財產保險公司檢查手冊(異動版)

一、財務狀況之查核(共 2 項)

項目編號	查核事項		法令規章	說明
	修正後	修正前		
1.1.2.2	②公司各項會計政策及作業程序之重大變更是否經董事會或高階經理階層之核准？於會計年度開始日後始自願變動會計政策者，若追溯適用新會計政策對當年度各季財務報告之影響數已達重編財務報告標準者，應重編相關期間財務報告並洽請簽證會計師重行查核或核閱後重新公告申報。	②公司各項會計政策及作業程序之重大變更是否經董事會或高階經理階層之核准？	保險業財務報告編製準則第 4 條及第 6 條第 1 項第 1 款第 6 目	修正查核事項及新增法令規章
1.2.6 1.2.6.4	(6)金融商品之公允價值衡量、分類及減損之查核 ④有無重分類之情形？是否符合規定？如依 IFRS9，將帳列透過其他綜合損益按公允價值衡量之金融資產重分類為按攤銷後成本衡量之金融資產，是否依規定提列特別盈餘公積，及於年度財務報告附註揭露前述重分類之金融資產公允價值變動數？	(5)金融商品之公允價值衡量、分類及減損之查核 ④有無重分類之情形？是否符合規定？	本會 111.11.4 金管保財字第 11104942741 號令	修正查核事項及新增法令規章

資料基準日：111 年 12 月 31 日

二、保險業務之查核(共 2 項)

項目編號	查核事項		法令規章	說明
	修正後	修正前		
2.15	15.辦理傷害險核保是否確實執行各項財務核保作業(含生存調查、保險通報機制及新契約各項電訪作業)？	15.辦理傷害險核保是否確實執行各項財務核保作業(含生存調查、保險通報機制及新契約各項電訪作業)？	保險業招攬及核保作業控管自律規範第 8、9、10、11、12、14、16 條	修正法令規章
2.17.4	(4)保險業辦理電子商務業務，其業務之交易面及管理面之安全需求及安全設計是否遵守「保險業經營電子商務自律規範」、「保險業辦理電子保單簽發及辦理電子化保險契約條款保單作業自律規範」及與客戶所訂契約應符合「網路保險服務定型化契約範本」之規範？	(4)保險業辦理電子商務業務，其業務之交易面及管理面之安全需求及安全設計是否遵守「保險業經營電子商務自律規範」、「保險業辦理電子保單簽發作業自律規範」及與客戶所訂契約應符合「網路保險服務定型化契約範本」之規範？	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及辦理電子化保險契約條款保單作業自律規範 3.網路保險服務定型化契約範本	修正查核項目及法令規章

三、內部管理之查核（共 4 項）

項目編號	查核事項		法令規章	說明
	修正後	修正前		
1.1.13	(13)保險業有無建立管理階層發展計畫，並由董事會定期評估該計畫之發展與執行，以確保永續經營，並落實董事會永續發展責任?	(13)保險業有無建立管理階層發展計畫，並由董事會定期評估該計畫之發展與執行，以確保永續經營？	保險業公司治理實務守則第 24 條之 1 及第 24 條之 2	修正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		
1.4.4	(4)保險業應建立獨立有效風險管理機制，以評估及監督其風險承擔能力、已承受風險現況、決定風險因應策略及風險管理程序遵循情形。 ①是否訂定適當之風險管理政策與程序，經董事會通過並定期檢討修訂？ ②是否建立適當風險控管機制，並發展適合其組織架構與風險管理系統的 ORSA 作業流程？	(4)保險業應建立獨立有效風險管理機制，以評估及監督其風險承擔能力、已承受風險現況、決定風險因應策略及風險管理程序遵循情形。風險控管機制應包括下列原則：業務規模、產品特質及整體經濟情勢等因素以辨識及評估可承受之風險範圍；應考慮之風險應包括核保風險、評估各項準備金之相關風險、市場風險（包括利率風險）、作業風險及法令風險及其他相關風險；管理階層應依據實際經濟情況，定期審視風險控制機制，並採取適當策略。	保險業內部控制及稽核制度實施辦法第 7 條第 2 項第 5 款及第 ~~8~~34-1、34-2 及 34-3 條	修正查核事項及法令規章
1.7	7.對保險業有控制能力之股東是否遵循「保險業公司治理實務守則」第 19 條之相關規定，且與保險業間之溝通聯繫原則透過該股東所指派當選為保險業董事之代表人為之？		保險業公司治理實務守則第 19 條	新增查核事項及法令規章
4.3.1.2	②除經核准採行風險導向內部稽核制度者外，稽核單位對財務、資產保管、資訊及其他管理單位每年至少應辦理一次一般查核，並依實際	②稽核單位對財務、資產保管、資訊及其他管理單位每年至少應辦理一次一般查核，並依實際需要辦理專案查核。	保險業內部控制及稽核制度實施辦法第 18、18-1 條	修正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		
	需要辦理專案查核。			

四、資訊作業之查核（共 31 項）

項目編號	查核事項		法令規章	說明
	修正後	修正前		
1.1	(一)內部組織與職務分工	(一)內部組織與職務分工	保險業內部控制及稽核制度實施辦法第 6 條~~：「保險業使用電腦化資訊系統處理者，其內部控制制度，資訊部門與使用者部門應明確劃分權責。」~~	修正法令規章
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：	1.保險業內部控制及稽核制度實施辦法第 6~~-1~~條之 1。	修正法令規章
2.1.3	3.是否已依機構規模大小、性質、業務範圍採行能有效維持網路安全之政策（如：系統安全責任之劃分、網路及資料存取控制政策、防火牆政策、網站應用程式防火牆(WAF)防護機制、入侵偵測及防禦機制、加密程序及控制、防毒軟體之使用政策）？前開安全政策是否定期檢討、修訂，	3.是否已依機構規模大小、性質、業務範圍採行能有效維持網路安全之政策（如：系統安全責任之劃分、網路及資料存取控制政策、防火牆政策、加密程序及控制、防毒軟體之使用政策）？前開安全政策是否定期檢討、修訂，以符實際運作之需？	保險業辦理資訊安全防護自律規範第 19 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		
	以符實際運作之需？			
2.2.1	1.是否建置一適當之網路系統安全管制措施、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制措施，以控制網際網路與其內部網路或電腦系統間之活動？	保險業辦理資訊安全防護自律規範第 19 條	修正查核事項及新增法令規章
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~~保險業網路電子商務身分驗證之資訊安全作業準則第 3 條	新增查核事項及修正法令規章
2.2.3.1	(1)靜態密碼	(1)靜態密碼		
2.2.3.1.1	A.是否規定需設定為英數字之密碼？	A.是否規定需設定為英數字之密碼？		
2.2.3.1.2	B.是否規定密碼最少字數？	B.是否規定密碼最少字數？		
2.2.3.1.3	C.是否設定密碼之有效期限？	C.是否設定密碼之有效期限？		
2.2.3.1.4	D.密碼是否以亂碼方式儲存？	D.密碼是否以亂碼方式儲存？		
2.2.3.1.5	E.是否設定密碼輸入錯誤失敗次數之控制？	E.是否設定密碼輸入錯誤失敗次數之控制？		
2.2.3.1.6	F.是否強迫第一次登錄時須變更密碼？	F.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？	G.系統是否控制不得使用前幾次用過的密碼？		
2.2.3.1.8	H.儲存時是否已進行不可逆運算（如雜湊演算法），且雜湊值已進行加密保護或加入不可得知的資			

項目編號	查核事項		法令規章	說明
	修正後	修正前		
	料運算。			
2.2.3.1.9	I.採用加密演算法者，其金鑰是否儲存於軟體式金鑰管理器，並與原資料庫區隔，或搭配經第三方認證（如 FIPS 140-2 Level 3 以上）之硬體安全模組並限制明文匯出功能等？			
2.2.3.2	(2)一次性密碼(OTP)	(2)一次性密碼(OTP)		
2.2.3.2.1	A.是否規定密碼最少字數？	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？	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?	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?		
2.2.3.2.4	D.帳號與密碼是否相同？			
2.2.15	15.使用特權帳號進行伺服器管理作業時，是否經主管審核通過，並透過特權帳號管理（PAM）、跳板機或獨立管制網段等連線至正式伺服主機？是否留存稽核軌跡，以確保連線安全性。		保險業辦理資訊安全防護自律規範第 19 條	新增查核事項及法令規章
2.4.1.5	(5)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	(5)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	個人資料保護法第 5 條~~：「個人資料之蒐集、處理或利用，應尊重當事人之權~~	修正法令規章

資料基準日：111 年 12 月 31 日

項目編號	查核事項		法令規章	說明
	修正後	修正前		
	益？	益？	~~益，依誠實及信用方法為之，不得逾越特定目的之必要範圍，並應與蒐集之目的具有正當合理之關聯。」~~	
2.4.1.8	(刪除)	(8)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？		刪除查核事項及法令規章，並修改查核事項款次
2.4.1.9	(刪除)	(9)作業實施前轉換計畫是否完妥並經確實執行？	~~金融機構資訊系統安全基準~~	
2.4.1.10	(刪除)	(10)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，皆加以確實驗收？		
2.4.1.11	(刪除)	(11)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？		
2.4.1.8 ~~2.4.1.12~~	(8)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？	(12)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？		

項目編號	查核事項		法令規章	說明
	修正後	修正前		
	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.程式及檔案資料修改頻率與原因之分析。 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。	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.程式及檔案資料修改頻率與原因之分析。 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。		
2.4.1.9 ~~2.4.1.13~~ 2.4.1.9.1 2.4.1.9.1.1 2.4.1.9.1.2 2.4.1.9.1.3 2.4.1.9.1.4 2.4.1.9.1.5 2.4.1.9.1.6	(9)對核心資訊系統置換作業： A.系統轉換前之準備工作： a.是否建立架構審查機制。 b.是否評估營運及業務需求所需備載容量，並建置擬真測試環境。 c.是否訂定測試計畫與產出標準，並進行各項測試及整體性演練。 d.進行上線變更審查及風險評估，辨識複雜度及影響範圍，並檢視測試個案及上線復原計畫之完整性，與建立多個檢核點及啟動復原之決策條件。 e.是否預留復原作業及上線驗證時間。 f.是否要求設備提供廠商與委外開	(13)對核心資訊系統之置換，相關系統開發及程式修改之控制作業是否至少包括成本效益分析、風險評估、需求分析、設計規劃、功能測試驗證(含完整性、正確性與穩定性)、轉換決策評估及平行測試等項目？	1.本會 108.11.21 金管保財字第 10804957681 號令 2.保險業辦理資訊安全防護自律規範第 5 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		
	發廠商於上線支援時，能緊急提供備品、問題查找及修改人力。			
2.4.1.9.1.7	g.是否提前公告及進行教育訓練（含異常話術）。			
2.4.1.9.2	B.系統轉換作業：			
2.4.1.9.2.1	a .是否執行系統及資料備份，並驗證各項資料內容之正確性及完整性。			
2.4.1.9.2.2	b.是否驗證各項變更作業，並監控網路及系統，以確保預期結果。			
2.4.1.9.3	C.系統轉換後之事件管理：			
2.4.1.9.3.1	a.是否落實事故應變，並以消費者權益及持續營運優先處理。			
2.4.1.9.3.2	b.是否集中管理問題及追蹤問題原因，並提出短、中、長期改善方案與持續追蹤。			
2.4.4	4.資訊系統作業委外，是否於規劃及遴選階段，將資訊安全相關內容納入評估項目？及是否遵循下列事項？	4.核心資訊系統作業委外，是否於規劃及遴選階段，將資訊安全相關內容納入評估項目？及是否遵循下列事項？	1.保險業辦理資訊安全防護自律規範第 16 條 2.保險業核心資訊系統作業委外資安注意事項	新增查核事項及法令規章
2.4.4.1	(1)服務提供廠商應具備資訊安全相關認證或已有資通安全維護之相關措施。	(1)服務提供廠商應具備資訊安全相關認證或已有資通安全維護之相關措施。		
2.4.4.2	(2)審核作業委外廠商資格	(2)審核作業委外廠商資格		

項目編號	查核事項		法令規章	說明
	修正後	修正前		
2.4.4.2.1	A.各會員公司應制定有關審核廠商資格之內控機制，並就作業委外提供廠商進行評選審查作業。	A.各會員公司應制定有關審核廠商資格之內控機制，並就作業委外提供廠商進行評選審查作業。		
2.4.4.2.2	B.將資訊安全相關認證納入遴選項目，且應訂定內部程序，其至少包含作業委外廠商遴選機制、合約或協議簽訂、作業委外廠商管理要項、產品交付和驗收或維運等項目。	B.將資訊安全相關認證納入遴選項目，且應訂定內部程序，其至少包含作業委外廠商遴選機制、合約或協議簽訂、作業委外廠商管理要項、產品交付和驗收或維運等項目。		
2.4.4.2.3	C.各會員公司應將資訊安全或個人資料隱私管理相關認證納入資訊系統之作業委外廠商評估項目。	C.各會員公司應將資訊安全或個人資料隱私管理相關認證納入核心資訊系統之作業委外廠商評估項目。		
2.4.4.3	(3)作業委外廠商管理要項	(3)作業委外廠商管理要項		
2.4.4.3.1	A.應建立作業委外廠商管理規範，其內容應含作業委外廠商之人員管控，並建立適當檢驗機制，以確保管理機制有效落實。	A.應建立作業委外廠商管理規範，其內容應含作業委外廠商之人員管控，並建立適當檢驗機制，以確保管理機制有效落實。		
2.4.4.3.2	B.作業委外廠商進行軟、硬體維運時，應具備資通安全維護之措施。	B.作業委外廠商進行軟、硬體維運時，應具備資通安全維護之措施。		
2.4.4.3.3	C.若作業委外內容有重大變更	C.若作業委外內容有重大變更		

項目編號	查核事項		法令規章	說明
	修正後	修正前		
	或重大事件時，應審查是否影響相關資訊安全管理制度或依循標準之要求並評估其風險，採取適當控制措施。	或重大事件時，應審查是否影響相關資訊安全管理制度或依循標準之要求並評估其風險，採取適當控制措施。		
2.4.4.3.4	D.各會員公司之資訊系統委外廠商管理時，其管理項目是否納入對委外廠商存取資訊之控管機制、資訊安全管理措施查核機制、發生資安事故時委外廠商通知機制及處理時效要求、與關係終止管理機制等項目？			
2.4.4.3.5	E.作業委外廠商簽訂合約或協議，是否遵循相關安全管理措施，其內容包含：	D.作業委外廠商簽訂合約或協議，是否遵循相關安全管理措施，其內容包含：		
2.4.4.3.5.1	a.服務供應廠商履行合約或協議時所提供軟體（或交付標的物）為交付產品，需具備合法性且不得違反智慧財產權之規定或侵害第三人合法權益。	a.服務供應廠商履行合約或協議時所提供軟體（或交付標的物）為交付產品，需具備合法性且不得違反智慧財產權之規定或侵害第三人合法權益。		
2.4.4.3.5.2	b.作業委外廠商進行資訊系統開發或維運時，若涉及客戶、員工個人資料，需考量	b.作業委外廠商進行核心資訊系統開發或維運時，若涉及客戶、員工個人資料，需考		

項目編號	查核事項		法令規章	說明
	修正後	修正前		
	具個人資料安全防範措施。	量具個人資料安全防範措施。		
	c.應訂定相關資訊安全管理責任。	c.應訂定相關資訊安全管理責任。		
2.4.4.3.5.3				
2.4.4.3.5.4	d.應約定資安檢測與弱點修補之責任與時效要求。			
2.4.4.3.5.5	e.委外廠商交付之系統或程式，應確保無惡意程式及後門程式，或提供相關掃描報告。			
2.4.4.3.5.6	f.資訊系統作業委外終止或結束時，委外廠商應提供移轉服務，將留存資料移回至各會員公司自行處理，並應刪除或銷毀全數資料，且提供刪除或銷毀之佐證資訊與紀錄。			
2.4.4.3.5.7	g.資訊安全事件之通報流程及處理程序。			
	(4)委外稽核			
2.4.4.4	A.定期進行查核作業。	(4)委外稽核		
2.4.4.4.1		A.若核心系統作業為委外之業務項目，需符合保險業作業委託他人處理應注意事項之規定，並定期進行實地查核。		
	B.辦理作業委外稽核時，於簽訂			

項目編號	查核事項		法令規章	說明
	修正後	修正前		
2.4.4.4.2	之合約應載明保留相關之稽核權利，得自行或委託獨立單位對委外廠商監督及查核之權責行為。 C.執行委外稽核作業後，應對稽核紀錄之文件進行複審及保存並由需求單位進行存查。	B.辦理作業委外稽核時，於簽訂之合約應載明保留相關之稽核權利，得自行或委託獨立單位對委外廠商監督及查核之權責行為。 C.執行委外稽核作業後，應對稽核紀錄之文件進行複審及保存並由需求單位進行存查。		
2.4.4.4.3				
	5.核心資訊系統作業委外：			
2.4.4.5	(1)是否辦理可行性分析、效益分析及評估委外風險與對策？專案成員中是否有資安人員參與？			
2.4.4.5.1				
2.4.4.5.2	(2)招標文件是否包含對資安要求事項，並明定資安要求事項之服務水準、罰責標準等？			
2.4.4.5.3	(3)遴選廠商時是否評估核心系統委外位置與提供產品或服務之位置，對資安有無不利影響，並納入評估項目。			
2.4.4.5.4	(4)核心資訊系統作業委外涉及敏感性或含資安疑慮時，是否識別委外廠商之限制，並邀請廠商提出資安對應方案？			
2.5.4	4.核心資訊系統及直接提供客戶自動	4.核心資訊系統及直接提供客戶自動	保險業辦理資訊安全防護	新增查核事項

項目編號	查核事項		法令規章	說明
	修正後	修正前		
	化服務系統日誌紀錄管理：	化服務系統稽核紀錄管理	自律規範第 17 條	
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？	(1)系統產生之稽核紀錄（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）是否有保留機制及存取管理？		
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？		
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，且定期備份日誌紀錄至原系統外之其他系統；或建置日誌伺服器？	(3)是否依據稽核紀錄儲存需求，配置稽核紀錄所需之儲存容量或建置日誌伺服器？		
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；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？			
2.6	(六)電子商務業務系統維護與管理	(六)電子商務業務系統維護與管理	1.保險業辦理電子商務應注意事項 2.保險業經營電子商務自	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		
			律規範	
2.6.1.3.3	C.核心資訊系統：是否至少每半年進行一次作業系統之弱點掃描，會員公司依掃描結果應進行風險評估，評估為高風險以上之弱點應於3個月內修補或完成補償性控制措施，評估為中、低風險應訂定適當措施及完成時間，執行矯正、紀錄處理情形並追蹤改善。		保險業辦理資訊安全防護自律規範第14條	新增查核事項及法令規章
2.6.1.3.4	D.核心資訊系統如為開放式系統，新系統或系統功能首次上線前及至少每半年應針對異動程式進行程式碼掃描或黑箱測試，並針對其掃描或測試結果進行風險評估，及針對不同風險訂定適當措施及完成時間，執行矯正、記錄處理情形並追蹤改善。			
2.6.1.3.5	E.提供員工外部連線使用之資訊系統，是否定期執行弱點掃描、滲透測試、原始碼掃描，並於指定時間內完成弱點修補？是否強化網頁防竄改機制及納入監控範圍。		保險業電腦系統資訊安全評估作業原則	
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	(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	1.本會保險局 109.5.4 保局(綜)字第 10904917361	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		
	教育訓練？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?	教育訓練？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?	號函 2.保險業電腦系統資訊安全評估作業原則 3.保險業電子商務參考查核項目	
~~2.6.1.7~~	(刪除)	(7)新系統或系統功能首次上線前及至少每半年是否有對異動程式進行程式碼掃描或黑箱測試？對其掃描或測試結果是否進行風險評估？	保險業辦理資訊安全防護自律規範第 14 條第 2 款	已併入其他查核事項，爰刪除本項
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？	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~~ 2.保險業電腦系統資訊安全評估作業原則	修正法令規章
2.6.5.1.2.4	d.與雲端服務提供者簽訂服務協議，維持所需之服務水準並定期提出報告與操作紀錄（如服務水準報告、系統變更紀錄、作業系統映像檔存取紀錄等）		保險業運用新興科技作業原則	新增查核事項
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	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		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		
	料或敏感資料等全數刪除、銷毀或不可復原，並留存刪除或銷毀之紀錄，以供查驗?	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?		
~~2.6.5.4.5~~	(刪除)	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？		配合法令修正及併入其他查核事項，爰刪除本項
2.6.5.4.5 ~~2.6.5.4.6~~	E.是否於首次使用生物辨識技術、每年定期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?	F. 是否於首次使用生物辨識技術、每年定期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?	保險業運用新興科技作業原則	修正查核事項項次
2.6.5.4.6 ~~2.6.5.4.7~~	F.運用生物特徵資料做為識別客戶身分時，其蒐集、處理及利用之行為，是否納入個資管理機制？包括於合約終止時，是否將該資料刪除並留存相關證據？	G.運用生物特徵資料做為識別客戶身分時，其蒐集、處理及利用之行為，是否納入個資管理機制？包括於合約終止時，是否將該資料刪除並留存相關證據？	1.保險業運用新興科技作業原則 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第 8 及 14 條 3.個人資料保護法第 11 條	
2.6.7	7.與客戶端之應用程式是否採加密連線，另對交付給客戶之應用程式，有無辦理下列檢測： (1)提供 https,SFTP 者應進行弱點掃	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	保險業電腦系統資訊安全評估作業原則	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		
	描。 (2)程式原始碼掃描或滲透測試。 (3)敏感性資料保護檢測(如記憶體、儲存媒體)。 (4)金鑰保護檢測。 (5)採最小權限原則，僅允許使用者依任務及業務功能所需完成指派之授權存取控管。	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(如記憶體、儲存媒體)。 (4)金鑰保護檢測。 (5)採最小權限原則，僅允許使用者依任務及業務功能所需完成指派之授權存取控管。		
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?不符合要求之檢測項目是否檢測報告提出？檢核結果是否與說明矛盾?	(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?	保險業提供行動應用程式（APP）作業原則	修正查核事項及新增法令規章
2.6.9	9.是否建立物聯網設備管理清冊，及每年至少更新一次？是否限制物聯網設備對網際網路不要之網路連線？物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」？	9.是否建立物聯網設備管理清冊？物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」？	1.保險業辦理資訊安全防護自律規範 2.保險業使用物聯網設備作業準則	修正查核事項及新增法令規章
2.6.10.3	(3)使用虛擬私有網路(VPN)或虛擬桌面(Virtual Desktop)之方式由外部連線內部電腦系統時，是否採多因子驗證，及進行異常連線管理。		保險業辦理資訊安全防護自律規範第 19 條	新增查核事項及法令規章
2.6.11	11.辦理電子商務運用網路身分驗證	11.辦理電子商務運用網路身分驗證	~~保險業網路身分驗證之資~~	修正查核事項及新增法

項目編號	查核事項		法令規章	說明
	修正後	修正前		
	技術，是否依據保險業電子商務身分驗證之資訊安全作業準則辦理？	技術，是否依據保險業網路身分驗證之資訊安全作業準則辦理？	~~訊安全作業準則~~ 保險業電子商務身分驗證之資訊安全作業準則	令規章
2.6.11.1	(1)運用多因子驗證是否依下列規定辦理：	(1)多因子驗證可運用的因子包含帳號及密碼、一次性密碼(OTP)、智慧卡、憑證、生物特徵辯識、或符合 FIDO 標準的驗證方式（Fast Identity Online）及 Mobile ID 行動身分識別服務等，運用多因子驗證是否依下列規定辦理：		
2.6.11.1.1	A.帳號及密碼、一次性密碼(OTP)安全性設計，是否參考「保險業電子商務身分驗證之資訊安全作業準則」執行？	A.帳號及密碼、一次性密碼(OTP)安全性設計，是否參考「保險業網路投保註冊會員密碼之設計安全作業準則」執行？		
2.6.11.1.4	D.生物特徵辨識是否符合「保險業運用新興科技作業原則」之(伍、生物特徵資料安全控管)規範？	D.生物特徵辯識是否符合「保險業運用新興科技作業原則」之(伍、生物特徵資料安全控管)規範？		修正查核事項
2.6.11.1.7	G.採用多因子驗證之安全設計是否具下列三項之任兩項以上技術：		保險業電子商務身分驗證之資訊安全作業準則第 6 條	新增查核事項及法令規章
2.6.11.1.7.1	a.使用者與保險業所約定之資訊，且無第三人知悉（如密			

項目編號	查核事項		法令規章	說明
	修正後	修正前		
	碼、圖形鎖、手勢等)。			
2.6.11.7.2	b.使用者所持有之設備，保險業是否已確認該設備為使用者與其所約定持有之實體設備（如密碼產生器、密碼卡、晶片卡、電腦、行動裝置、憑證載具等)。			
2.6.11.7.3	c. 使用者所擁有之生物特徵(如指紋、臉部、虹膜、聲音、掌紋、靜脈、簽名等)，保險業是否直接或間接驗證該生物特徵。			
2.6.11.2	(2)網路身分驗證，是否符合「保險業辦理電子商務應注意事項規範」，並依下列規定辦理：	(2)辦理網路身分認證，是否有依下列規定辦理：	1. 保險業辦理電子商務應注意事項規範 2.保險業電子商務身分驗證之資訊安全作業準則第 8 條	修正查核事項及新增法令規章
2.6.11.2.1	A.建立身分驗證控管機制是否有防範自動化程式之登入或密碼更換嘗試？	A.建立身份驗證機制是否有防範自動化程式之登入或密碼更換嘗試？		
2.6.11.2.2	B.當進行密碼重設機制(如忘記密碼)時，是否有針對使用者發送一次性及具有時效性符記？	B.當進行密碼重設機制時，是否有針對使用者重新身分確認，並發送一次性及具有時效性符記？		
2.6.11.2.3	C.供應商或合作廠商之網路身分驗證，是否有依合作性質建立適當控管機制，如限制登入 IP 及加強進行登入身分核實？	C.供應商或合作廠商之網路身分驗證，是否有依合作性質建立適當控管機制，如限制登入 IP 及加強進行登入身分核實？		

項目編號	查核事項		法令規章	說明
	修正後	修正前		
2.6.12 2.6.12.1 2.6.12.2 2.6.12.3	12.辦理「保全／理賠聯盟鏈」業務 (1)針對所傳輸或儲存之申請人個人資料或敏感資料，是否建置適當之保護設備或技術，採取適當之存取管制？ (2)是否監控並建立資通安全事件通報程序？遇事件發生時，相關單位及人員是否依循通報程序辦理？	12.辦理「保全／理賠聯盟鏈」業務 (1)針對所傳輸或儲存之申請人個人資料或敏感資料，是否建置適當之保護設備或技術，採取適當之存取管制？ (2)是否監控並建立資通安全事件通報程序？遇事件發生時，相關單位及人員是否依循通報程序辦理？	1.保險業辦理「保全／理賠聯盟鏈」業務應遵循事項規範第 7 條第 5 款第 4 及 5 目 2.保險業網路電子商務身分驗證之資訊安全作業準則第 9 條	新增法令規章
3.3.4	4.提供跨機構合作夥伴資訊服務者，是否採用雙因子認證或相關身分驗證方式、定期辦理帳號密碼變更及帳號清查？	4.提供跨機構合作夥伴資訊服務者，是否採用雙因子認證或相關身分驗證方式且帳號密碼應定期變更？	保險業辦理資訊安全防護自律規範第 18 條	修正查核事項及新增法令規章