人與異業合作推廣附屬性保險商品業務應注意事項」規定辦理	本會 108 年 7 月 31 日金管保產字第 10804943351 號令 「保險業保險代理人保險經紀人與異業合作推廣附屬性保險商品業務應注意事項」	
6.21	21.專業再保險業務分入及定價 (1) <u>辦理分入再保險業務時,是否</u>		本會 109.4.16 金管保財字第 10904138172 號函	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>依相關法令規定，於再保險契約訂定前進行符合顯著風險移轉與否之判斷或簡易測試？</u> (2) <u>於分入再保險業務定價時，是否綜合評估項目再保險型態、再保險架構、承保範圍、風險性質、損失經驗、再保險條件及再保險費率(若適用)等，以決定參與成分。？」</u>			
9	<u>保全作業之查核：</u> <u>經營傷害及健康保險業務，有無訂定相關保全控制作業處理程序？對要保人申請終止保險契約之保件，有無訂定相關電訪控制作業處理程序？終止保險契約申請書內容是否依公會所訂範本辦理？</u>		<u>本會 109.3.4 金管保壽字第 10904903341 號令及 10904903344 號函</u> <u>本會 109.6.8 金管保壽字第 1090492041 號函</u>	新增查核事項及法令規章。

三、資金運用項目之查核（共 1 項）

項目編號	查核事項		法令規章	說明
	修正後	修正前		

項目編號	查核事項		法令規章	說明
	修正後	修正前		
12.9	9.制訂風險胃納及各主要風險限額應依下列規定辦理： (1)是否依公司之風險特性與風險胃納，訂定各主要風險限額？	9.制訂風險胃納及各主要風險限額應依下列規定辦理： (1)是否依公司之風險特性與風險胃納，訂定各主要風險限額？	金融監督管理委員會 102.3.5 金管保財字第 10202502111 號函 本會 107.10.31 金管保財字 第 10704503781 號令	修訂法令規章。

四、內部管理之查核（共 6 項）

項目編號	查核事項		法令規章	說明
	修正後	修正前		
1.1.1	(1)董（理）事會成員之資格及人數、開會頻率及出席人數是否符合規定？董事會召集之通知，除緊急情事之召集外，是否於七日前通知各董事及監察人？委託出席是否出具委託書及授權表決事項？董事會之決議，除公司法另有規定外，是否過半數董事之出席，出席董事過半數之同意行之？	(1)董（理）事會成員之資格及人數、開會頻率及出席人數是否符合規定？董事會召集之通知，除緊急情事之召集外，是否於七日前通知各董事及監察人？委託出席是否出具委託書及授權表決事項？董事會之決議，除公司法另有規定外，是否過半數董事之出席，出席董事過半數之同意行之？	1.公司法第 192、195、204、205、206、208 條 2.保險業負責人應具備資格條件準則第 3 條、 <u>第 8 條、第 11 條</u>	修訂法令規章。
1.1.10	(10)對於負責人兼職(任)及分層負責之管理機制，是否依本會 107 年 10 月 30 日金管保壽字第 10704546070 號函及 109 年 3 月 20 日金管保壽字第 10904906651 號	(10)對於負責人兼職及分層負責之管理機制，是否依本會 107 年 10 月 30 日金管保壽字第 10704546070 號函，落實保險業負責人兼任非保險相關事業職務之管理（如：有無	1.保險業負責人應具備資格條件準則第 3 條第 2 項 1.保險業負責人應具備資格條件準則 4、5 條 2.本會 107 年 10 月 30 日金	修訂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		
	令，落實保險業負責人兼職(任)之管理規範？定期對負責人兼任職務之績效予以考核？考核結果作為繼續兼任及酌減兼任任務之參考？	建立負責人兼職行為之內部管理機制？董(理)事長、總經理或與其職責相當之人是否符合不得擔任非保險相關事業之董(理)事長、總經理或與其職責相當之人之規定？已兼任者是否依規定出具承諾及符合內部規範？）？	管保壽字第 10704546070 號函 3.本會 109 年 3 月 20 日金管保壽字第 10904906651 號令	
1.1.12	(12)董（監）事(含自然人及法人)，本人或其關係人是否同時擔任其他金融機構之董（監）事？如有是否符合規定？	(12)保險業之董（理）事長、總經理或與其職責相當之人是否未擔任非保險相關事業之董（理）事長、總經理或職責相當之人？但擔任財團法人或非營利之社團法人職務者，不在此限。	保險業負責人應具備資格條件準則第 6 條	修訂查核事項及法令規章。
1.2 1.2.1 1.2.2 1.2.3	2.監察人(監事)之成員、職權與功能 (1)監察人(監事)成員之資格及人數應符合規定。 (2)監察人(監事)職權應充分發揮。 (3)監察人(監事)之配偶、二親等以內之血親或一親等姻親，無擔任同一保險業之董（理）事、經理人情事。	2.監察人(監事)之成員、職權與功能 (1)監察人(監事)成員之資格及人數應符合規定。 (2)監察人(監事)職權應充分發揮。 (3)監察人(監事)之配偶、二親等以內之血親或一親等姻親，無擔任同一保險業之董（理）事、經理人情事。	1.公司法第 216 條至 222 條 2.保險業負責人應具備資格條件準則第 3、9、11 條	修訂法令規章。
1.4.10	(10)保險業之獨立董事不得於同一公	(10)保險業之獨立董事不得於同一公	1.保險業公司治理實務守	修訂法令規章。

項目編號	查核事項		法令規章	說明
	修正後	修正前		
	司連任逾三屆。	司連任逾三屆。	則第 25 條 2.本會 108.4.25 金管保產字第 10804122010 號函 3. 保險局 109.01.03 保局(壽)字第 1080439818 號函	
4.1.2 4.1.2.1 4.1.2.2 4.1.2.3	(2)總稽核之資格與職務 ①總稽核之資格應符合「保險業負責人應具備資格條件準則」規定。 ②總稽核之職位應相當於副總經理。 ③總稽核不得兼任與稽核工作相互衝突或牽制之職務。	(2)總稽核之資格與職務 ①總稽核之資格應符合「保險業負責人應具備資格條件準則」規定。 ②總稽核之職位應相當於副總經理。 ③總稽核不得兼任與稽核工作相互衝突或牽制之職務。	1.保險業內部控制及稽核制度實施辦法第 11 條第 2、3、4 項 2.保險業負責人應具備資格條件準則第 8 條	修訂法令規章。

五、資訊作業之查核（共 22 項）

項目編號	查核事項		法令規章	說明
	修正後	修正前		
2.6.4	4.行動投保業務系統維護與管理	4.行動投保業務系統維護與管理	保險業經營行動投保業務自律規範 保險業經營行動服務自律規範	修訂法令規章。
2.6.4.1	(1)辦理行動投保業務，是否制訂內部控制作業處理程序，至少包括作業	(1)辦理行動投保業務，是否制訂內部控制作業處理程序，至少包括作	保險業經營行動投保業務自律規範第 5 條	修訂法令規章。

項目編號	查核事項		法令規章	說明
	修正後	修正前		
	流程、行政控管機制、系統控管機制等內容，以供作業遵循？	業流程、行政控管機制、系統控管機制等內容，以供作業遵循？	保險業經營行動服務自律規範第5條	
2.6.4.2	(2)是否限制業務員僅得使用公司配給之帳號及密碼，始得登入行動裝置之作業系統？登入後是否於行動裝置上，完成客戶要保相關資料之輸入？是否由客戶確認輸入內容後，於行動裝置上親自簽名？ <u>客戶申請變更行動電話號碼時，是否以電訪、簡訊或其他方式確認號碼正確性？</u>	(2)是否限制業務員僅得使用公司配給之帳號及密碼，始得登入行動裝置之作業系統？登入後是否於行動裝置上，完成客戶要保相關資料之輸入？是否由客戶確認輸入內容後，於行動裝置上親自簽名？	保險業經營行動投保業務自律規範第6條 保險業經營行動服務自律規範第6條	修訂查核事項及法令規章。
2.6.4.3	(3)辦理行動投保業務，是否建立資訊安全控管機制？	(3)辦理行動投保業務，是否建立資訊安全控管機制？	保險業經營行動投保業務自律規範第8條 保險業經營行動服務自律規範第9條	修訂法令規章。
2.6.4.3.1	A.是否依「保險業經營行動服務自律規範」之各項規定，建立妥適之安控措施，至少包括行動裝置作業系統登入身分認證機制、對輸入之要保資料傳輸及儲存安全維護措施、業務員遺失行動裝置之通報以及接獲通報後之處理程序等？	A.是否依「保險業經營行動投保業務自律規範」之各項規定，建立妥適之安控措施，至少包括行動裝置作業系統登入身分認證機制、對輸入之要保資料傳輸及儲存安全維護措施、業務員遺失行動裝置之通報以及接獲通報後之處理程序等？		修訂法令規章。

項目編號	查核事項		法令規章	說明
	修正後	修正前		
1.3.1	1.內部控制三道防線對資訊安全控管之執行情形：	1.內部控制三道防線對資訊安全控管之執行情形：	1.本會保險局 105.11.17 保局(綜)字第 1050087049 號書函	配合自律規範修訂，修正引用之參考規範及新增項目編號。
<u>1.3.1.1</u>	(1)對於保險業辦理資訊安全防護自律規範及保險業辦理電腦系統資訊安全評估作業原則，是否已納入內部控制、內部稽核及自行查核之範圍？	(1)對於產險業辦理資訊安全防護自律規範及產險業辦理電腦系統資訊安全評估作業原則，是否已納入內部控制、內部稽核及自行查核之範圍？	2. 保業 保險業辦理資訊安全防護自律規範	
<u>1.3.1.2</u>	(2)是否於 106 年底完成個人資訊管理制度(PIMS)之驗證、且於 107 年底完成資訊安全管理制度(ISMS)驗證？	(2)是否於 106 年底完成個人資訊管理制度(PIMS)之驗證、且於 107 年底完成資訊安全管理制度(ISMS)驗證？	3.本會保險局 106.3.1 保局(綜)字第 10602560070 號函	
<u>1.3.1.3</u>	(3)是否每年於董事會報告資安整體執行情形(如落實資安防護作業，提升人員資安防護意識及資安專業職能)？	(3)是否每年於董事會報告資安整體執行情形(如落實資安防護作業，提升人員資安防護意識及資安專業職能)？		
1.3.2	2.資訊安全專責單位及主管之設置及相關運作情形：	2.資訊安全專責單位及主管之設置及相關運作情形：	保險業內部控制及稽核制度實施辦法第 6-1 條	新增項目編號。
<u>1.3.2.1</u>	(1)資訊安全專責單位及主管是否未兼辦資訊或其他與職務有利益衝突之業務?(保險合作社另有規定者依其規定)	(1)資訊安全專責單位及主管是否未兼辦資訊或其他與職務有利益衝突之業務?(保險合作社另有規定者依其規定)		
<u>1.3.2.2</u>	(2)保險業達一定規模者，其資訊安全專責單位是否具職權行使獨立性?其專責單位主管是否指派協	(2)保險業達一定規模者，其資訊安全專責單位是否具職權行使獨立性?其專責單位主管是否指派協		

項目編號	查核事項		法令規章	說明
	修正後	修正前		
1.3.2.3	理級以上或職責相當之人擔任？ (3)是否由資訊安全專責單位主管與董(理)事長、總經理、總稽核聯名出具前一年度資訊安全整體執行情形聲明書，並於會計年度終了後3個月內提報董(理)事會？	理級以上或職責相當之人擔任？ (3)是否由資訊安全專責單位主管與董(理)事長、總經理、總稽核聯名出具前一年度資訊安全整體執行情形聲明書，並於會計年度終了後3個月內提報董(理)事會？		
1.3.2.4	(4)資訊安全專責單位人員，每年是否至少接受15小時以上資訊安全相關訓練？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，每年是否至少接受3小時以上教育訓練？	(4)資訊安全專責單位人員，每年是否至少接受15小時以上資訊安全相關訓練？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，每年是否至少接受3小時以上教育訓練？		
2.2.3	3.有關網路系統對使用者之建置管理是否嚴謹？使用者密碼設定之相關限制是否適當？如：	3.有關網路系統對使用者之建置管理是否嚴謹？使用者密碼設定之相關限制是否適當？如：	1.保險業辦理資訊安全防護自律規範 2.保險業網路投保註冊會員密碼之設計安全作業準則	配合自律規範修訂，增修引用之參考規範及查核事項。
2.2.3.1	(1)靜態密碼	(1)是否規定需設定為文數字之密碼？		
2.2.3.1.1	A.是否規定需設定為英數字之密碼？	(2)是否規定密碼最少字數？		
2.2.3.1.2	B.是否規定密碼最少字數？	(3)是否設定密碼之有效期限？		
2.2.3.1.3	C.是否設定密碼之有效期限？	(4)密碼是否以亂碼方式儲存？		
2.2.3.1.4	D.密碼是否以亂碼方式儲存？	(5)是否設定密碼輸入錯誤失敗次數之控制？		
2.2.3.1.5	E.是否設定密碼輸入錯誤失敗次數			

項目編號	查核事項		法令規章	說明
	修正後	修正前		
2.2.3.1.6	數之控制？ F.是否強迫第一次登錄時須變更密碼？	(6)是否強迫第一次登錄時須變更密碼？		
2.2.3.1.7	G.系統是否控制不得使用前幾次用過的密碼？	(7)系統是否控制不得使用前幾次用過的密碼？		
2.2.3.2	(2)一次性密碼(OTP)			
2.2.3.2.1	A.是否規定密碼最少字數？			
2.2.3.2.2	B.是否設定密碼輸入錯誤失敗次數之控制？			
2.2.3.2.3	C.是否設定每次密碼有效性時效，若超過需重新申請發給新密碼？			
2.6.1.6	(6)是否定期辦理電子郵件社交工程演練？是否對員工加強資通安全教育訓練？ <u>是否持續參考F-ISAC所發布之資安威脅情資及防護建議，並宣導防範社交工程手法？</u>	(6)是否定期辦理電子郵件社交工程演練？是否對員工加強資通安全教育訓練？	本會保險局 109.5.4 保局（綜）字第 10904917361 號函	配合函令修正查核事項。
2.6.3	3.對透過網際網路之交易，是否依相關之安控標準適時更新所使用之安全及憑證技術，以提升交易安全等級？	3.對透過網際網路之交易，是否依相關之安控標準適時更新所使用之安全及憑證技術，以提升交易安全等級？	3. 財產保險業辦理電腦系統 資訊安全評估作業原則	配合自律規範修訂，修正引用之參考規範。
2.6.4	(刪除)	4.辦理網路投保業務，網路投保註冊會員密碼之安全設計，是否符合「財產保險業網路投保註冊會員密碼之設計安全作業準則」之密碼安全強度規	1.財產保險業辦理資訊安全防護自律規範第9條 2.財產保險業網路投保註冊會員密碼之設計安全	本項刪除，將內容納入項次 2.2.3

項目編號	查核事項		法令規章	說明
	修正後	修正前		
		則？	作業準則	
2.6.5	5.運用新興科技(包含雲端服務、社群媒體、生物特徵資料及自攜裝置等)	5.使用行動裝置(含 BYOD)、社群媒體或雲端服務(含私有雲)等新興科技之安全控管機制	財產保險業辦理資訊安全防護自律規範	配合自律規範修訂，修正引用之參考規範及查核事項。
2.6.5.1	(1) 雲端服務安全控管	(3) 使用雲端服務(含私有雲)之安全防護措施	財產保險業辦理資訊安全防護自律規範第 7 條	配合自律規範修訂，增修引用之參考規範及查核事項，並調整項目編號。
2.6.5.1.1	A.是否制定雲端服務管理政策，並定期檢視？	A. 是否制定使用雲端服務之相關規範，至少包括雲端服務安全管理、雲端服務提供者遴選機制、雲端服務持續營運管理等，並定期檢視？	<u>保險業運用新興科技作業原則</u>	
2.6.5.1.2	B.導入 IaaS 或 PaaS 雲端服務模式前，是否評估下列事項：	B.導入前有無評估資訊安全、災害應變、資料存取控制等風險控管措施，是否符合資訊安全相關自律規範之要求？		
2.6.5.1.2.1	a.雲端服務業者之合格條件、服務水準、復原時間、備援機制、供應鏈關係、權責歸屬及資訊安全防护等項目。	C.是否建置妥適之資料存取管控機制(包含使用者帳號權限管理、身分驗證機制等)？		
2.6.5.1.2.2	b.雲端服務業者所提供之平台、協定、介面、檔案格式等，以確保互通性與可移植性。	D.是否建置客戶資料或敏感資料傳輸或儲存之安全控管措施(如資料加密等)？		
2.6.5.1.2.3	c.雲端服務業者所建置安全控管措施(如防火牆區隔)之妥適性，以確保其提供之資源與其他承租人所使用之資源各自獨立。			
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？			

項目編號	查核事項		法令規章	說明
	修正後	修正前		
2.6.5.1.4	D.是否監控並建立資通安全事件通報程序?			
2.6.5.1.5	E.是否於服務合約終止或轉移時，將使用之作業系統映像檔、儲存空間、快取空間、備份媒體、客戶資料或敏感資料等全數刪除或銷毀，並留存刪除或銷毀之紀錄，以供事後確認?			
2.6.5.2	(2)社群媒體控管程序	(2) 使用社群媒體之安全防護措施	財產保險業辦理資訊安全防護自律規範第6條	配合自律規範修訂，增修引用之參考規範及查核事項文字。
2.6.5.2.1	A.是否制定社群媒體管理政策，並定期檢視?	A.是否制定社群媒體管理與監督相關規範，並定期檢視?	保險業運用新興科技作業原則	
2.6.5.2.2	B.有無制定社群媒體使用守則(包含可接受使用之社群媒體、功能等)?是否制定公司發言規範，明定發言角色與權責?	B.有無制定社群媒體使用守則(包含可接受使用之社群媒體、功能等)?是否制定公司發言規範，明定發言角色與權責?		
2.6.5.2.3	C.是否建立內容過濾與監視機制?	C.是否建立內容過濾與監視機制?		
2.6.5.2.4	D.是否制定申訴處理機制?	D.是否制定申訴處理機制?		
2.6.5.3	(3)自攜裝置安全控管	(1) 對員工使用行動裝置(含 BYOD)之安全防護措施	財產保險業辦理資訊安全防護自律規範第5條	配合自律規範修訂，增修引用之參考規範及查核事項文字。
2.6.5.3.1	A.是否制定自攜裝置管理政策，並定期檢視?	A. 是否制定行動裝置(含 BYOD)管理及使用行動裝置之安全控管等相關規範，並定期檢視?	保險業運用新興科技作業原則	
2.6.5.3.2	B.是否建置使用者身分與裝置識別之機制(如帳號密碼識別、裝置識別碼)?	B.是否建置使用者身分與裝置識別之機制(如帳號密碼識別、裝置識		
2.6.5.3.3	C.使用人員與裝置是否列冊管理，			

項目編號	查核事項		法令規章	說明
	修正後	修正前		
2.6.5.3.4	且至少每年審閱一次？採取之資安管控措施，是否包括制定自攜裝置連網環境標準？如未符合標準(如作業系統疑似遭破解或提權、未安裝病毒防護、重大漏洞未修復)，是否限制其連網功能？ D.對資料存取權限控管及資料保護措施(如資料加密或遮罩)是否妥適？	別碼)？ C.對行動裝置(含 BYOD)採取之資安管控措施，是否取得持有者同意，並列冊管理使用人員與裝置，且至少每年審閱一次？ D.員工透過行動裝置(含 BYOD)提供保險服務，對資料存取權限控管及資料保護措施(如資料加密或遮罩)是否妥適？		
2.6.5.4	(4) <u>生物特徵資料安全控管</u>		<u>保險業運用新興科技作業原則</u>	配合自律規範修訂，新增引用之參考規範及查核事項。
2.6.5.4.1	<u>A.運用客戶生物識別資料(如聲紋、指紋等)，是否建立內部作業及資料保存之控管程序？</u>			
2.6.5.4.2	<u>B.取得及利用客戶生物特徵資料前，是否先取得客戶同意並留存客戶同意之紀錄？</u>			
2.6.5.4.3	<u>C.是否針對生物識別機制，建立其錯誤接受率及錯誤拒絕率之標準，並每年定期檢視？</u>			
2.6.5.4.4	<u>D.生物特徵資料儲存於會員公司內部系統時，是否去識別化、進行加密儲存、分別儲存於不同之儲存媒體(如資料庫)？儲存於會員公司提供之終端設備時，是否儲存</u>			

項目編號	查核事項		法令規章	說明
	修正後	修正前		
2.6.5.4.5	於符合 FIPS 140-2 Level 3 標準含以上之設備？			
2.6.5.4.6	E. 對生物特徵資料於傳輸過程中之相關控管措施，是否確認符合「保險業經營電子商務自律規範」及「保險業網路投保註冊會員密碼之設計安全作業準則」之規定？ F. 是否於首次使用生物辨識技術或技術有重大變更時(如輔助資料、技術提供商)，經資訊部門檢視該技術足以有效識別客戶身分？			
2.6.6	6. 是否依所訂評估計畫辦理整體電腦系統(含自建與委外維運)資訊安全評估作業，並提交電腦系統資訊安全評估報告？缺失改善事項是否送稽核單位追蹤覆查？報告及相關文件是否至少保存 5 年？	6. 是否依所訂評估計畫辦理整體電腦系統(含自建與委外維運)資訊安全評估作業，並提交電腦系統資訊安全評估報告？缺失改善事項是否送稽核單位追蹤覆查？報告及相關文件是否至少保存 5 年？	1. 財產保險業辦理資訊安全防護自律規範第 8 條 2. 保險業辦理電腦系統資訊安全評估作業原則	配合自律規範修訂，修正引用之規範。
2.6.7	7. 對交付給客戶之應用程式，有無辦理下列檢測： (1) 提供 http, https, FTP 者應進行弱點掃描。 (2) 程式原始碼掃描或滲透測試。 (3) 敏感性資料保護檢測(如記憶		保險業電腦系統資訊安全評估作業原則	配合自律規範修訂，新增引用之參考規範及查核事項。

項目編號	查核事項		法令規章	說明
	修正後	修正前		
	體、儲存媒體)。 (4)金鑰保護檢測。			
2.6.8	8.對行動應用程式是否建立資訊安全控管機制？是否符合公會所訂「保險業提供行動應用程式(APP)作業原則」之各項技術要求？	7.對行動應用程式 APP(含提供給消費者或員工使用者)是否建立資訊安全控管機制？是否符合「產險業提供行動裝置應用程式作業原則」之各項技術要求？	1. 財產保險業辦理資訊安全防護自律規範第9條 2. 保險業提供行動裝置應用程式作業(APP)原則	配合自律規範修訂，修正引用之參考規範及查核事項。
2.6.8.1	(1)是否依行動應用程式之重要性，定期委由專業機構完成資安檢測？專業機構是否參考經濟部工業局「行動應用 APP 基本資安檢測基準」及 OWASP 公布之 Mobile Top 10 項目辦理並通過檢測？			
2.6.8.2	(2)是否辦理程式碼掃碼或黑箱測試，並修正中/高風險漏洞？			
2.6.8.3	(3)是否就專業機構檢測報告建立檢核機制？檢核項目是否有缺漏、是否與佐證資料不符？檢核結果是否與說明矛盾？			
2.6.8.4	(4)是否建立行動應用程式上架前之資安檢測程序？			
2.6.8.5	(5)與行動裝置有關之安全設計，如設備指定、生物辨識、敏感資料保護等，是否評估其有效性？			
2.6.9	9.是否建立物聯網設備管理清冊？物		保險業辦理資訊安全防護	配合自律規範修訂，新

項目編號	查核事項		法令規章	說明
	修正後	修正前		
	<u>聯網設備相關安全控管是否符合公會訂定之「保險業使用物聯網設備作業準則」？</u>		<u>自律規範</u>	增引用之參考規範及查核事項。
2.6.10	10.於非公司職場實施異地辦公或遠端工作時，是否評估相關作業風險，以強化遠端作業之安全？		保險業辦理資訊安全防護自律規範	配合自律規範修訂，新增引用之參考規範及查核事項。
2.6.10.1	(1)是否針對營運環境調整、資料傳輸及加密機制、機敏資料防護、稽核軌跡留存、異常行為監控及對外遠端存取設備進行評估及強化？系統及設備如有重大漏洞是否立即處理及因應，降低業務運作風險，確保整體保險系統穩定及安全？			
2.6.10.2	(2)針對使用之視訊會議系統、VPN及VDI等設備，是否訂定相關使用規範並落實各項安全管控作業？			
3.3.3	(刪除)	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17-1條	配合自律規範修訂，刪除並將查核事項移至2.6.5.1.3

六、其他事項之查核（共 1 項）

項目編號	查核事項		法令規章	說明
	修正後	修正前		
8	(八)保險業營運持續管理或緊急應變相關措施 是否依據「保險業營運持續管理或緊急應變相關因應措施」落實執行營運持續管理、訂定營運持續性策略，及因應重大風險或緊急應變之措施？		109.6.22 金 管 保 壽 字 第 1090417831 號函	新增查核事項及法令規章。