

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		
1.1.3	(3)資訊公開之查核	(3)資訊公開之查核	1.保險業公司治理實務守則	配合 108 年度檢查重點 增列相關法令規章
1.1.3.1	①是否於每會計年度終了後三個月內，將經會計師查核簽證、董事會通過及監察人承認之年度財務報告公告並彙送主管機關申報？	①是否於每會計年度終了後三個月內，將經會計師查核簽證、董事會通過及監察人承認之年度財務報告公告並彙送主管機關申報？	2.保險業財務報告編制準則	
			3.人身保險業辦理資訊公開管理辦法	
			4.專業再保險業財務業務管理辦法	
1.1.3.2	②是否於網站建置公司財務業務相關資訊並即時更新異動資料？	②是否於網站建置公司財務業務相關資訊並即時更新異動資料？	5.本會 106.2.24 金管保財字第 10602501060 號函	
1.1.3.3	③外國專業再保險業是否依規定登載財務業務相關資訊於臺灣分公司網站或以書面備置於臺灣分公司營業處所？	③外國專業再保險業是否依規定登載財務業務相關資訊於臺灣分公司網站或以書面備置於臺灣分公司營業處所？	6.公開發行公司年報應行記載事項準則	
1.1.3.4	④財務資料是否以簽證會計師出具查核簽證或核閱財務報	④財務資料是否以簽證會計師出具查核簽證或核閱財務報		

項目編號	查核事項		法令規章	說明
	修正後	修正前		
1.1.3.5	告內容為準？ ⑤是否依財務報告編製準則揭露應附註揭露事項？是否於年度財務報告其他揭露事項中揭露勞工檢查結果違反勞動基準法事項？	告內容為準？ ⑤是否依財務報告編製準則揭露應附註揭露事項？是否於年度財務報告其他揭露事項中揭露勞工檢查結果違反勞動基準法事項？		
<u>1.1.3.6</u>	<u>⑥年報之記載事項是否確實依「公開發行公司年報應行記載事項準則」相關規定辦理？</u>			

二、保險業務之查核（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		
8 8.1	<u>(八)對保經代業務往來管理之查核</u> <u>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？</u>		108 年度檢查重點	配合 108 年度檢查重點增列查核事項

三、資金運用之查核(共 17 項)

項目編號	查核事項		法令規章	說明
	修正後	修正前		
3.3-1	<u>(5)保險業是否依保險法第一百四十六條之一第三項第五款規定，未參加股東自行召集具董事、監察人選舉議案之股東臨時會行為？</u>		本會 107.11.12 金管保財字第 10704504271 號解釋令	增列法令規章及查核事項

項目編號	查核事項		法令規章	說明
	修正後	修正前		
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:	1.保險業投資未上市未上櫃及私募有價證券管理辦法第4條 2.公開發行公司取得或處分資產處理準則	配合 108 年度檢查重點增列查核事項及法令規章
3.10 3.10.1 3.10.2	10.保險業是否依規於國內股權投資作業相關處理程序內,訂定從事股權投資相關人員之利益衝突防範機制? (1)保險業是否要求國內股權商品投資相關人員(指「保險業資產管理自律規範」(下稱本自律規範)第7條之1第2項所列兩類人員)應盡忠實誠信原則,除法令或本自律規範另有規定外,不得有本自律規範第7條之1第1項各款之行為? (2)保險業是否要求國內股權商品投資相關人員於買賣其知悉交易相關內容之國內股權商品(除本自律規範第7條之1第3項但	10.保險業是否依規於國內股權投資作業相關處理程序內,訂定從事股權投資相關人員之利益衝突防範機制?	1.本會 105.3.31 金管保財字第 10502501691 號令 2.保險業資產管理自律規範第6條、第7條之1	增列查核事項

項目編號	查核事項		法令規章	說明
	修正後	修正前		
3.10.3	<u>書所列原因取得及取得後賣出國內股權商品以外者)前應取得其所屬保險業之核准?</u> (3)<u>保險業是否要求國內股權商品投資相關人員至少每月依本自律規範附件範本格式向各屬保險業申報其本人、配偶、未成年子女及被本人利用名義交易者之國內股權商品交易情形?</u>			
3.10.4	(4)<u>保險業是否要求國內股權商品投資相關人員交付本人、配偶及未成年子女之同意書授權公司或本人親自向台灣證券交易所股份有限公司、財團法人中華民國證券櫃檯買賣中心及台灣集中保管結算所查詢上述買賣國內股權商品之情形，以辦理本自律規範第7條之1第4項交易查核機制。</u>			
3.10.5	(5)<u>若因情形特殊，致有無法取得相關當事人從事國內股權商品交</u>			

項目編號	查核事項		法令規章	說明
	修正後	修正前		
3.10.6	<u>易情形(本自律規範第 7 條之 1 條第 4 項)或同意書(本自律規範第 7 條之 1 第 5 項)者，保險業是否研擬內部控制因應措施，其內容包括相關人員應提供之證明文件及定期稽核機制，並確實控管？</u> <u>(6)保險業是否訂定國內股權商品投資相關人員從事國內股權商品交易應受禁止之情形、申報及違規處理方式，並檢核是否有利益衝突之情事，且內部稽核單位是否至少每年查核相關人員遵循情形及揭露於內部稽核報告？</u>			
3.11	11.保險業是否依規訂定國內及國外有價證券投資作業(含私募有價證券)相關處理程序(投資前及投資後管理機制:包括投資政策與程序之建立、投資後之檢討機制、前台、中台及後台作業權責之控管、投資人員利益衝突防範機制之妥適	11.保險業是否依規訂定國內及國外有價證券投資作業相關處理程序，並落實執行？	1.本會 105.3.31 金管保財字第 10502501691 號令 2.保險業資產管理自律規範第 6 條、<u>第 7 條</u>及第 16 條之 1 3.<u>保險業投資未上市未上櫃</u>	1.增列查核事項及法令規章。 2.配合法規異動及參酌 108 年度新增檢查重點一(七) 增修文字。

項目編號	查核事項		法令規章	說明
	修正後	修正前		
6.5.7.3	<u>之三以上同意之決議後為之？</u> ③對於被投資對象經營，是否有保險法第 146-1 條第 3 項及第 4 項之情事？			
6.13	13.保險業辦理經外國中央政府所設立信用保證機構保證之放款業務，以擔任聯合貸款案之參加行為限： (1)保險業是否評估該信用保證機構財務狀況足以償付所擔保之債務，並應訂定對其風險承擔之限額，以落實風險控管？ (2)併入「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」第七條第一項第一款規定計算，且對於同一放款對象之放款及投資總額，合計是否未超過該保險業資金百分之五？		本會 107.12.07 金管保財字第 10704505101 號解釋令	增列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>(3)是否具備本會 107.12.07 金管保財字第 10704505101 號令第四點第 1 目至第 7 目所列文件供主管機關事後查核？</u>			
7.3	3.保險業資金購買國外有價證券種類是否以下列為限： (1)外國中央政府發行之公債、國庫券及該政府所屬機構發行之債券。 (2)外國地方政府發行或保證之債券及該政府所屬機構發行或保證之債券。 (3)外國銀行發行或保證之金融債	3.保險業資金購買國外有價證券種類是否以下列為限： (1)外國中央政府發行之公債、國庫券。 (2)外國地方政府發行或保證之債券。 (3)外國銀行發行或保證之金融債券、可轉讓定期存單、浮動利率中期債券。	1. 保險業辦理國外投資管理辦法第 5 條 2. 本會 107.8.22 金管保財字第 10704145310 號函	增列文字及調整項次

項目編號	查核事項		法令規章	說明
	修正後	修正前		
	券、可轉讓定期存單、浮動利率中期債券。 (4)外國銀行在臺分行（含國際金融業務分行）及大陸地區銀行在臺分行發行之外幣可轉讓定期存單。 (5)本國銀行發行以外幣計價之金融債券及外幣可轉讓定期存單。 (6)本國企業發行以外幣計價之公司債。 (7)以外幣計價之商業本票。 (8)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。 (9)國外表彰基金之有價證券。 (10)資產證券化商品。 (11)國際性組織所發行之債券。 (12)國內證券市場上市或上櫃買賣之外幣計價股權或債權憑	(4)外國銀行在臺分行（含國際金融業務分行）及大陸地區銀行在臺分行發行之外幣可轉讓定期存單。 (5)本國銀行發行以外幣計價之金融債券及外幣可轉讓定期存單。 (6)本國企業發行以外幣計價之公司債。 (7)以外幣計價之商業本票。 (8)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。 (9)國外表彰基金之有價證券。 (10)資產證券化商品。 (11)國外政府機構發行之債券。 (12)國際性組織所發行之債券。 (13)國內證券市場上市或上櫃買賣之外幣計價股權或債權憑		

項目編號	查核事項		法令規章	說明
	修正後	修正前		
	證。 (13)其他經主管機關核准之有價證券。	證。 (14)其他經主管機關核准之有價證券。		
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 2 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	調整文字
7.8	8.保險業資金投資於第 5 條第 11 款至第 12 款有價證券，是否符合規定條件、等級及限額？	8.保險業資金投資於第 5 條第 11 款至第 13 款有價證券，是否符合規定條件、等級及限額？	保險業辦理國外投資管理辦法第 10 條	調整文字
7.14	14.險業投資之國外資產得委由保管機構保管或自行保管，其保管機構是否為臺灣集中保管結算所股份有限公司，或最近一年經國內外信用評等機構評定信用評等等級為 A-級或相當等級以上之本國金融機構及外國金融機構在臺分支機構。但報經主管機關核准者，不在此限，並得委由符合下列標準之國外金融機構保管：	14.險業投資之國外資產得委由保管機構保管或自行保管，其保管機構是否為臺灣集中保管結算所股份有限公司，或符合下列標準之金融機構： (4)成立滿三年以上，在我國境內設有分公司或經核准辦理保管業務之子公司。 (5)最近一年經國內外信用評等機構評定信用評等等級為 A- 級	保險業辦理國外投資管理辦法第 16 條	增列及調整文字

項目編號	查核事項		法令規章	說明
	修正後	修正前		
	(1)成立滿三年以上，在我國境內設有分公司或經核准辦理保管業務之子公司。 (2)最近一年經國內外信用評等機構評定信用評等等級為 A- 級或相當等級以上。 (3)<u>最近一年資產或淨值排名居全世界前五百名以內之銀行或所保管之資產達五千億美元以上之機構。</u> <u>保險業最近一期自有資本與風險資本之比率未達百分之二百者，應將國外資產委由臺灣集中保管結算所股份有限公司或最近一期自有資本與風險性資產之比率符合法定標準之本國金融機構及外國金融機構在臺分支機構保管。</u> 保險業經核定國外投資額度達資金百分之三十五或國外投資金額	或相當等級以上。 (6)最近一年資產或淨值排名居全世界前五百名以內之銀行或所保管之資產達五千億美元以上之機構。但本國機構不在此限。 保險業最近一期自有資本與風險資本之比率未達百分之二百者，應於本辦法修正施行後半年內，將國外資產委由臺灣集中保管結算所股份有限公司或最近一期自有資本與風險性資產之比率符合法定標準之本國金融機構及外國金融機構在臺分支機構保管。但報經主管機關同意者，得延長之。 保險業經核定國外投資額度達資金百分之三十五或國外投資金額達美金十億元以上者，除經由金融機構辦理特定金錢信託投資國外之有價證券及國外表彰基金之有		

項目編號	查核事項		法令規章	說明
	修正後	修正前		
	達美金十億元以上者，除經由金融機構辦理特定金錢信託投資國外之有價證券及國外表彰基金之有價證券外，其國外投資有價證券是否集中由保管機構負責保管，且保管機構不得超過五家？ 保險業委由國外保管機構保管國外資產者，其全權委託之受託機構是否與保管機構分屬不同之金融機構？國外保管契約之簽訂、修正及保管帳戶授權人員之異動，是否經董事會通過？且保險業應確認保管契約須載明下列事項： (1) 主管機關認為必要時，得派員或令保險業委託會計師或其他專業人員查核保險業委由保管機構保管之國外資產，並向主管機關提出報告或表示意見，保險業委任之保管機構對於相	價證券外，其國外投資有價證券是否集中由保管機構負責保管，且保管機構不得超過五家？ 保險業委由國外保管機構保管國外資產者，其全權委託之受託機構是否與保管機構分屬不同之金融機構？國外保管契約之簽訂、修正及保管帳戶授權人員之異動，是否經董事會通過？且保險業應確認保管契約須載明下列事項： (7) 主管機關認為必要時，得派員或令保險業委託會計師或其他專業人員查核保險業委由保管機構保管之國外資產，並向主管機關提出報告或表示意見，保險業委任之保管機構對於相關查核事項不得拒絕。 (8) 保險業國外保管帳戶資產不得以任何形式為他人債務之擔		

項目編號	查核事項		法令規章	說明
	修正後	修正前		
	關查核事項不得拒絕。 (2) 保險業國外保管帳戶資產不得以任何形式為他人債務之擔保。 (3) 未經保險業同意者，不得將保險業國外保管帳戶資產移轉予第三人。 (4) 保管機構應就保險業簽證會計師函證帳戶詢證項目(包括餘額是否相符、是否設定擔保等)逐項確認後，直接函復會計師事務所。 (5) 保管契約應明確訂定合約最終受益人、資產所有權歸屬及主次帳戶之受益人僅限該保險業。 (6) 其他經主管機關指定之事項 本辦法修正施行時，保管機構如未符合第一項<u>規定</u>，保險業是否於修	保。 (9) 未經保險業同意者，不得將保險業國外保管帳戶資產移轉予第三人。 (10) 保管機構應就保險業簽證會計師函證帳戶詢證項目(包括餘額是否相符、是否設定擔保等)逐項確認後，直接函復會計師事務所。 (11) 保管契約應明確訂定合約最終受益人、資產所有權歸屬及主次帳戶之受益人僅限該保險業。 (12) 其他經主管機關指定之事項 本辦法修正施行時，保管機構如未符合第一項第一款或第三款之標準，保險業是否於修正施行後半年內將國外資產移轉至符合第一項標準之機構保管？保管契約如未符合		

項目編號	查核事項		法令規章	說明
	修正後	修正前		
	正施行後 <u>一年內將國外資產移轉至符合第一項本文規定之機構保管或依第一項但書規定報經主管機關核准？</u>	前項規定者，保險業是否於修正施行後一年內進行調整？		
7.15.2.1	① <u>投資私募基金前是否辦理投資評估分析？是否於交易前建立利害關係人檢核機制？是否就風險管理單位意見評估及分析後始辦理交易？是否落實所訂私募基金之風險控管機制？</u>		<u>保險業辦理國外投資自律規範</u>	配合 108 年度檢查重點增列查核事項及法令規章
7.15.2.2	② <u>公開發行公司於辦理私募基金交易前，是否洽請會計師出具交易價格合理性表示意見？</u>		<u>公開發行公司取得或處分資產處理準則</u>	配合 108 年度檢查重點增列查核事項及法令規章
7.23	23. <u>保險業依保險業辦理國外投資管理辦法（下稱本辦法）第 3 條第 1 項第 8 款規定之其他經主管機關核准之資金運用項目，從事本辦法第五條之外國中央政府發行之公債及國庫券之附買回及附賣回交</u>		<u>本會 107.12.24 金管保財字第 10704967151 號令</u>	增列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>易：</u> <u>(1)各該政府所屬國家之主權評等等級，是否經國外信用評等機構評定 BBB+ 級或相當等級以上？</u> <u>(2)交易之約定期間是否未超逾六個月？</u> <u>(3)交易對手是否以本國債券自營商或最近一年長期債務信用評等等級經本辦法第二條第一項第三款所定國外信用評等機構評定為 BBB+ 級或相當等級以上之外國金融機構為限？</u> <u>(4)是否依本辦法第十五條第一項所定國外投資相關交易處理程序增訂辦理附買回及附賣回交易之處</u> <u>理程序？</u>			
8.2	2.保險業投資保險相關事業，是否遵守下列規定：	2.保險業投資保險相關事業，是否遵守下列規定：	保險業申請投資保險相關事業管理辦法第6條	配合修訂法令規章及增列查核事項
8.2.1	(1)保險業與被投資公司之交易應	(1)保險業與被投資公司之交易應	<u>保險業投資保險相關事業管理辦法第4、6、7條</u>	

項目編號	查核事項		法令規章	說明
	修正後	修正前		
8.2.2	符合本法第一百四十六條之三及第一百四十六條之七相關規定。	符合本法第一百四十六條之三及第一百四十六條之七相關規定。		
8.2.3	(2)保險業應確實執行第四條第一項第七款至第九款所列評估機制或內部規範。	(2)保險業應確實執行第四條第一項第七款至第九款所列評估機制或內部規範。		
8.2.4	(3) <u>被投資事業有第七條第一項第三款第一至九目所列情事之一者，是否於事實發生後七日內檢具事由及相關資料報主管機關？</u>			
	(4) <u>是否依財產保險業辦理資訊公開管理辦法第十一條規定，於資訊公開網頁之說明文件其他應記載事項項下公開揭露從事保險相關事業投資之被投資保險相關事業名稱、投資金額及各年度投資損益情形，並每年更新一次？</u>			

項目編號	查核事項		法令規章	說明
	修正後	修正前		
8.2.5	<u>(5)是否依第六條訂定處理程序，並經董(理)事會通過，修正時亦同？</u>			
12.6	6.指定「保險業風險管理實務守則」應執行條文，依保險業內部控制及稽核制度實施辦法第5條第1項第14款規定納入內部控制作業之處理程序。	6.指定「保險業風險管理實務守則」應執行條文，依保險業內部控制及稽核制度實施辦法第5條第10款規定納入內部控制作業之處理程序。	行政院金融監督管理委員會 101.1.5 金管保財字第 10002517821 號函 本會 107.10.31 金管保財字第 10704503781 令	增修法令規章
12.12	<u>12.投資以國外債券或權益證券為成分之新臺幣計價之基金投資(含量身訂作之債券ETF)，是否確實執行投資前分析(包含但不限於匯率風險、信用風險、風險集中等)、投資後管理(包含但不限於國家風險、產業別風險及匯率風險等)以及建立定期追蹤機制(包含但不限於流動性風險)？</u>		1.保險業風險管理實務守則 2.保險業資產管理自律規範	配合 108 年度關注查核項目增列查核事項法令規章

四、內部管理之查核（共 68 項，資訊作業之查核共 47 項，個人資料檔案安全維護之查核共 14 項，其餘共 7 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		
1.1.10	(10) <u>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？）？</u>		1.保險業負責人應具備資格條件準則第 3 條第 2 項 2.本會 107 年 10 月 30 日金管保壽字第 10704546070 號函	參酌本局關注查核項目相關法規增列查核事項
1.1.11	(11) <u>針對董事就本身利害關係人利益相關之案件，是否適當迴避或保持明確分際，及建立有效牽制監督機制？</u>		保險業與利害關係人從事放款以外之其他交易管理辦法	參酌本局關注查核項目訂定

項目編號	查核事項		法令規章	說明
	修正後	修正前		
2.1.1	(1)保險業應分別業務性質及規模，依內部牽制原理訂定各項控制作業之處理程序，且應適時檢討修訂。	(1)保險業應分別業務性質及規模，依內部牽制原理訂定各項控制作業之處理程序，且應適時檢討修訂。	1.保險法第 148-3 條。 2.保險業內部控制及稽核制度實施辦法第 5 條 3.保險局 107.11.21 保局(財)字第 10704964800 號函	增列法令規章
2.13	13.保險業是否建立重大偶發事件之通報機制?是否依規定辦理申報?		保險業通報重大偶發事件之範圍與適用對象	增列查核事項及法令規章
3.1	1.組織與管理	1.資訊單位查核 (1)組織與管理		修正查核項目 3.1.1 調升一階至 3.1
3.1.1	(1)內部組織與職務分工	①內部組織與職務分工		3.1.1.1 調升一階至 3.1.1 修正項目編號
3.1.2	(2)管理辦法及作業規範之訂定	②管理辦法及作業規範之訂定		3.1.1.2 調升一階至 3.1.2 修正項目編號
3.1.3	(3)資訊安全管理			調整架構 增列查核事項子項
3.1.3.1	①內部控制三道防線對資訊安全控管之執行情形： I.對於產險業辦理資訊安全防護	4.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	1. 本會保險局 105.11.17 保局(綜)字第 1050087049 號書函	原 3.4 查核事項調整至 3.1.3 項下 修正項目編號

項目編號	查核事項		法令規章	說明
	修正後	修正前		
	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？ <u>II.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)？</u> <u>III.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)？</u>	部控制、內部稽核及自行查核之範圍？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)？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)？若有辦理網路投保業務，是否參考財產保險業網路投保註冊會員密碼之設計安全作業準則辦理？	2. 財產保險業辦理資訊安全防護自律規範 3. 本會保險局 106.3.1 保局(綜)字第 10602560070 號函	修正查核事項部分文字 末段查核事項內容調整至 3.2.5.1 項下
3.1.3.2	<u>②資訊安全專責單位及主管之設置及相關運作情形：</u> <u>I.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> <u>II.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</u>	5.保險業是否設置資訊安全專責單位及主管?是否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) 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理級以上或職責相當之人擔任?(適用本項規定之保險業，應於符合條	「保險業內部控制及稽核制度實施辦法」第 6-1 條	調整架構 原 3.5 查核事項調整至 3.1.3 項下 修正項目編號 修正查核事項部分文字 考量調整期 6 個月已屆滿，刪除部分查核事項

項目編號	查核事項		法令規章	說明
	修正後	修正前		
	協理級以上或職責相當之人擔任? III.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? IV.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?	件起 6 個月內調整之) 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? 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?		文字
3.1.4	(4)內部稽核辦理情形 ①辦理電子商務業務及行動投保業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	(7)內部稽核辦理情形 內部稽核之範圍是否包括網路系統提供之各項業務、網路系統使用管理、委外作業管理、病毒偵測及預防、及檢核實際運作情形與所訂	1.「保險業辦理電子商務應注意事項」 2.「保險業電子商務參考查核項目」 3.「保險業經營行動投保業	調整架構 原 3.2.7 查核事項調整至 3.1.4 項 修正項目編號 修正查核事項部分文字

項目編號	查核事項		法令規章	說明
	修正後	修正前		
	<u>稽核？</u> 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？ 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？	安控標準是否一致等？	<u>務自律規範」</u>	
3.2	2.網路及系統安全控管查核	2.網路系統安全查核		修正查核項目文字
<u>3.2.5</u>	<u>(5)系統開發及維護管理</u>	(3)系統開發及維護控制		調整架構 原 3.1.3 查核事項調整至 3.2.5 項 修正項目編號 修正查核事項子項文字
<u>3.2.5.1</u>	①系統開發管理 I. 若訂有系統開發、維護規範(standards)，是否包括下列項目，以作為系統開發、維護及文件製作之標準：	①系統開發控制 I. 若訂有系統開發、維護規範(standards)，是否包括下列項目，以作為系統開發、維護及文件製作之標準：	「金融機構資訊系統安全基準」	調整架構 原 3.1.3.1 查核事項調整至 3.2.5.1 項 修正項目編號 修正查核事項文字

項目編號	查核事項		法令規章	說明
	修正後	修正前		
	A.系統開發／設計程序。 B.套裝軟體選擇基準。 C.程式設計標準。 D.程式及系統測試方法及標準。 E.實施（轉換）事宜。 F.系統文件撰寫規格。 G.系統/程式異動管理。 H.系統評估。 II.系統開發是否依可行性研究、系統分析、系統設計、程式撰寫、系統測試及系統轉換之標準開發步驟進行？ III.系統開發階段是否訂有明確的作業進度計畫表，並妥善控制之？ IV.系統開發、設計是否有由業務、稽核、會計、企劃等有關單位參與，以求操作、管理、查核各方面之考慮周全？ V.系統之開發、設計，對於個人資料之蒐集、處理及利用，有無逾越特定目的之範圍或妨害當事人之權	A.系統開發／設計程序。 B.套裝軟體選擇基準。 C.程式設計標準。 D.程式及系統測試方法及標準。 E.實施（轉換）事宜。 F.系統文件撰寫規格。 G.系統/程式異動管理。 H.系統評估。 II.系統開發是否依可行性研究、系統分析、系統設計、程式撰寫、系統測試及系統轉換之標準開發步驟進行？ III.系統開發階段是否訂有明確的作業進度計畫表，並妥善控制之？ IV.系統開發、設計是否有由業務、稽核、會計、企劃等有關單位參與，以求操作、管理、查核各方面之考慮周全？ V.系統之開發、設計，對於個人資料之蒐集、處理及利用，有無逾越特定目的之範圍或妨害當事人之權		

項目編號	查核事項		法令規章	說明
	修正後	修正前		
	益？ VI.若涉及個人資料檔案之應用，其程式之設計及管理有無妥善規劃，以防止資料遭不當使用？ VII.對於各項應用系統之控制設計，是否有徵求稽核人員意見，並於設計中考量？各項控制設計是否周延？ VIII.各項系統實施前是否訂有測試計畫？所有程式、相關子系統及整體系統是否均經完整之測試？其測試結果是否均經相關主管覆核？是否由使用單位作接受性測試？ IX.作業實施前轉換計畫是否完妥並經確實執行？ X.系統正式作業實施前，是否經業務單位參與驗收？對系統及說明文件、作業（操作）手冊、測試紀錄、轉換（實施）計畫之完整性以及是否符合原訂需求（功能）等，皆加	益？ VI.若涉及個人資料檔案之應用，其程式之設計及管理有無妥善規劃，以防止資料遭不當使用？ VII.對於各項應用系統之控制設計，是否有徵求稽核人員意見，並於設計中考量？各項控制設計是否周延？ VIII.各項系統實施前是否訂有測試計畫？所有程式、相關子系統及整體系統是否均經完整之測試？其測試結果是否均經相關主管覆核？是否由使用單位作接受性測試？ IX.作業實施前轉換計畫是否完妥並經確實執行？ X.系統正式作業實施前，是否經業務單位參與驗收？對系統及說明文件、作業（操作）手冊、測試紀錄、轉換（實施）計畫之完整性以及是否符合原訂需求（功能）等，		

項目編號	查核事項		法令規章	說明
	修正後	修正前		
	以確實驗收？ XI.系統實施時，是否訂定妥適的雙軌作業期間及經確認新系統之可靠性後才正式啟用？ XII.已正式實施之系統，是否由有關單位人員對下列事項適時予以檢討、評估，以求改進，並作為開發其他新系統之參考？ A.業務電腦化後，操作、管理與查核上尚待加強、改進者。 B.系統控制功能設計之完整性。 C.程式及檔案資料修正頻率與原因之分析。 D.輸出報表之實用性、完整性。 E.實際開發時間、人力、成本與原計畫之比較分析。	皆加以確實驗收？ XI.系統實施時，是否訂定妥適的雙軌作業期間及經確認新系統之可靠性後才正式啟用？ XII.已正式實施之系統，是否由有關單位人員對下列事項適時予以檢討、評估，以求改進，並作為開發其他新系統之參考？ A.業務電腦化後，操作、管理與查核上尚待加強、改進者。 B.系統控制功能設計之完整性。 C.程式及檔案資料修正頻率與原因之分析。 D.輸出報表之實用性、完整性。 E.實際開發時間、人力、成本與原計畫之比較分析。		
<u>3.2.5.2</u>	②系統維護管理 I.對每一應用系統，是否均派專人負責維護的工作？ II.修正系統時，是否採取足夠的控制，以免修正人員接觸未經許可修	②系統維護控制 I.對每一應用系統，是否均派專人負責維護的工作？ II.修正系統時，是否採取足夠的控制，以免修正人員接觸未經許可修	「金融機構資訊系統安全基準」	調整架構 原 3.1.3.2 查核事項調整至 3.2.5.2 項 修正項目編號 修正查核事項文字

項目編號	查核事項		法令規章	說明
	修正後	修正前		
	正之部份？ III.系統如需重大變更時，是否比照開發新系統之程序，由有關單位參與研討變更內容、範圍，並參與驗收？ IV.已正式實施之作業，其程式變更： A.是否有書面申請，並經相關部門（使用單位、資訊單位）主管核准後方才修正？ B.書面申請是否詳細敘明變更原因及內容？ C.修正後是否加以測試（含第三者），並經主管審核其測試結果？ 對修正前後程式是否由換版人員利用公用程式作比對，並列印差異報表送主管審核？ D.系統說明文件是否配合修正？ E.操作程序上如有變更是否通報有關單位？	正之部份？ III.系統如需重大變更時，是否比照開發新系統之程序，由有關單位參與研討變更內容、範圍，並參與驗收？ IV.已正式實施之作業，其程式變更： A.是否有書面申請，並經相關部門（使用單位、資訊單位）主管核准後方才修正？ B.書面申請是否詳細敘明變更原因及內容？ C.修正後是否加以測試（含第三者），並經主管審核其測試結果？ 對修正前後程式是否由換版人員利用公用程式作比對，並列印差異報表送主管審核？ D.系統說明文件是否配合修正？ E.操作程序上如有變更是否通報有關單位？		

項目編號	查核事項		法令規章	說明
	修正後	修正前		
3.2.5.3	③系統文件編製 I.對已實施之系統是否有下列文件： A.系統需求分析報告。 B.系統設計說明書。 C.程式設計說明書。 D.操作說明（含批次作業及端末使用者操作說明）。 E.測試計畫書（含測試報告及測試記錄）。 F.系統轉換計畫書。 G.系統驗收紀錄。 H.與有關單位研討之會議紀錄。 II.各項系統說明文件或紀錄文件（如軟硬體系統變更申請單等）是否指定專人妥善整理與保管？調閱是否均經登記？ III.前述文件如以電腦媒體形態保存時，對其建檔、變更、調閱，是否被授權人員始得為之，並留存紀錄備查？ IV.系統說明文件之撰寫及程式、檔	③系統文件編製 I.對已實施之系統是否有下列文件： A.系統需求分析報告。 B.系統設計說明書。 C.程式設計說明書。 D.操作說明（含批次作業及端末使用者操作說明）。 E.測試計畫書（含測試報告及測試記錄）。 F.系統轉換計畫書。 G.系統驗收紀錄。 H.與有關單位研討之會議紀錄。 II.各項系統說明文件或紀錄文件（如軟硬體系統變更申請單等）是否指定專人妥善整理與保管？調閱是否均經登記？ III.前述文件如以電腦媒體形態保存時，對其建檔、變更、調閱，是否被授權人員始得為之，並留存紀錄備查？ IV.系統說明文件之撰寫及程式、檔	「金融機構資訊系統安全基準」	調整架構 原 3.1.3.3 查核事項調整至 3.2.5.3 項 修正項目編號

項目編號	查核事項		法令規章	說明
	修正後	修正前		
	案名稱之命名是否標準化？	案名稱之命名是否標準化？		
<u>3.2.6</u>	(6)運作管理	(4)運作管理	「金融機構資訊系統安全基準」	調整架構 原 3.1.4 查核事項調整至 3.2.6 項 修正項目編號
<u>3.2.6.1</u>	①主機操作管理 I.控制台及週邊設備（磁碟機、磁帶機、列表機等）是否僅限輪值操作員操作？ II.是否備有作業手冊供操作員使用？操作員是否依作業說明（作業手冊、工作申請單）執行作業？ III.每班作業是否至少有二名操作員輪值？對正常上班時間以外之留守人員是否注意牽制？ IV.除例行作業外，假日及夜間使用正式電腦作業系統是否先經核准？	①主機操作管理 I.控制台及週邊設備（磁碟機、磁帶機、列表機等）是否僅限輪值操作員操作？ II.是否備有作業手冊供操作員使用？操作員是否依作業說明（作業手冊、工作申請單）執行作業？ III.每班作業是否至少有二名操作員輪值？對正常上班時間以外之留守人員是否注意牽制？ IV.除例行作業外，假日及夜間使用正式電腦作業系統是否先經核准？		調整架構 原 3.1.4.1 查核事項調整至 3.2.6.1 項 修正項目編號

項目編號	查核事項		法令規章	說明
	修正後	修正前		
	V.例行性作業是否按預定的排程來處理？非例行作業是否均經申請核准？ VI.作業排程是否妥當？若非自動排程是否有書面之排程表？對工作執行情形及結果有否留存紀錄？異常情形有否查核追蹤？ VII.執行可直接變更目的程式及資料檔案等之公用程式是否先經核准並留存紀錄？ VIII.機房內是否設置工作日誌，記載電腦開關機紀錄、故障維護情形，及操作人員、時間等，並定期陳報？對異常情況有否查核追蹤？ IX.電腦系統運作紀錄或控制台操作紀錄是否由系統管理人員予以檢核？並保留適當之期間？對異常情形有否追蹤查核？ X.電腦作業是否經常發生重覆處理情形？其原因為何？有否採取適	V.例行性作業是否按預定的排程來處理？非例行作業是否均經申請核准？ VI.作業排程是否妥當？若非自動排程是否有書面之排程表？對工作執行情形及結果有否留存紀錄？異常情形有否查核追蹤？ VII.執行可直接變更目的程式及資料檔案等之公用程式是否先經核准並留存紀錄？ VIII.機房內是否設置工作日誌，記載電腦開關機紀錄、故障維護情形，及操作人員、時間等，並定期陳報？對異常情況有否查核追蹤？ IX.電腦系統運作紀錄或控制台操作紀錄是否由系統管理人員予以檢核？並保留適當之期間？對異常情形有否追蹤查核？ X.電腦作業是否經常發生重覆處理情形？其原因為何？有否採取適		

項目編號	查核事項		法令規章	說明
	修正後	修正前		
	當措施以減少發生？ XI.對於電腦軟硬體系統運作狀況及各項電腦資源之使用情形（如主機及週邊設備、端末機等之使用狀況、每月交易情況、系統反應時間、及軟硬體故障情形），是否定期予以統計分析與檢討改進？	當措施以減少發生？ XI.對於電腦軟硬體系統運作狀況及各項電腦資源之使用情形（如主機及週邊設備、端末機等之使用狀況、每月交易情況、系統反應時間、及軟硬體故障情形），是否定期予以統計分析與檢討改進？		
3.2.6.2	②端末機使用管理 I.端末機使用人員資料（如使用者代號、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？ II.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？ III.系統最高權限使用者密碼，是否分人各持一半並密封妥善保管，如有拆封使用是否確實登記並隨即	②端末機使用管理 I.端末機使用人員資料（如使用者代號、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？ II.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？ III.系統最高權限使用者密碼，是否分人各持一半並密封妥善保管，如有拆封使用是否確實登記並隨即		調整架構 原 3.1.4.2 查核事項調整至 3.2.6.2 項 修正項目編號

項目編號	查核事項		法令規章	說明
	修正後	修正前		
	變更？是否由系統自動留存作業紀錄俾供查核？ IV. 端末機操作人員是否憑被授予之使用者代號操作？有無共用同一使用者代號之情形？ V. 由端末設備存取主機或端末設備系統之正式作業程式、檔案或工作執行指令，是否依使用人員職務工作範圍等予以限制？存取時是否先經核准或授權，並留存紀錄？對違規使用有否查核追究？ VI. 對於調離職人員，是否立即取消其使用者代號、密碼？	變更？是否由系統自動留存作業紀錄俾供查核？ IV. 端末機操作人員是否憑被授予之使用者代號操作？有無共用同一使用者代號之情形？ V. 由端末設備存取主機或端末設備系統之正式作業程式、檔案或工作執行指令，是否依使用人員職務工作範圍等予以限制？存取時是否先經核准或授權，並留存紀錄？對違規使用有否查核追究？ VI. 對於調離職人員，是否立即取消其使用者代號、密碼？		
<u>3.2.6.3</u>	③程式、資料檔案管理 I. 系統程式及應用程式之登錄與維護是否指定專人負責？其登錄與維護是否均經申請、核可及覆核程序，並留存紀錄？ II. 程式之登錄、變更程序是否能控制同一程式在程式館內之原始碼及目的碼為同一版本？	③程式、資料檔案管理 I. 系統程式及應用程式之登錄與維護是否指定專人負責？其登錄與維護是否均經申請、核可及覆核程序，並留存紀錄？ II. 程式之登錄、變更程序是否能控制同一程式在程式館內之原始碼及目的碼為同一版本？		調整架構 原 3.1.4.3 查核事項調整至 3.2.6.3 項 修正項目編號

項目編號	查核事項		法令規章	說明
	修正後	修正前		
	III.在特殊情況下，對正式作業檔案資料之更正是否以書面申請，並經核准？電腦是否留存完整之更正紀錄（內容），可憑以查核所有更正皆經申請、核可程序？ IV.具有修正檔案資料或目的程式功能之公用程式是否嚴密管制其使用？ V.是否使用安全軟體對程式及資料檔案之存取加以控管？若有，評估其存取權限控制是否嚴謹？ VI.對重要或機密性之檔案是否採亂碼化措施加以保護，以防止不法之使用？ VII.對重要檔案之使用（含使用被拒絕）是否有由電腦留存作業紀錄，以供查核？ VIII.正式作業與測試作業之程式、資料、工作控制指令等檔案是否分開存放？ IX.是否禁止主機操作員存取正式作	III.在特殊情況下，對正式作業檔案資料之更正是否以書面申請，並經核准？電腦是否留存完整之更正紀錄（內容），可憑以查核所有更正皆經申請、核可程序？ IV.具有修正檔案資料或目的程式功能之公用程式是否嚴密管制其使用？ V.是否使用安全軟體對程式及資料檔案之存取加以控管？若有，評估其存取權限控制是否嚴謹？ VI.對重要或機密性之檔案是否採亂碼化措施加以保護，以防止不法之使用？ VII.對重要檔案之使用（含使用被拒絕）是否有由電腦留存作業紀錄，以供查核？ VIII.正式作業與測試作業之程式、資料、工作控制指令等檔案是否分開存放？ IX.是否禁止主機操作員存取正式作		

項目編號	查核事項		法令規章	說明
	修正後	修正前		
	業程式、資料檔案及應用系統說明文件（操作手冊除外）？ X.是否有資料庫管理員，負責資料庫使用上的協調和控制事宜？ XI.資料庫管理員是否定期重新評估各作業的資料庫結構，並作成紀錄？ XII.對資料庫管理人員及系統管理人員是否限制其存取及變更資料庫之資料？ XIII.對於資料庫不成功的存取是否有紀錄，並加以查核，以防止弊端？	業程式、資料檔案及應用系統說明文件（操作手冊除外）？ X.是否有資料庫管理員，負責資料庫使用上的協調和控制事宜？ XI.資料庫管理員是否定期重新評估各作業的資料庫結構，並作成紀錄？ XII.對資料庫管理人員及系統管理人員是否限制其存取及變更資料庫之資料？ XIII.對於資料庫不成功的存取是否有紀錄，並加以查核，以防止弊端？		
<u>3.2.6.4</u>	④媒體管理 I.對於儲存資料或程式之媒體是否責成專人負責管理？ II.對於保管中或使用中之媒體是否皆予設簿登記控管，並定期派員盤點？ III.媒體之採購、作廢是否經主管核准並留存申請單或紀錄簿備查？	④媒體管理 I.對於儲存資料或程式之媒體是否責成專人負責管理？ II.對於保管中或使用中之媒體是否皆予設簿登記控管，並定期派員盤點？ III.媒體之採購、作廢是否經主管核准並留存申請單或紀錄簿備查？		調整架構 原 3.1.4.4 查核事項調整至 3.2.6.4 項 修正項目編號

項目編號	查核事項		法令規章	說明
	修正後	修正前		
	IV.媒體廢棄前是否先經銷磁或其他處理，以防媒體資料外洩？ V.正式作業所使用之媒體，是否貼有外標籤（包含媒體編號、檔案名稱、建檔日期、保存期限）？ VI.因作業需要存取媒體是否有經主管核准之申請單或紀錄單備查？	IV.媒體廢棄前是否先經銷磁或其他處理，以防媒體資料外洩？ V.正式作業所使用之媒體，是否貼有外標籤（包含媒體編號、檔案名稱、建檔日期、保存期限）？ VI.因作業需要存取媒體是否有經主管核准之申請單或紀錄單備查？		
3.2.7	(7)電子商務業務系統維護與管理		「保險業辦理電子商務應注意事項」	增列查核事項子項
3.2.7.1	<u>①辦理電子商務業務(包括網路投保業務及網路保險服務)，相關安全控管設計：</u> <u>I.對資訊架構之妥適性是否定期辦理檢視？相關網路安全系統規則設定維護是否建立適當管控程序？</u> <u>II.對網路設備、伺服器之存取及資安設備等網路活動是否建立妥適警示機制？網路活動日誌及進出紀錄是否有完整留存及管控機制？是否定期檢討？</u>		「保險業電子商務參考查核項目」	配合法令規章修正增列查核事項

項目編號	查核事項		法令規章	說明
	修正後	修正前		
	<u>III.對網路設備及伺服器等是否定期辦理滲透測試及弱點掃描作業？</u> <u>後續修補管控機制是否妥適？</u> <u>IV.是否建立作業系統安全參數檢核清單並定期檢視與維護？安全參數設定(如密碼設定原則與帳號鎖定原則等)是否符合資訊安全要求？</u> <u>V.對使用者帳號及系統存取權限(含特權帳號)之管理是否妥適？稽核軌跡是否完整留存並建立覆核機制？</u> <u>VI.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>			
3.2.7.2	<u>②辦理電子商務業務，如有網路技術提昇、重購軟硬體系統，或發生網路入侵等是否評估分析可能發生之風險？是否配合檢討或修正相關控管程序與管理規範？</u>		「保險業電子商務參考查核項目」	配合法令規章修正增列查核事項

項目編號	查核事項		法令規章	說明
	修正後	修正前		
3.2.7.3	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？		1.「保險業經營電子商務自律規範」 2.「保險業辦理電子保單簽發作業自律規範」 3.「產險業辦理電腦系統資訊安全評估作業原則」	配合法令規章修正增列查核事項
3.2.7.4	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」之密碼安全強度規則？	若有辦理網路投保業務，是否參考財產保險業網路投保註冊會員密碼之設計安全作業準則辦理？	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作業準則」	原 3.4 末段之查核事項內容調整至 3.2.7.4 項修正查核事項部分文字
3.2.8	(8)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」	配合新增法令規章增列查核事項子項
3.2.8.1	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？		「保險業經營行動投保業務自律規範」第5條	配合新增法令規章增列查核事項
3.2.8.2	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		「保險業經營行動投保業務自律規範」第6條	配合新增法令規章增列查核事項

項目編號	查核事項		法令規章	說明
	修正後	修正前		
	<u>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>			
3.2.8.3	<u>③辦理行動投保業務，是否建立資訊安全控管機制？</u> <u>I.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？</u> <u>II.是否定期檢視行動投保業務相關資訊系統之安全性及資訊安全控管制度之有效性等？</u> <u>III.是否依內部控制三道防線機制，對行動投保業務加強辦理自行查核及內部稽核？</u>		<u>「保險業經營行動投保業務自律規範」第8條</u>	配合新增法令規章增列查核事項
3.2.9	<u>(9)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</u>		<u>「財產保險業辦理資訊安全防護自律規範」</u>	配合新增法令規章增列查核事項子項

項目編號	查核事項		法令規章	說明
	修正後	修正前		
3.2.9.1	①對員工使用行動裝置(含 BYOD)之安全防護措施： I.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？ II.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)？ III.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？ IV.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？		「財產保險業辦理資訊安全防護自律規範」第 5 條	配合新增法令規章增列查核事項
3.2.9.2	②使用社群媒體之安全防護措施： I.是否制定社群媒體管理與監督相關規範，並定期檢視？ II.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		「財產保險業辦理資訊安全防護自律規範」第 6 條	配合新增法令規章增列查核事項

項目編號	查核事項		法令規章	說明
	修正後	修正前		
	<u>等)?是否制定公司發言規範,明 定發言角色與權責?</u> <u>III.是否建立內容過濾與監視機制?</u> <u>IV.是否制定申訴處理機制?</u>			
3.2.9.3	<u>③使用雲端服務(含私有雲)之安全防 護措施:</u> <u>I.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> <u>II.導入前有无評估資訊安全、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?</u> <u>III.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)?</u> <u>IV.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)?</u>		<u>「財產保險業辦理資訊安 全防護自律規範」第7條</u>	配合新增法令規章 增列查核事項

項目編號	查核事項		法令規章	說明
	修正後	修正前		
3.2.10	(10)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10條 2.「產險業辦理電腦系統資訊安全評估作業原則」	配合新增法令規章增列查核事項
3.2.11	(11)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「財產保險業行動應用程式(App)資訊安全作業準則」之各項技術要求？ ①辦理行動應用程式 APP 之發布、更新、安全性問題回報及上架資安檢測與評估等，是否建立妥適控管程序？ ②對行動應用程式 APP 之存取權限，是否建立審核作業機制並留存書面紀錄及佐證資料？是否於上架前洽會相關部門，以評估其存取權限之適法性及安全性？ ③辦理行動應用程式 APP 程式變更		1.「財產保險業辦理資訊安全防護自律規範」第9條 2.「財產保險業行動應用程式(App)資訊安全作業準則」	配合新增法令規章增列查核事項

項目編號	查核事項		法令規章	說明
	修正後	修正前		
	<u>作業，是否建立妥適之控管程序？</u> <u>(包含版本控管、原始碼檢測及引用第三方函式庫(API)等)</u> ④行動應用程式 APP 委外開發時， <u>是否自廠商處取得程式原始碼？</u> <u>如未取得原始碼，是否評估可能面臨風險及未來對業務之影響，預先擬定因應措施？</u>			
3.2.12	(12) <u>對金融資安資訊分享與分析中心(F-ISAC)資安情資之接收與處理，是否建立妥善管理機制？</u> ① <u>是否依金融資安資訊分享與分析中心(F-ISAC)所訂「情資分享管理辦法」，建立資安情資內部作業處理流程與規範，並妥善處置所接收之資安情資？</u> ② <u>對所訂資安情資處理流程之相關控制措施，是否建立定期檢視機制，以確認其有效性？</u> ③ <u>是否依內部控制三道防線機制，對資安警訊處理機制加強辦理自行</u>			配合金融業建置資訊分享與聯合防禦機制 增列查核事項

項目編號	查核事項		法令規章	說明
	修正後	修正前		
	<u>查核及內部稽核？</u>			
<u>3.3</u>	<u>3.災害應變</u>			調整架構 增列查核項目
<u>3.3.1</u>	(1)安全控制	(2)安全控制		調整架構 原 3.1.2 查核事項調整至 3.3 項下 修正項目編號
<u>3.3.1.1</u>	①環境安全防護 I.電腦設備及相關設施之安全防護是否完善？ A.是否有完善的防火、防水、防震、防犯（如機房自動門禁控制系統）及不斷電設備等安全防護措施？ B.除不斷電設備外有無裝置自動發電機，以供長時間停電使用？ C.有無裝置火災自動警報系統及自動滅火設備？	①環境安全防護 I.電腦設備及相關設施之安全防護是否完善？ A.是否有完善的防火、防水、防震、防犯（如機房自動門禁控制系統）及不斷電設備等安全防護措施？ B.除不斷電設備外有無裝置自動發電機，以供長時間停電使用？ C.有無裝置火災自動警報系統及自動滅火設備？		調整架構 原 3.1.2.1 查核事項調整至 3.3.1 項下 修正項目編號

項目編號	查核事項		法令規章	說明
	修正後	修正前		
	D.對電腦及相關設備是否訂有維護契約，定期或不定期實施維護，並留存紀錄備查？ E.保險及維護契約涵蓋範圍是否完全？並在有效期間內？ II.機房是否放置非工作需要或危險物品？ III.電腦媒體存放場所是否有防火、防水、防塵等安全防護措施？是否注意溫、濕度？ IV.系統說明文件存放場所是否有防火、防水等安全防護措施？	D.對電腦及相關設備是否訂有維護契約，定期或不定期實施維護，並留存紀錄備查？ E.保險及維護契約涵蓋範圍是否完全？並在有效期間內？ II.機房是否放置非工作需要或危險物品？ III.電腦媒體存放場所是否有防火、防水、防塵等安全防護措施？是否注意溫、濕度？ IV.系統說明文件存放場所是否有防火、防水等安全防護措施？		
<u>3.3.1.2</u>	②人員進出管理 對進出資訊單位、辦公場所、機房、媒體室及文件保管室之人員是否加以嚴格管制？	②人員進出管理 對進出資訊單位、辦公場所、機房、媒體室及文件保管室之人員是否加以嚴格管制？	「金融機構資訊系統安全基準」	調整架構 原 3.1.2.2 查核事項調整至 3.3.1 項下 修正項目編號
<u>3.3.1.3</u>	③備援措施 I.電腦設備及相關設施是否有備援主機、週邊設備、網路傳輸設備、端末設備等及相關設施（如空調、電力、不斷電設備等）？或其他因	③備援措施 I.電腦設備及相關設施是否有備援主機、週邊設備、網路傳輸設備、端末設備等及相關設施（如空調、電力、不斷電設備等）？或其他因	「金融機構資訊系統安全基準」	調整架構 原 3.1.2.3 查核事項調整至 3.3.1 項下 修正項目編號

項目編號	查核事項		法令規章	說明
	修正後	修正前		
	應措施，如：與廠商簽訂備用契約或與同類機器使用者互相締結支援契約？ II.程式及資料檔案 A.對重要或需要長期保留檔案（含應用、系統程式及資料檔等）是否有備份？備份媒體是否使用具有防火、防濕、防磁等之設備異地存放？安全措施是否嚴密？有無隨時更新？ B.各種重要程式及資料檔案是否有損毀時之重建程序？ III.人員 各項重要工作是否均有備援人員？ IV.系統說明文件 各項系統開發、設計或作業處理程序之說明文件，如以媒體型態儲存，是否備份異地妥為存放？	應措施，如：與廠商簽訂備用契約或與同類機器使用者互相締結支援契約？ II.程式及資料檔案 A.對重要或需要長期保留檔案（含應用、系統程式及資料檔等）是否有備份？備份媒體是否使用具有防火、防濕、防磁等之設備異地存放？安全措施是否嚴密？有無隨時更新？ B.各種重要程式及資料檔案是否有損毀時之重建程序？ III.人員 各項重要工作是否均有備援人員？ IV.系統說明文件 各項系統開發、設計或作業處理程序之說明文件，如以媒體型態儲存，是否備份異地妥為存放？		
3.3.1.4	④故障及災害因應對策 I.是否分別或綜合訂定電腦軟硬體	④故障及災害因應對策 I.是否分別或綜合訂定電腦軟硬體	「金融機構資訊系統安全基準」	調整架構 原 3.1.2.4 查核事項調整

項目編號	查核事項		法令規章	說明
	修正後	修正前		
	系統故障時之復原程序、使用備援系統之轉換程序或故障期間之權宜應變作業方式？ II.前述故障復原程序，使用備援系統之轉換程序，或權宜應變之作業方式，是否定期或不定期辦理測試、演練？ III.是否訂有災害應變計畫以處理各種可能之意外（狀況），俾能在最短時間內及最低成本下，恢復電腦作業功能？ IV.應變計畫是否經最高主管批准？有無每年定期演練？有關人員是否確知在災害中應扮演之角色及責任？	系統故障時之復原程序、使用備援系統之轉換程序或故障期間之權宜應變作業方式？ II.前述故障復原程序，使用備援系統之轉換程序，或權宜應變之作業方式，是否定期或不定期辦理測試、演練？ III.是否訂有災害應變計畫以處理各種可能之意外（狀況），俾能在最短時間內及最低成本下，恢復電腦作業功能？ IV.應變計畫是否經最高主管批准？有無每年定期演練？有關人員是否確知在災害中應扮演之角色及責任？		至 3.3.1 項下 修正項目編號
<u>3.3.2</u>	(2)緊急應變計畫及災害復原程序	(6)緊急應變計畫及災害復原程序		調整架構 原 3.2.6 查核事項調整至 3.3.2 項下 修正項目編號
<u>3.3.2.1</u>	①是否適當評估網路系統無法運作時對該單位業務之影響？並已訂	①是否適當評估網路系統無法運作時對該單位業務之影響？並已訂	「保險業電子商務參考查核項目」	調整架構 修正項目編號

項目編號	查核事項		法令規章	說明
	修正後	修正前		
	定緊急應變計畫及災害復原程序，其內容是否適當？ <u>所訂災變應變計畫書，是否已針對電子商務業務無法運作時，對營運之衝擊影響進行評估並研擬因應措施？對系統故障或災害引起電子商務業務無法運作，所引發之法律責任，是否列為因應措施之一環？</u>	定緊急應變計畫及災害復原程序，其內容是否適當？		修正查核事項部分文字
<u>3.3.2.2</u>	②緊急應變程序能否有效掌控未經授權之侵入？該程序對遠端存取之控制是否符合安全管理政策？是否嚴格監控其存取情形？對遠端存取是否留有稽核軌跡？	②緊急應變程序能否有效掌控未經授權之侵入？該程序對遠端存取之控制是否符合安全管理政策？是否嚴格監控其存取情形？對遠端存取是否留有稽核軌跡？		調整架構 修正項目編號
<u>3.3.2.3</u>	③對緊急應變計畫及災害復原程序是否加以演練並留存紀錄？	③對緊急應變計畫及災害復原程序是否加以演練並留存紀錄？		調整架構 修正項目編號
<u>3.4</u>	<u>4.資訊作業委外管理</u>			調整架構 增列查核項目
<u>3.4.1</u>	(1)資訊軟硬體採購及資訊系統委外開發或維護合約之管理 <u>①法規規定之應記載事項是否均已</u>	(5)協力廠商管理 ①軟硬體買賣合約或委外維護合約內容是否包括作業安全、委託內	「金融機構資訊系統安全基準」	調整架構 原 3.2.5 查核事項調整至 3.4 項下

項目編號	查核事項		法令規章	說明
	修正後	修正前		
	<u>納入合約載明？</u> ②<u>其他重要應注意事項，如：作業安全、委託內容、機密維護、損害賠償等雙方權責之劃分、委外服務品質保證、終止委託之通知時程及配合移轉程序等事項，是否明訂，相關條款是否妥適明確？</u>	容、機密維護、損害賠償等雙方權責之劃分？ ④系統委外開發作業管理 II.上述業務之委外作業，其開發、維護之預定進度及作業安全、委託內容、機密維護、損害賠償等雙方權責之劃分，是否明訂於委外作業契約內？		修正項目編號 修正查核事項部分文字
3.4.2	<u>(2)對協力廠商之監督管理</u> ①是否建立適當控管程序以確保委外維護程式係屬適當？並指定專人負責監控廠商維護活動及服務？ ②若廠商可遠端連線至受檢單位電腦診斷及維護系統，受檢單位是否建立適當程序以控制廠商存取範圍？ ③系統委外開發作業管理 I.系統之開發或維護委外作業時，對軟體開發或維護規範之訂定，軟體設計或修正之督導、核定及驗收等	(5)協力廠商管理 ②是否建立適當控管程序以確保委外維護程式係屬適當？並指定專人負責監控廠商維護活動及服務？ ③若廠商可遠端連線至受檢單位電腦診斷及維護系統，受檢單位是否建立適當程序以控制廠商存取範圍？ ④系統委外開發作業管理 I.系統之開發或維護委外作業時，對軟體開發或維護規範之訂定，軟體設計或修正之督導、核定及驗收等	「金融機構資訊系統安全基準」	調整架構 原 3.2.5 查核事項調整至 3.4 項下 修正項目編號。 修正查核事項部分文字 原 3.1.3.4 查核事項調整至 3.4 項下 修正項目編號 修正查核事項部分文字

項目編號	查核事項		法令規章	說明
	修正後	修正前		
	是否比照自行開發設計準則及控管程序辦理？ II.委外作業業務是否有專人管理，並控制進度？ III.是否嚴禁委外作業廠商進入正式作業環境存取程式或資料？ IV.是否建立適當程序以檢核委外作業廠商修正程式內容係屬適當？並指定專人負責監控廠商維護活動？ V.若廠商可透過網路遠端連線至受檢單位電腦診斷及維護系統，受檢單位是否建立適當程序以控制廠商存取範圍，並由電腦自動留存作業紀錄以供查核？	是否比照自行開發設計準則及控管程序辦理？ III.委外作業業務是否有專人管理，並控制進度？ IV.是否嚴禁委外作業廠商進入正式作業環境存取程式或資料？ V.是否建立適當程序以檢核委外作業廠商修正程式內容係屬適當？並指定專人負責監控廠商維護活動？ VI.若廠商可透過網路遠端連線至受檢單位電腦診斷及維護系統，受檢單位是否建立適當程序以控制廠商存取範圍，並由電腦自動留存作業紀錄以供查核？		
3.5	5.使用單位查核	3.使用單位查核		配合架構調整 原 3.3 查核項目修正項目編號為 3.5 此查核項目之查核子項配合依序修正項目編號

項目編號	查核事項		法令規章	說明
	修正後	修正前		
4.4.1.1	①保險業之總機構是否依其規模、業務性質及組織特性，指定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，並置法令遵循主管一人，其職位是否相當於副總經理？法令遵循單位及總機構法令遵循主管是否符合兼任(辦)業務之規定？	①保險業之總機構是否依其規模、業務性質及組織特性，指定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，並置法令遵循主管一人，其職位是否相當於副總經理？法令遵循單位及總機構法令遵循主管是否符合兼任(辦)業務之規定？	1.保險業內部控制及稽核制度實施辦法第 30 條第 1、2、3 及 4 項 2.本會 107.11.13 金管保財字第 10701939680 號函	增列法令規章
4.4.4	(4)是否依規定建立檢舉制度，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？對檢舉人之保護是否符合規定？受理及調查過程，有利益衝突之人是否迴避？被檢舉人為一定層級以上者，調查報告是否陳報至監察人(監事、監事會)或審計委員會複審？調查後發現重大偶發或違法案件，是否主動向機關通報或告發？	(4)是否依規定建立檢舉制度，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？對檢舉人之保護是否符合規定？受理及調查過程，有利益衝突之人是否迴避？被檢舉人為一定層級以上者，調查報告是否陳報至監察人(監事、監事會)或審計委員會複審？調查後發現重大偶發或違法案件，是否主動向機關通報或告發？	1.保險業內部控制及稽核制度實施辦法第 32-2 條 2.保險業公司治理實務守則第 28-1 條	配合 108 年度關注查核項目增列法令規章
4.6.4	(4)是否依保險業稽核工作考核要點所列內部稽核組織與制度、內部稽核查核工作、稽核管理、其他事		保險業稽核工作考核要點	配合 108 年度關注查核項目增列法令規章及查核事項

項目編號	查核事項		法令規章	說明
	修正後	修正前		
	<u>項、重大及期後事項等各項考核項目強化內部稽核效能？</u>			
5.2	2. <u>對涉及個資之應用系統功能、報表文件或電子檔之管理及資安教育宣導等辦理情形</u>		1.「 <u>個人資料保護法</u> 」 2.「 <u>金融監督管理委員會指定非公務機關個人資料檔案安全維護辦法</u> 」	增列查核事項子項
5.2.1	(1) <u>對涉及個資之系統功能、報表、文件或電子檔，是否建立個資檔案清冊，並定期執行清查及留存相關作業紀錄？有無依個人資料保護相關法令，定期查核確認個人資料檔案維護管理機制之妥適性？並列入內部控制及內部稽核項目？</u>	2.有無依個人資料保護相關法令，定期查核確認所保有之個人資料現況、評估可產生之風險、訂定適當之管理機制及列入內部控制及稽核項目。		原 5.2 查核事項調整至 5.2.1 項 修正項目編號 修正查核事項部分文字
5.2.2	(2) <u>是否定期對個資檔案安全防護，實施資料安全防護教育訓練及相關宣導措施？</u>			增列查核事項
5.2.3	(3) <u>是否訂定個人資料安全事故應變、通報及預防機制，定期辦理演練並留存紀錄？</u>			增列查核事項

項目編號	查核事項		法令規章	說明
	修正後	修正前		
5.3	3.對個資之儲存、傳遞及使用之控管機制		1.「個人資料保護法」 2.「金融監督管理委員會指定非公務機關個人資料檔案安全維護辦法」	增列查核事項子項
5.3.1	(1)存放於資料庫、檔案內之個資，是否建立妥適之去識別化或加密處理機制，相關存取是否建立控管機制，並留存完整稽核軌跡？(如：將正式營運資料複製到測試環境且未去識別化時，是否訂定控管機制？)			增列查核事項
5.3.2	(2)儲存客戶資料之重要資料庫主機是否置於內部網路，是否經由防火牆適當設定這些資料庫主機與對外主機之連線？			增列查核事項
5.3.3	(3)對傳遞個資，是否建立妥適之加密及監控機制，並留存完整稽核軌跡？			增列查核事項
5.3.4	(4)對 FTP、檔案分享(如網路芳鄰、SAMBA)、檔案下載、電子郵件等傳檔功能之應用程式，是否訂定控			增列查核事項

項目編號	查核事項		法令規章	說明
	修正後	修正前		
	<u>管機制、留存完整稽核軌跡，並落實執行？對不同網區間之檔案傳輸系統，是否訂有管控機制，以避免不當夾帶或外洩個資檔？</u>			
5.3.5	<u>(5)對行動碟、光碟、磁帶等移動式儲存媒體及筆記型電腦、平板電腦等可攜式設備，是否建立使用管理機制、留存完整稽核軌跡，並落實執行？</u>			增列查核事項
5.3.6	<u>(6)提供電子商務服務系統，是否採取下列資訊安全措施？</u> <u>①使用者身分確認及保護機制。</u> <u>②個人資料顯示之隱碼機制。</u> <u>③網際網路傳輸之安全加密機制。</u> <u>④應用系統於開發、上線、維護等各階段軟體驗證與確認程序。</u> <u>⑤個人資料檔案及資料庫之存取控制與保護監控措施。</u> <u>⑥防止外部網路入侵對策。</u> <u>⑦非法或異常使用行為之監控與因應機制。</u>		<u>「金融監督管理委員會指定非公務機關個人資料檔案安全維護辦法」第 10 條</u>	增列查核事項

項目編號	查核事項		法令規章	說明
	修正後	修正前		
5.3.7	(7) <u>執行個人資料保護機制、程序及措施，是否記錄其個人資料使用、刪除、停止處理或利用等情況，並留存軌跡資料或相關證據至少五年？</u>			增列查核事項
5.4	4. <u>是否妥適設定及控管相關人員(含協力廠商人員)對個人資料檔案之存取權限，並與所屬人員(含協力廠商人員)簽定保密義務？</u>	3.是否設定相關人員接觸個人資料之權限及控管其接觸情形，並與所屬人員設定保密義務。		修正項目編號 修正查核事項部分文字
5.5	5. <u>對於保戶個人資料於合作推廣或共同行銷傳遞之安全維護措施是否妥適，如：控管資料檔案傳遞過程之安全存取設定，且資料檔案經加密保護之隱密處理？</u>	4.對於保戶個人資料於合作推廣或共同行銷傳遞之安全維護措施是否妥適？		修正項目編號 修正查核事項部分文字

五、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		
4.5.6	(6)投資取得、處分利害關係人發行之共同信託基金受益證券、證券投資	(6)投資取得、處分利害關係人發行之共同信託基金受益證券、證券投資	1.本會 106.7.17 金管證發字第 1060023551 號函	增列法令規章

項目編號	查核事項		法令規章	說明
	修正後	修正前		
	信託基金受益憑證或期貨信託基金受益憑證（包括指數股票型基金及指數股票型期貨信託基金，但不包括封閉式基金）；且經理部門應逐筆彙整成交記錄及其損益情形，按季提報董事會備查。但其他法規另有規定者，依其規定。	信託基金受益憑證或期貨信託基金受益憑證（包括指數股票型基金及指數股票型期貨信託基金，但不包括封閉式基金）；且經理部門應逐筆彙整成交記錄及其損益情形，按季提報董事會備查。但其他法規另有規定者，依其規定。	2.本會 107.11.23 金管保財字第 10704212880 號函	