

## 六、資訊作業之查核

項 目 編 號	查 核 事 項	法 令 規 章
1	一、組織管理	保險業內部控制及稽核制度實施辦法第 6 條
1.1	(一)內部組織與職務分工	
1.1.1	1.資訊單位是否獨立於其他部門？	
1.1.2	2.是否有高階人員組成資訊作業推動小組負責審議、核准或督導、協調下列事項？ (1)資訊作業重要規章。 (2)資訊作業中、長期計畫。 (3)資訊作業安全控管措施。 (4)重要軟硬體系統購置、更新。 (5)資訊作業預算。 (6)資訊作業成本效益評估。 (7)重要專案之進度及目標達成情形。	
1.1.3	3.是否有明確資訊單位各科（組）職掌訂定？各科（組）權責是否有重疊情形？人員配置是否適當？	

項 目 編 號	查 核 事 項	法 令 規 章
1.1.4	4.下列工作有無適當之職責分工？ (1)應用系統分析與設計。 (2)系統軟體建置與維護。 (3)電腦主機操作。 (4)連線管理(安全控管)。 (5)作業或資料管制。 若無，有無配合之控管措施？	金融機構資訊系統安全基準
1.1.5	5.人員管理與訓練	
1.1.5.1	(1)人事任免及適任性評估是否建立妥善管理制度，並落實執行？對資訊作業人員之進用，是否依規定填具保密切結書，並辦理人事查核，隨時督導考核？	
1.1.5.2	(2)是否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？	保險業辦理資訊安全防護自律規範第4條
1.1.5.3	(3)是否制定移交制度，對於調離職人員是否點收其保管之文物，取銷其使用者代號、密碼並收繳其通行證、卡及相關證件？	
1.1.5.4	(4)對預定解僱或已遞出辭呈之人員是否有控制	

項 目 編 號	查 核 事 項	法 令 規 章
1.1.5.5	其接近敏感之程式或檔案、並禁止在非正常上班時間使用電腦？ (5)如有外雇人員，其管理是否有明確的規範，以確保重要資料無外洩之可能？	1.保險業內部控制及稽核制度實施辦法第 6 條 2.金融機構資訊系統安全基準
1.1.5.6	(6)各級人員是否有充分的在職訓練及資安教育訓練？教育訓練計畫之擬定是否切合業務需要，年度教育訓練計畫執行情形是否落實？	
1.2	(二)管理辦法及作業規範之訂定	
1.2.1	1.為健全資訊作業制度，是否分別或綜合訂定下列有關規範？以作為資訊作業操作、管理、查核之依據： (1)有關係統文件標準化之規範。 (2)有關係統開發、維護規範。 (3)有關電腦軟硬體系統及其附屬設施之管理規範。 (4)有關係統操作之一般規範。 (5)有關批次作業處理操作規範。 (6)有關程式及資料檔案管理及維護規範。	

項 目 編 號	查 核 事 項	法 令 規 章
1.2.2	<p>(7)有關媒體管理規範。</p> <p>(8)系統故障對策及災變因應措施。</p> <p>(9)有關委外作業之管理規範。</p> <p>(10)有關內部工作分配及其管理之規範。</p> <p>(11)有關內部自行查核之規範。</p> <p>上述規範之訂定，稽核部門是否有派員參與？</p> <p>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？</p>	保險業辦理資訊安全防护自律規範第 4 條
1.2.3	3.工作計畫之訂定	
1.2.3.1	(1)有無訂定電腦軟硬體、人力配置及資訊作業之短、中、長期計畫，並經該機構最高階主管核定？	
1.2.3.2	(2)所訂計畫項目是否符合業務上之需求？	
1.2.3.3	(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	保險業辦理資訊安全防护自律規範第 4 條

項 目 編 號	查 核 事 項	法 令 規 章
1.3	維持其正確性？ (三)資訊安全管理	
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.本會保險局 105.11.17 保局(綜)字第 1050087049 號書函 2.保險業辦理資訊安全防护自律規範
1.3.1.1	(1)對於保險業辦理資訊安全防护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？	3.本會保險局 106.3.1 保局(綜)字第 10602560070 號函 4.保險業辦理電子商務應注意事項
1.3.1.2	(2)是否取得個人資訊管理制度(PIMS)及資訊安全管理制度(ISMS)認證？	
1.3.1.3	(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：	1.保險業內部控制及稽核制度實施辦法第 6 條之 1 2.公開發行公司建立內部控制制度處理準則第 9 條之 1
1.3.2.1	(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)	3.本會 110.12.28 金管證審字第 11003656544 號令
1.3.2.2	(2)保險業達一定規模者，是否指派副總經理以	

項 目 編 號	查 核 事 項	法 令 規 章
1.3.2.3	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？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？	
1.3.2.4	(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？	
1.3.2.5	(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？	
1.3.2.5.1	(5)是否依人身保險業辦理資訊公開管理辦法強化資通安全之管理，並於年度終了後三個月內更新？	人身保險業辦理資訊公開管理辦法第8條第20款
	A.是否敘明資通安全風險管理架構、資通安	

項 目 編 號	查 核 事 項	法 令 規 章
1.3.2.5.2	全政策、具體管理方案及投入資通安全管理之資源等？ B.是否揭露最近年度因重大資通安全事件所遭受之損失、可能影響及因應措施，如無法合理估計者，應說明其無法合理估計之事實及原因？	
1.3.2.5.3	C.是否揭露資通安全風險對公司財務業務之影響及因應措施？	
1.3.3	3.發展金融科技服務，董事會與高階管理階層是否有效評估金融科技經營與風險管理？是否同時評估金融服務使用雲端運算、大數據分析個資管理、行動應用 App 安全等資安風險？是否將相關資訊安全管理納入公司治理架構？	
1.3.4	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？	保險業辦理資訊安全防护自律規範第 13 條
1.4	(四)營運環境管理人員之遵循情形	保險業辦理資訊安全防护自律規範第 4 條之 1
1.4.1	1.是否建立人員之註冊、異動及撤銷註冊程序，	

項 目 編 號	查 核 事 項	法 令 規 章
1.4.2	<p>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？</p> <p>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？</p>	
1.4.3	<p>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？</p>	
1.4.4	<p>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？</p>	
1.4.5	<p>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？</p>	
1.4.6	<p>6.採用固定密碼進行身分確認時，是否符合下列要求：</p>	
1.4.6.1	<p>(1)訂定密碼檢核邏輯。</p>	
1.4.6.2	<p>(2)使用後三個月內應變更密碼。</p>	
1.4.6.3	<p>(3)提供給系統使用之帳號應採取適當之管控</p>	



項 目 編 號	查 核 事 項	法 令 規 章
1.4.7	措施（如限制人工登入、監控告警）。 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，是否先取得權責主管或授權人員同意，並保留稽核軌跡？	
1.4.9	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？	
1.4.10	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？	
1.4.11	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？	

項 目 編 號	查 核 事 項	法 令 規 章
1.5	(五)內部稽核辦理情形	
1.5.1	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稽核？	保險業經營電子商務自律規範第 31 條 保險業經營行動服務自律規範第 13 條
1.5.2	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？	
1.5.3	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？	
2	二、網路及系統安全控管	保險業辦理資訊安全防護自律規範
2.1	(一)網路安全控管及防範措施	
2.1.1	1.是否已明訂網際網路作業相關管理辦法及作業規範？前開規範之訂定，稽核部門是否有派員參與？	
2.1.2	2.各項作業規範或管理辦法是否周延妥適、符合內部控制原則？是否付諸實施，並適時檢討、修訂俾切合實際？	

項 目 編 號	查 核 事 項	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，以符實際運作之需？	保險業辦理資訊安全防护自律規範第 19 條
2.1.4	4.網路系統相關之硬體、軟體及通訊設備（如：網路伺服器、防火牆...等）有無適當之門禁管制措施？有否指定專責單位（人員）監管？	
2.1.5	5.對電腦中心或其他存放文件之場所有無適當之安全管制措施？	
2.1.6	6.對於各項軟、硬體設備是否有妥善之備援措施？	
2.1.7	7.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？	
2.1.7.1	(1)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	

項 目 編 號	查 核 事 項	法 令 規 章
2.1.7.2	處置所接收之資安情資？ (2)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？	保險業辦理資訊安全防护自律規範第 19 條
2.1.7.3	(3)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查核及內部稽核？	
2.2	(二)網路系統安全控管	
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？	
2.2.2	2.有關網路系統安全管制是否指定專人負責管理，並明訂其職責？對系統使用者權限設定是否嚴謹？	
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：	
2.2.3.1	(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？	
2.2.3.1.2	B.是否規定密碼最少字數？	
		1.保險業辦理資訊安全防护自律規範 2.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

項 目 編 號	查 核 事 項	法 令 規 章
2.2.3.1.3	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？	
2.2.3.1.5	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？	
2.2.3.1.7	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)	
2.2.3.2.1	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？	保險業網路電子商務身分驗證之資訊安全作業準則第4條

項 目 編 號	查 核 事 項	法 令 規 章
2.2.3.2.4	D.帳號與密碼是否相同？	
2.2.4	4.是否限定使用者登入系統失敗次數，以防止非授權人員無限制地嘗試密碼？	
2.2.5	5.對系統資源（如：檔案資料）之使用權限設定是否嚴謹？	
2.2.6	6.安全管制類報表（如：系統管理者使用紀錄、非法存取使用紀錄...）是否周全？是否確實查核並依規定陳報或陳閱？	
2.2.7	7.是否建立適當程序，以辨識任何未經過防火牆之遠端存取及如何監控、控制該項存取？	
2.2.8	8.防火牆設定維護是否指定專人負責？其異動程序是否均經申請、核可及覆核程序，並留存紀錄？	
2.2.9	9.變更防火牆設定是否經測試，並經主管審核其測試結果？防火牆設定文件是否配合修正？	
2.2.10	10.對防火牆設定相關文件是否妥善保存，並嚴格控管文件之使用？	
2.2.11	11.若防火牆係委外維護，受檢單位是否已明確定義其與廠商間之責任？	

項 目 編 號	查 核 事 項	法 令 規 章
2.2.12	12.網路系統是否建置適當之病毒偵測及預防程序？	保險業辦理資訊安全防护自律規範第 19 條
2.2.13	13.各工作站是否建置防毒軟體，以偵測及預防病毒感染？	
2.2.14	14.對重要資料之傳送是否加密，以確保網路傳輸資料之安全？	
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？	
2.3	(三)網路系統監控及偵測	
2.3.1	1.是否定期評估網路安全控制系統，並適時檢討以改進監控及偵測技術？	
2.3.2	2.是否利用網路監控軟體並指定專人監看網路流量？並即時注意異常狀況？	
2.3.3	3.網路活動日誌是否指定專人每日檢視並呈核主管？	
2.3.4	4.對於監控及偵測之異常事件是否明確定義須通報之事件？是否建置適當之通報機制，並依規	

項 目 編 號	查 核 事 項	法 令 規 章
2.3.5	定分別陳報單位主管或管理階層？ 5.受檢單位若委外作業進行網際網路安全檢測（如入侵測試、病毒預防偵測等），是否注意下列事項：	金融機構資訊系統安全基準
2.3.5.1	(1)是否由客觀第三者執行入侵測試？	
2.3.5.2	(2)執行入侵測試之人員是否能提供適當保證？	
2.3.5.3	(3)如何決定測試頻率？係採一年至少執行一次入侵測試或依管理者對風險分析及對風險之容忍度決定可接受之入侵測試頻率？	
2.3.5.4	(4)入侵測試結果是否經相關主管人員覆核？測試結果及相關文件是否嚴格管制調閱？	
2.4	(四)系統開發及維護管理	
2.4.1	1.系統開發管理	
2.4.1.1	(1)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： 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。	



項 目 編 號	查 核 事 項	法 令 規 章
	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。	
2.4.1.2	(2)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？	
2.4.1.3	(3)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？	
2.4.1.4	(4)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？	
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益？	個人資料保護法第 5 條
2.4.1.6	(6)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？	

項 目 編 號	查 核 事 項	法 令 規 章
2.4.1.7	(7)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？	
2.4.1.8	(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？ 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	(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：	
2.4.1.9.1	A.系統轉換前之準備工作：	
2.4.1.9.1.1	a.是否建立架構審查機制。	
2.4.1.9.1.2	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。	
		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

項 目 編 號	查 核 事 項	法 令 規 章
2.4.1.9.1.3	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。	
2.4.1.9.1.4	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。	
2.4.1.9.1.5	e.是否預留復原作業及上線驗證時間。	
2.4.1.9.1.6	f.是否要求設備提供廠商與委外開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	

項 目 編 號	查 核 事 項	法 令 規 章
2.4.1.9.3.2	續營運優先處理。 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。	金融機構資訊系統安全基準
2.4.2	2.系統維護管理	
2.4.2.1	(1)對每一應用系統，是否均派專人負責維護的工作？	
2.4.2.2	(2)修改系統時，是否採取足夠的控制，以免修改人員接觸未經許可修改之部份？	
2.4.2.3	(3)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？	
2.4.2.4	(4)已正式實施之作業，其程式變更：	
2.4.2.4.1	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？	
2.4.2.4.2	B.書面申請是否詳細敘明變更原因及內容？	
2.4.2.4.3	C.修改後是否加以測試（含第三者），並經主管審核其測試結果？	
2.4.2.4.4	D.對修改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	

項 目 編 號	查 核 事 項	法 令 規 章
2.4.2.4.5	核？ E.系統說明文件是否配合修正？	金融機構資訊系統安全基準
2.4.2.4.6	F.操作程序上如有變更是否通報有關單位？	
2.4.3	3.系統文件編製	
2.4.3.1	(1)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。	
2.4.3.2	(2)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？	
2.4.3.3	(3)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，	

項 目 編 號	查 核 事 項	法 令 規 章
2.4.3.4	並留存紀錄備查？ (4)系統說明文件之撰寫及程式、檔案名稱之命名是否標準化？	
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？	1.保險業辦理資訊安全防护自律規範第 16 條 2.保險業核心資通系統作業委外資安注意事項
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。	
2.4.4.2	(2)審核作業委外廠商資格	
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。	
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。	
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	

項 目 編 號	查 核 事 項	法 令 規 章
2.4.4.3	商評估項目。	
2.4.4.3.1	(3)作業委外廠商管理要項 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。	
2.4.4.3.3	C.若作業委外內容有重大變更或重大事件時，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：	

項 目 編 號	查 核 事 項	法 令 規 章
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。	
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，需考量具個人資料安全防範措施。	
2.4.4.3.5.3	c.應訂定相關資訊安全管理責任。	
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。	



項 目 編 號	查 核 事 項	法 令 規 章
2.4.4.4	(4)委外稽核	
2.4.4.4.1	A.定期進行查核作業。	
2.4.4.4.2	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。	
2.4.4.4.3	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。	
2.4.4.5	5.核心資訊系統作業委外：	
2.4.4.5.1	(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？	
2.4.4.5.2	(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)資訊安全事件之通報流程及處理程序。	
2.4.4.5.4	(4)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？	

項 目 編 號	查 核 事 項	法 令 規 章
2.4.4.5.5	(5)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	(五)運作管理	
2.5.1	1.主機操作管理	
2.5.1.1	(1)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？	金融機構資訊系統安全基準
2.5.1.2	(2)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？	金融機構資訊系統安全基準
2.5.1.3	(3)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？	
2.5.1.4	(4)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？	
2.5.1.5	(5)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？	
2.5.1.6	(6)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？	

項 目 編 號	查 核 事 項	法 令 規 章
2.5.1.7	(7)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？	
2.5.1.8	(8)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？	
2.5.1.9	(9)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？	
2.5.1.10	(10)電腦作業是否經常發生重覆處理情形？其原因為何？有否採取適當措施以減少發生？	
2.5.1.11	(11)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？	
2.5.2	2.端末機使用管理	
2.5.2.1	(1)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？是否定	金融機構資訊系統安全基準

項 目 編 號	查 核 事 項	法 令 規 章
2.5.2.2	<p>期審核資訊系統帳號？</p> <p>(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？</p>	金融機構資訊系統安全基準
2.5.2.3	<p>(3)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變更？是否由系統自動留存作業紀錄俾供查核？</p>	
2.5.2.4	<p>(4)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？</p>	
2.5.2.5	<p>(5)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？</p>	
2.5.2.6	<p>(6)對於調離職人員，是否立即取消其使用者代號、密碼？</p>	

項 目 編 號	查 核 事 項	法 令 規 章
2.5.3	3.程式、資料檔案管理	
2.5.3.1	(1)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？	金融機構資訊系統安全基準
2.5.3.2	(2)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？	
2.5.3.3	(3)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？	
2.5.3.4	(4)具有修改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？	
2.5.3.5	(5)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？	金融機構資訊系統安全基準
2.5.3.6	(6)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？	金融機構資訊系統安全基準
2.5.3.7	(7)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？	

項 目 編 號	查 核 事 項	法 令 規 章
2.5.3.8	(8)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？	金融機構資訊系統安全基準
2.5.3.9	(9)是否禁止主機操作員存取正式作業程式、資料檔案及應用系統說明文件（操作手冊除外）？	
2.5.3.10	(10)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？	
2.5.3.11	(11)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？	
2.5.3.12	(12)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？	
2.5.3.13	(13)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？	
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：	保險業辦理資訊安全防護自律規範第 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	

項 目 編 號	查 核 事 項	法 令 規 章
2.5.4.2	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)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？	
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？	
2.5.4.5	(5)是否訂定日誌處理失效之告警及應處機制？	
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护自律規範第 17 條
2.6	(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

項 目 編 號	查 核 事 項	法 令 規 章
2.6.1	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	2.保險業經營電子商務自律規範
2.6.1.1	(1)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？	保險業電子商務參考查核項目
2.6.1.2	(2)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？	
2.6.1.3	(3)辦理弱點掃描與滲透測試	保險業辦理資訊安全防護自律規範第 14 條第 1 款
2.6.1.3.1	A.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？後續修補管控機制是否妥適？	
2.6.1.3.2	B.對網際網路應用系統是否至少每季進行一次作業系統之弱點掃描，並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 2 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	



項 目 編 號	查 核 事 項	法 令 規 章
2.6.1.3.3	<p>蹤改善。</p> <p>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。</p>	保險業辦理資訊安全防护自律規範第 14 條
2.6.1.3.4	<p>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。</p>	
2.6.1.4	<p>(4)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？</p>	
2.6.1.5	<p>(5)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</p>	

項目編號	查核事項	法令規章
2.6.1.6	建立覆核機制？ (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？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？	1.本會保險局 109.5.4 保局（綜）字第 10904917361 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
2.6.2	2.辦理電子商務業務管理：	保險業電子商務參考查核項目
2.6.2.1	(1)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？	
2.6.2.2	(2)是否訂定偵測偽冒網站之處理措施？	保險業電腦系統資訊安全評估作業原則
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？	1.保險業經營電子商務自律規範 2.保險業電腦系統資訊安全評估作業原則
2.6.4	4.行動投保業務系統維護與管理	保險業經營行動服務自律規範
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	保險業經營行動服務自律規範第 6 條

項 目 編 號	查 核 事 項	法 令 規 章
2.6.4.3	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？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？	保險業經營行動服務自律規範第 9 條
2.6.4.3.1	(3)辦理行動投保業務，是否建立資訊安全控管機制？ 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？	
2.6.4.3.2	B.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？	
2.6.4.3.3	C.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？	

項 目 編 號	查 核 事 項	法 令 規 章
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）	保險業辦理資訊安全防护自律規範
2.6.5.1	(1)雲端服務安全控管	保險業運用新興科技作業原則
2.6.5.1.1	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
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：	
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。	
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。	
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。	
2.6.5.1.2.4	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	保險業運用新興科技作業原則

項 目 編 號	查 核 事 項	法 令 規 章
2.6.5.1.3	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）。	保險業作業委託他人處理應注意事項第 18 條
2.6.5.1.4	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？	
2.6.5.1.5	D.是否監控並建立資通安全事件通報程序？	
2.6.5.1.6	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、銷毀或不可復原，並留存刪除或銷毀之紀錄，以供查驗？	保險業運用新興科技作業原則
2.6.5.1.7	F.是否制定雲端資料管理程序，並明訂資料保存期限及應留存之相關重要軌跡紀錄？	
2.6.5.1.8	G.是否遵循「個人資料保護法」，資料當事人如申請行使其權利，要求停止處理或利用其資料？是否確保其資料皆從雲端刪除或提供相關佐證？	
	H.是否具專業技術及資源監督雲端服務業者	

項 目 編 號	查 核 事 項	法 令 規 章
	執行受託作業，或委託專業第三人輔助監督作業？	保險業作業委託他人處理應注意事項第 18 條
2.6.5.1.9	I.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：	保險業作業委託他人處理應注意事項第 18 條
2.6.5.1.9.1	a. 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。	
2.6.5.1.9.2	b. 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。	
2.6.5.1.9.3	c. 對所委託作業範圍進行查核並出具報告。	
2.6.5.1.10	J.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：	保險業作業委託他人處理應注意事項第 18 條
2.6.5.1.10.1	a. 保有指定資料處理及儲存地之權利。	
2.6.5.1.10.2	b. 境外當地資料保護法規不得低於我國要求。	
2.6.5.1.10.3	c. 涉及重大性自然人客戶業務資訊系 統	

項 目 編 號	查 核 事 項	法 令 規 章
2.6.5.2	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。	保險業運用新興科技作業原則
2.6.5.2.1	(2)社群媒體控管程序 A.是否制定社群媒體管理政策，並定期檢視？	
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？	
2.6.5.2.3	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？	保險業運用新興科技作業原則
2.6.5.3	(3)自攜裝置安全控管	
2.6.5.3.1	A.是否制定自攜裝置管理政策，並定期檢視？	
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)？	
2.6.5.3.3	C.使用人員與裝置是否列冊管理，且至少每年審閱一次？對自攜裝置採取之資安管控措施，是否包括制定自攜裝置連網環境標	

項 目 編 號	查 核 事 項	法 令 規 章
2.6.5.3.4	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?	
2.6.5.4	(4)生物特徵資料安全控管	保險業運用新興科技作業原則
2.6.5.4.1	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?	
2.6.5.4.2	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?	
2.6.5.4.3	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?	
2.6.5.4.4	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)?	保險業運用新興科技作業原則
2.6.5.4.5	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	保險業運用新興科技作業原則



項 目 編 號	查 核 事 項	法 令 規 章
2.6.5.4.6	別客戶身分? 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？	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
2.6.6	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？	1.保險業辦理資訊安全防護自律規範 2.保險業電腦系統資訊安全評估作業原則
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：	保險業電腦系統資訊安全評估作業原則
2.6.7.1	(1)提供 https、SFTP 者應進行弱點掃描。	
2.6.7.2	(2)程式原始碼掃描或滲透測試。	
2.6.7.3	(3)敏感性資料保護檢測(如記憶體、儲存媒體)。	
2.6.7.4	(4)金鑰保護檢測。	
2.6.7.5	(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。	

項 目 編 號	查 核 事 項	法 令 規 章
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？	1.保險業辦理資訊安全防護自律規範 2.保險業提供行動應用程式作業(APP)原則
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？不符合要求之檢測項目是否於檢測報告提出？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
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？	

項 目 編 號	查 核 事 項	法 令 規 章
2.6.8.6	(6)是否進行身分驗證相關資訊不以明文傳輸並具備帳戶鎖定機制？	保險業提供行動應用程式(App)作業原則
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」？	1.保險業辦理資訊安全防护自律規範 2.保險業使用物聯網設備作業準則
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护自律規範
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？	

項 目 編 號	查 核 事 項	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护自律規範第 19 條
2.6.10.4	(4)遠端作業時，是否使用會員公司配發之裝置或設備？或使用資料不落地之機制？	
2.6.11	11.辦理電子商務運用網路身分驗證技術，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？	保險業電子商務身分驗證之資訊安全作業準則
2.6.11.1	(1) 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？	
2.6.11.1.2	B.智慧卡應設有密碼功能(Pin Code)，於晶片進行密碼驗證，晶片是否符合共通準則(Common Criteria) EAL 4+以上或其他相同安全強度之認證。	
2.6.11.1.3	C.憑證是否由憑證機構依經濟部核定之憑證實務作業基準簽發？憑證是否具有時效	

項 目 編 號	查 核 事 項	法 令 規 章
2.6.11.1.4	性？過期是否立即失效，須重新簽發或展延期限？ 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？	保險業電子商務身分驗證之資訊安全作業準則第 6 條
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？	
2.6.11.1.6	F.Mobile ID 行動身分識別服務是否由提供手機門號之電信業者進行身分驗證？	
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：	
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（如密碼、圖形鎖、手勢等）。	
2.6.11.1.7.2	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）。	
2.6.11.1.7.3	c.使用者所擁有之生物特徵(如指紋、臉	

項 目 編 號	查 核 事 項	法 令 規 章
2.6.11.2.	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。	
2.6.11.2.1	(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： 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？	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
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？	
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？	
2.6.12	12.辦理「保全／理賠聯盟鏈」業務	1.保險業辦理「保全／理賠聯盟鏈」業務應遵循事項規範第7
2.6.12.1	(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？	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
2.6.12.2	(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	

項 目 編 號	查 核 事 項	法 令 規 章
3	程序辦理？ 三、個人資料安全維護	
3.1	(一)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	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
3.1.1	1.是否依其業務規模及特性，衡酌經營資源之合理分配，配置管理之人員及相關資源，以規劃、訂定、修正與執行其個人資料檔案安全維護計畫、業務終止後個人資料處理方法、資安事故應變、通報及預防機制、員工教育訓練、設備安全及資安措施等內部規範？	
3.1.2	2.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？	
3.1.3	3.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？	
3.1.4	4.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？	
3.2	(二)對個資之儲存、傳遞及使用之控管機制	1.個人資料保護法

項 目 編 號	查 核 事 項	法 令 規 章
3.2.1	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？)	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
3.2.2	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？	
3.2.3	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？	
3.2.4	4.對 FTP、檔案分享(如網路芳鄰、SAMB A)、檔案下載、電子郵件等傳檔功能之應用程式，是否訂定控管機制、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？	
3.2.5	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	



項 目 編 號	查 核 事 項	法 令 規 章
3.2.6	<p>使用管理機制、留存完整稽核軌跡，並落實執行？</p> <p>6.提供電子商務服務系統，是否採取下列資訊安全措施？</p> <p>(1)使用者身分確認及保護機制。</p> <p>(2)個人資料顯示之隱碼機制。</p> <p>(3)網際網路傳輸之安全加密機制。</p> <p>(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。</p> <p>(5)個人資料檔案及資料庫之存取控制與保護監控措施。</p> <p>(6)防止外部網路入侵對策。</p> <p>(7)非法或異常使用行為之監控與因應機制。</p>	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
3.2.7	<p>7.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？</p>	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 14 條
3.2.8	<p>8.保有個人資料之特定目的消失或期限屆滿者，是否依規定刪除、停止處理或利用？</p>	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 條
3.2.9	<p>9.設備或儲存媒體報廢或轉作他用時，是否採取</p>	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

項 目 編 號	查 核 事 項	法 令 規 章
3.3	防範資料洩漏之適當措施？ (三)對提供客戶資訊予委外機構、合作推廣、共同行銷或集團關係企業之管理機制	辦法第 9 條
3.3.1	1.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？	
3.3.2	2.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？	
3.3.3	3.與跨機構合作夥伴合約簽訂時，是否進行風險評估並規劃風險處置措施？於雙方簽訂備忘錄或契約中，是否載明相關要求，如：資訊安全及保戶個人資料保護相關條款、禁止多人共用同一帳號、相關業務往來之查核機制或控管措施？	保險業辦理資訊安全防护自律規範第 18 條
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？	保險業辦理資訊安全防护自律規範第 18 條

項 目 編 號	查 核 事 項	法 令 規 章
4.	四、災害應變	
4.1	(一)安全控制	
4.1.1	1.環境安全防護	
4.1.1.1	(1)電腦設備及相關設施之安全防護是否完善？	
4.1.1.1.1	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？	
4.1.1.1.2	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？	
4.1.1.1.3	C.有無裝置火災自動警報系統及自動滅火設備？	
4.1.1.1.4	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？	
4.1.1.1.5	E.保險及維護契約涵蓋範圍是否完全？並在有效期間內？	
4.1.1.2	(2)機房是否放置非工作需要或危險物品？	
4.1.1.3	(3)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？	

項 目 編 號	查 核 事 項	法 令 規 章
4.1.1.4	(4)系統說明文件存放場所是否有防火、防水等安全防護措施？	金融機構資訊系統安全基準
4.1.2	2.人員進出管理	
4.1.2.1	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？	
4.1.3	3.備援措施	金融機構資訊系統安全基準
4.1.3.1	(1)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？	
4.1.3.2	(2)程式及資料檔案	
4.1.3.2.1	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？	
4.1.3.2.2	B.各種重要程式及資料檔案是否有損毀時之	

項 目 編 號	查 核 事 項	法 令 規 章
4.1.3.2.3	重建程序？ C.對於儲存資料或程式之媒體是否責成專人負責管理？	保險業電腦系統資訊安全評估作業原則
4.1.3.2.4	D.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？	
4.1.3.2.5	E.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？	
4.1.3.2.6	F.媒體廢棄前是否先經銷磁或其他處理，以防媒體資料外洩？	
4.1.3.2.7	G.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）？	
4.1.3.2.8	H.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？	
4.1.3.2.9	I.備份之系統備份媒體，是否擬定驗證計畫，並驗證備份媒體之可靠性及資訊之完整性。	
4.1.3.3	(3)人員 各項重要工作是否均有備援人員？	

項 目 編 號	查 核 事 項	法 令 規 章
4.1.3.4	(4)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？	
4.1.4	4.故障及災害因應對策	
4.1.4.1	(1)是否分別或綜合訂定電腦軟硬體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？	金融機構資訊系統安全基準
4.1.4.2	(2)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？	金融機構資訊系統安全基準
4.1.4.3	(3)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？	
4.1.4.4	(4)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？	金融機構資訊系統安全基準
4.2	(二)緊急應變計畫及災害復原程序	
4.2.1	1.是否適當評估網路系統無法運作時對該單位業	保險業電子商務參考查核項目

項 目 編 號	查 核 事 項	法 令 規 章
4.2.2	<p>務之影響？</p> <p>2. 緊急應變計畫及災害復原程序，其內容是否適當？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？</p>	保險業電子商務參考查核項目
4.2.3	<p>3. 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？</p>	
4.2.4	<p>4. 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？</p>	
5	五、資訊作業委外管理	
5.1	(一) 資訊軟硬體採購及資訊系統委外開發或維護合約之管理	
5.1.1	1. 法規規定之應記載事項是否均已納入合約載明？	
5.1.2	2. 其他重要應注意事項，如：作業安全、委託內	

項 目 編 號	查 核 事 項	法 令 規 章
	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？	
5.2	(二)對協力廠商之監督管理	
5.2.1	1.對委外維護廠商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？	
5.2.2	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？	
5.2.3	3.系統委外開發作業管理	
5.2.3.1	(1)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、核定及驗收等是否比照自行開發設計準則及控管程序辦理？	
5.2.3.2	(2)委外作業業務是否有專人管理，並控制進度？	
5.2.3.3	(3)是否嚴禁委外作業廠商進入正式作業環境存	



項 目 編 號	查 核 事 項	法 令 規 章
5.2.3.4	取程式或資料？ (4)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？	
5.2.3.5	(5)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？	