「保險業作業委外使用雲端服務自律規範」

金管會 114 年 2 月 17 日金管保壽字第 1130432032 號同意備查

條文	訂定說明
保險業作業委外使用雲端服務自律規範	依金管會 112 年 11 月 20 日金管保壽字第 1120494046 號函訂定「保險業作業委外使用雲端服務自律規範」(下稱本自律規範)。
第一條 中華民國人壽保險商業同業公會與中華民國產物保險商業同業公會為確保會員公司依「保險業作業委託他人處理應注意事項」將作業委託他人處理涉及使用雲端服務具有一致性管理標準，並依風險基礎方法採取適當的控管措施，以達成妥適使用雲端服務之目的，特訂定本自律規範。	說明本自律規範訂定目的與立法意旨。
第二條 本自律規範適用之範圍，以保險業依「保險業作業委託他人處理應注意事項」將作業委託他人處理，並涉及使用雲端服務為限。除本自律規範另有訂定外，會員公司應按「保險業作業委託他人處理應注意事項」辦理。 外國保險業在臺分支機構因內部分工將作業交由國外總機構或經其授權之區域總部處理使用雲端服務者，可依國外總機構或經其授權之區域總部所訂之管控措施辦理，惟相關控管措施不得低於我國法規及自律規範之要求。外國保險業在臺分支機構應就在臺業務建立妥適內部控制制度及風險管理機制，充分掌握在臺作業雲端委外事項之控管情形。	一、說明本自律規範訂定適用範圍。 二、第二條第一項係參照「保險業作業委託他人處理應注意事項」明定適用對象，會員公司辦理作業委外涉及使用雲端服務應遵循「保險業作業委託他人處理應注意事項」之規定，並依風險基礎方法管理雲端服務作業之委外風險。 三、第二條第二項係參照「人壽保險業防制洗錢及打擊資恐、資助武擴注意事項範本」，並依據外國保險業運作實務擬訂外國保險業在臺分支機構適用範圍。
第三條 本自律規範用詞定義如下： 一、雲端服務：利用網路提供運算或儲存資源之服務模式，使用者依據需求使用網路設備、伺服器、儲存空間、應用程式等服務。如：IaaS（基礎設施即服務）、PaaS（平台即服務）、SaaS（軟體即服務）。	一、明訂本自律規範提及之名詞解釋。 二、第三條第一項第一款係依據「保險業運用新興科技作業原則」及「國家資通安全研究院」之內容，並參酌「金融機構作業委外使用雲端服務自律規範」第三條，明定雲端服務之定義。 三、第三條第一項第二款係參照「保險業作

條文	訂定說明
二、雲端服務業者(Cloud Service Provider(s), CSP)：係指提供前揭雲端服務之業者，以及透過雲端平台對客戶提供應用軟體服務、工具或解決方案之業者。 三、風險基礎方法（Risk Based Approach, RBA)：各會員公司確認、評估及瞭解其使用雲端之風險，並採取適當的防制措施以有效降低相關風險。依該方法，對於較高風險情形應採取加強措施，對於較低風險情形，則可採取相對簡化措施，以有效分配資源，並以最適當且有效之方法降低風險。 四、軟體即服務（SaaS)：雲端服務業者提供基於雲端基礎架構運行的軟體或應用程式，承租人能透過網頁瀏覽器或程式介面使用雲端服務，但並不掌控軟體、應用程式、作業系統、硬體和網路架構。 五、平台即服務（PaaS)：提供承租人使用雲端服務業者支援的程式語言、函式庫、服務和工具，以創建或取得應用程式，並部署到雲端基礎設施上的能力。承租人可掌控運作軟體的環境也擁有作業系統部分掌控權，但並不掌控作業系統、硬體和網路架構。 六、基礎設施即服務（IaaS)：雲端服務業者提供基礎運算資源(如處理能力、儲存空間、網路元件或中介軟體)，承租人能掌控作業系統、儲存空間、已自行部署的應用程式及網路元件(如防火牆、負載平衡器等)，但並不掌控雲端基礎運算資源。 七、互通性(Interoperability)：係指系統或資料可從原本受委託之雲端服務業者，移轉至其他雲端服務業者或移回會員公司。 八、服務水準協議（Service Level Agreement, SLA)：為雲端服務業者與各會員公司就雲端服務水準所約定的協議。該協議將	業委託他人處理應注意事項」與「保險業運用新興科技作業原則」所採用之名稱，並參照國家標準暨技術研究（National Institute of Standards and Technology，NIST） Special Publication 500-332「The NIST Cloud Federation Reference Architecture」 Appendix A. Cloud Federation Terms and Definitions，明定雲端服務業者之定義。 四、第三條第一項第三款係參照「人壽保險業防制洗錢及打擊資恐、資助武擴注意事項範本」第三條第一項第六款所明定之風險基礎方法定義。 五、第三條第一項第四款、第五款與第六款係參照「保險業運用新興科技作業原則」第貳條第一項第三款、第四款、第五款與NIST Special Publication 800-145「The NIST Definition of Cloud Computing」，明定軟體即服務（SaaS）、平台即服務（PaaS）與基礎設施即服務（IaaS）之定義。 六、第三條第一項第七款係參照「保險業作業委託他人處理應注意事項」第十六點第二項第六款及參酌新加坡金融管理局（Monetary Authority of Singapore, MAS）Advisory on Addressing the Technology and Cyber Security Risks Associated with Public Cloud Adoption 之降低鎖定供應商之規範意旨，明定互通性之定義。 七、第三條第一項第八款係參照 Amazon Web Services（AWS）、Google Cloud Platform（GCP）與 Microsoft Azure 之說明，明定服務水準協議之定義。

條文	訂定說明
說明雲端服務的上線時間約定，以及未達成約定服務水準時的補救措施。	
第四條 各會員公司應建立雲端服務治理機制，規劃並確認以下事項： 一、應制訂雲端服務之規範，並至少每年檢視一次。 二、專責單位及相關單位對雲端服務使用之角色權責與責任劃分。 三、建立風險評估機制，評估使用雲端服務之潛在風險。風險評估機制係指各會員公司應針對雲端服務採取風險基礎方法評估潛在風險與管理風險議題，評估項目宜包括： (一) 雲端服務使用模式與情境。 (二) 雲端服務所涉及之業務與資料。 (三) 雲端服務中斷所造成影響及衝擊程度。 (四) 雲端服務的互通性。 (五) 會員公司對於雲端服務之管理能力與經驗。 四、建立對雲端服務業者之管理盡職調查與定期審查程序。 五、依風險基礎方法進行查核及監督。 六、建立雲端服務查核及業務持續性管理要求。 七、定期舉辦或參加雲端服務相關的人才培訓，以確保會員公司具備管理雲端技術風險、監督及審查雲端服務之知識及能力。 各會員公司使用雲端服務與控管其風險事項應注意以下事項： 一、各會員公司採用雲端服務應具備定期審查制度，並應與組織資訊策略一致，以確保管理策略及機制可因應組織、外在科技等議題影響持續更新。 二、各會員公司如將作業項目委託至境外處	一、本條明定各會員公司涉及雲端服務委外事項時，應規劃及注意之治理制度與風險管理事項，包含董（理）事會及雲端服務使用之角色權責、風險管理、委外管理及雲端服務管理。 二、第四條第一項係依據「金融機構作業委外使用雲端服務自律規範」第四條第一項之內容，鑑於各會員公司執行涉及雲端服務委外事項時，應設立完善之治理制度並實施相關管理機制，明定各會員公司於使用雲端服務時應規劃事項。 三、第四條第一項第一款係依據「保險業作業委託他人處理應注意事項」第四點第一項第一款與「金融機構作業委外使用雲端服務自律規範」第四條第一項第一款訂定。 四、第四條第一項第二款係依據「保險業作業委託他人處理應注意事項」第四點第一項第二款要求內部作業規範應載明對委外事項控管之權責分工，並參酌「金融機構作業委外使用雲端服務自律規範」第四條第一項第二款之內容，故於第四條第一項第二款明定會員公司應確保專責單位與相關單位之權責分工。 五、第四條第一項第三款係依據新加坡銀行公會（The Association of Banks in Singapore, ABS）「Cloud Computing Implementation Guide 2.0」；英國金融行為監理總署（Financial Conduct Authority, FCA）「FG 16/5 Guidance for firms outsourcing to the 'cloud' and other third-party IT services」Risk management；新加坡金融管理局（Monetary Authority of Singapore, MAS）「Guidelines on Outsourcing（Financial Institutions other

條文	訂定說明
理，應評估雲端服務業者之客戶資料處理地及其儲存地之資料保護法規，不得低於我國要求。如有高風險之情形者，會員公司應採行妥適之風險控管措施。 三、作業委託雲端服務業者宜適度分散，惟採取多雲或其他分散策略時，應同時考量營運複雜性提升之風險。 四、各會員公司應依使用雲端服務之風險建立適當之監控機制，監控雲端資源負載、安全防護與服務可用性，以健全業務持續性運作。 五、應建立雲端服務資料可用性與互通性政策和程序，確保於服務結束時，可將系統遷移或資料遷出雲端服務。 董（理）事會應認知及監督各會員公司涉及雲端服務委外事項之風險，確保各會員公司對於控管雲端服務風險事項具備充足之資源、專業及權限。	than Banks）」5.3.1；歐洲保險和職業養老金管理局（European Insurance and Occupational Pensions Authority, EIOPA）「Guidelines on outsourcing to cloud service providers」Guideline 7 以及「金融機構作業委外使用雲端服務自律規範」第四條第一項第三款及第三項之內容，說明各會員公司應具備風險評估機制，採取風險基礎方法，確保各會員公司營運之穩定性，並透過建立風險管理機制確保各會員公司識別和評估委外事項涉及雲端服務之潛在風險。 六、第四條第一項第三款第四目係依據「保險業作業委託他人處理應注意事項」第七點第一項第三款要求，明定各會員公司於使用雲端服務時，應考量雲端服務資料可用性與互通性要求，降低各會員公司供應商鎖定之風險。 七、第四條第一項第四款係依據「保險業作業委託他人處理應注意事項」第四點與「金融機構作業委外使用雲端服務自律規範」第四條第一項第四款之內容，明定各會員公司建立對雲端服務業者之管理盡職調查與定期審查程序。 八、第四條第一項第五款依據「保險業作業委託他人處理應注意事項」第十七點規定，明定各會員公司依風險基礎方法進行查核及監督。 九、第四條第一項第六款係依據「保險業作業委託他人處理應注意事項」第四點、第十八點與「金融機構作業委外使用雲端服務自律規範」第四條第一項第七款之內容，明定各會員公司建立雲端服務查核及業務持續性管理要求。 十、第四條第一項第七款係依據「保險業作業委託他人處理應注意事項」第十八點之規定，並參酌 ABS「Cloud Computing

條文	訂定說明
	Implementation Guide 2.0」第四章 Key controls recommended when entering into a cloud outsourcing arrangement； FCA「FG 16/5 Guidance for firms outsourcing to the ‘cloud’ and other third-party IT services」 Oversight of service provider；雲端安全聯盟（Cloud Security Alliance, CSA「Cloud Controls Matrix」 Human Resources （人力資源安全），以及「金融機構作業委外使用雲端服務自律規範」第四條第一項第五款之內容，明定各會員公司應定期舉辦或參加雲端服務相關的人才培訓，確保會員公司具備管理雲端技術風險、監督及審查雲端服務之知識及能力。 十一、 第四條第二項係依據 ABS「Cloud Computing Implementation Guide 2.0」與 FCA「FG 16/5 Guidance for firms outsourcing to the ‘cloud’ and other third-party IT services」 Oversight of service provider 以及「金融機構作業委外使用雲端服務自律規範」第四條第五項之內容，明定各會員公司使用雲端服務時與控管其風險事項應注意事項。 十二、 第四條第二項第一款係依據 CSA「Cloud Controls Matrix」Security Incident Management, E-Discovery, & Cloud Forensics（資安事件管理，數位取證與雲端鑑識）以及「金融機構作業委外使用雲端服務自律規範」第四條第五項第一款之內容，明定各會員公司採用雲端服務應具備定期審查制度，以確保各會員公司之管理策略及機制將持續更新。 十三、 第四條第二項第二款係依據「保險業作業委託他人處理應注意事項」第十八點第一項第六款第二目與「金融機構作業委外使用雲端服務自律規範」第四

條文	訂定說明
	條第五項第二款之內容，明定各會員公司如將作業項目委託至境外處理，應評估之事項及應採行風險控管措施。 十四、 第四條第二項第三款依據「保險業作業委託他人處理應注意事項」第十八點第一項第一款與「金融機構作業委外使用雲端服務自律規範」第四條第五項第三款之內容，明定各會員公司應注意作業委託雲端服務業者之適度分散，並應考慮該雲端業者無法提供服務時應採取的措施及該集中風險是否在其風險承受能力範圍內。又參照新加坡 ABS「Cloud Computing Implementation Guide 2.0」第四章 Key controls recommended when entering into a cloud outsourcing arrangement 採用多雲或其他分散策略時，雖可避免過度集中，但仍應與組織內部的技術、管理能力達到平衡。 十五、 第四條第二項第四款係依據 ABS「Cloud Computing Implementation Guide 2.0」第四章 Key controls recommended when entering into a cloud outsourcing arrangement 與「金融機構作業委外使用雲端服務自律規範」第四條第五項第四款之內容，明定各會員公司應依使用雲端服務之風險建立適當之監控機制，以健全業務持續性運作。 十六、 第四條第二項第五款係依據「保險業作業委託他人處理應注意事項」第七點第一項第三款與 ABS「Cloud Computing Implementation Guide 2.0」第四章 Key controls recommended when entering into a cloud outsourcing arrangement 與「金融機構作業委外使用雲端服務自律規範」第四條第五項第五款之內容，明定各會員公司於使用雲端

條文	訂定說明
	服務時，應考量雲端服務資料可用性與互通性要求。 十七、 第四條第三項係依據「保險業作業委託他人處理應注意事項」第四點第二項第一款與「金融機構作業委外使用雲端服務自律規範」第四條第四項之內容，明定董事會應確保各會員公司作業委外使用雲端服務之風險得到全面監督與審核，保障各會員公司之整體利益及提升治理水平，確保各會員公司能夠有效管理和應對各種風險。
第五條 各會員公司使用雲端服務時，應對雲端服務業者進行盡職調查及定期審查程序，並遵循下列事項： 一、應評估雲端服務業者之專業知識、經驗與資源、財務健全、內部控制、資安管理機制及符合法規要求。 二、以風險基礎方法決定其執行強度，評估項目宜包含： (一) 各會員公司是否保有其指定資料處理地及其儲存地之權利，以及雲端服務業者辦理受託作業之客戶資料處理地及其儲存地之司法管轄區，是否可能對各會員公司使用雲端服務造成其他營運風險。 (二) 雲端服務業者是否實施適當之資訊安全控管措施，如：威脅與弱點管理機制、雲端基礎架構及虛擬化設備安全管理程序。 (三) 雲端服務業者是否已建立資料銷毀、資料遺失和資料外洩通報管理機制。 (四) 雲端服務業者之服務水準、備援機制、資訊安全防護能力、資訊安全事件通報責任管理、業務持續運作與災難復原能力是否可符合各會員公	一、本條明定各會員公司使用雲端服務作業時應遵循之管理架構控管事項，包含雲端服務業者之盡職調查及其審查流程，與各會員公司監督及審查雲端服務之責任。 二、第五條第一項係依據「保險業作業委託他人處理應注意事項」第十六點、第十八點與「金融機構作業委外使用雲端服務自律規範」第五條第一項之內容，鑑於盡職調查為簽署委外契約前之關鍵任務，爰定義各會員公司對於業者盡職調查之要項。 三、第五條第一項第一款係依據「保險業作業委託他人處理應注意事項」第四點與「金融機構作業委外使用雲端服務自律規範」第五條第一項第一款之內容，明定各會員公司評估雲端服務業者之專業知識、經驗與資源、財務健全、內部控制、資安管理機制、及符合法規要求。 四、第五條第一項第二款第一目係依據「保險業作業委託他人處理應注意事項」第十六點與「金融機構作業委外使用雲端服務自律規範」第五條第一項第二款第一目之內容，明定各會員公司於盡職調查時應瞭解雲端服務業者實際辦理受託作業地點之司法管轄區，並評估是否會

條文	訂定說明
司需求。 (五) 雲端服務之互通性，確保於服務結束時，是否可將系統遷移或將資料遷出雲端服務。 (六) 雲端服務業者提供之資源與其他承租人所使用之資源是否有邏輯區隔。 (七) 雲端服務業者之安全性事件及系統日誌紀錄保存機制是否符合會員公司資訊安全之需求。 三、外國保險業在臺分支機構經由國外總機構或經其授權之區域總部複委託第三方提供雲端服務之情形，得援用其國外總機構或經其授權之區域總部負責統籌辦理並提供雲端服務業者之盡職調查及定期審查報告。 前項所提之評估項目，得要求雲端服務業者出具符合委外事項內容、範圍及性質的國際標準驗證報告，作為佐證資料。如國際標準組織之 ISO27001、ISO27017、ISO27018、ISO27701、ISO22301 、雲端安全聯盟（CSA）STAR 驗證或美國註冊會計師協會（AICPA）SOC 2 報告等。 各會員公司對使用雲端服務負有最終監督義務，應具有專業技術及資源負責辨識風險因子，監督及審查雲端服務，並宜以風險基礎方法和所採用之雲端服務模式決定其執行強度與頻率，必要時得視需要委託專業第三人以輔助其監督作業。 一、各會員公司應以風險基礎方法定期審查雲端服務作業委外契約或書面協議的執行情形，並依據風險、法令和業務變化評估其妥適性。 二、各會員公司除直接委託雲端服務業者外，如同意其受委託機構將雲端服務複委託予雲端服務業者時，應針對複委託情形，訂明複委託之範圍、限制或條件。	造成會員公司之營運風險。 五、第五條第一項第二款第二目係依據 ABS「Cloud Computing Implementation Guide 2.0」第三章 Activities recommended as part of due diligence 與「金融機構作業委外使用雲端服務自律規範」第五條第一項第二款第二目之內容，明定各會員公司應確認雲端服務業者已實施適當之資訊安全控管措施。 六、第五條第一項第二款第三目係依據 FCA「FG 16/5 Guidance for firms outsourcing to the 'cloud' and other third-party IT services」 Data security 與「金融機構作業委外使用雲端服務自律規範」第五條第一項第二款第三目之內容，明定各會員公司確保雲端服務業者是否已建立資料銷毀、資料遺失和資料外洩通報管理機制。 七、第五條第一項第二款第四目係依據「保險業作業委託他人處理應注意事項」第四點第三項、第十六點、第十八點之規定，並參酌 ABS「Cloud Computing Implementation Guide 2.0」第三章 Activities recommended as part of due diligence 以及「金融機構作業委外使用雲端服務自律規範」第五條第一項第二款第四目之內容，因雲端服務營運持續性及有效性需高度依賴雲端服務業者，且其於雲端服務之熟稔度及緊急應變能力將高度影響使用雲端服務之會員公司，故明定各會員公司針對雲端服務業者之災難復原及營運持續能力評估規範。 八、第五條第一項第二款第五目係依據 ABS「Cloud Computing Implementation Guide 2.0」第三章 Activities recommended as part of due diligence、EIOPA「Guidelines on outsourcing to cloud service providers 」

條文	訂定說明
三、各會員公司使用雲端服務涉及客戶資料之登錄、處理、輸出或儲存時，應確認雲端服務業者於辦理涉及提供雲端服務之設備更換或銷毀時，具備相關機制可確保資料遷移過程安全性及完整性，及汰換設備內之資料經刪除或銷毀。 四、各會員公司應定期確認雲端服務是否維持所需之服務水準並定期檢視服務水準報告。	Guideline 15、ISO 27002 #5.23、ISO 27017 #CLD.8.1.5 與「金融機構作業委外使用雲端服務自律規範」第五條第一項第二款第五目之內容，明定各會員公司應遵守之安全控管規定，以確保於服務結束時，是否可將系統遷移或將資料遷出雲端服務。 九、第五條第一項第二款第六目係依據「保險業作業委託他人處理應注意事項」第十七點與「金融機構作業委外使用雲端服務自律規範」第五條第一項第二款第六目之內容，明定各會員公司應確保雲端服務業者提供之資源與其他承租人所使用之資源是否有邏輯區隔。 十、第五條第一項第二款第七目係依據 CSA「Cloud Controls Matrix」Governance, Risk and Compliance（治理風險與法律遵循管理）、MAS「Guidelines on Outsourcing（Financial Institutions other than Banks）」5.6、ISO 27002 #5.23 以及「金融機構作業委外使用雲端服務自律規範」第五條第一項第二款第七目之內容，明定各會員公司應確保雲端服務業者之安全性事件及系統日誌紀錄保存機制是否符合會員公司資訊安全之需求。 十一、 第五條第一項第三款係依據「保險業作業委託他人處理應注意事項」第四點第二項第四款、第四點第三項與「金融機構作業委外使用雲端服務自律規範」第五條第一項第三款之內容，明定外國保險業在臺分支機構執行「保險業作業委託他人處理應注意事項」第四點第二項所規定之辦理事項時，得由總機構或經其授權之區域總部負責及辦理，故明定外國保險業在臺分支機構經由國外總機構或經其授權之區域總部複委託第三方提供雲端服務之情形，得援用其國外

條文	訂定說明
	總機構或經其授權之區域總部負責統籌辦理並提供雲端服務業者之盡職調查及定期審查報告。 十二、 第五條第二項要求係考量雲端服務業者應實施適當之資訊安全控管措施以確保受託作業之安全及對客戶資料之保護，爰明定保險業得要求雲端服務業者出具符合委外事項內容、範圍及性質的國際標準驗證報告，作為佐證資料。如國際標準組織之 ISO27001、ISO27017、ISO27018、ISO27701、ISO22301、雲端安全聯盟（CSA） STAR 驗證或美國註冊會計師協會 （AICPA） SOC 2 報告等。 十三、 第五條第三項係參照「保險業作業委託他人處理應注意事項」第九點第三項、第十六點第二項第六款、第十八點第一項第二款；CSA「Cloud Controls Matrix」 Supply Chain Management, Transparency, and Accountability（供應商管理、透明與可歸責性）與「金融機構作業委外使用雲端服務自律規範」第五條第三項之內容，明定各會員公司對所使用之雲端服務應負最終監督義務及相關應執行事項，包含各會員公司應監督及定期審查服務執行情形、確認服務水準報告與操作紀錄等。
第六條 各會員公司作業委外使用雲端服務應與雲端服務業者達成服務使用契約或協議，其內容除依「保險業作業委託他人處理應注意事項」第九點及第十六點規定外，應涵蓋下列事項： 一、委外事項範圍及雲端服務業者之權責，應包括各會員公司與雲端服務業者間之責任區分及雲端服務水準。 二、雲端服務業者提供的資料備份機制及資料刪除機制。	一、本條明定各會員公司應與雲端服務業者達成服務使用契約或協議，以及其內容宜涵蓋之事項。 二、第六條第一項係參照「保險業作業委託他人處理應注意事項」第九點第一項第一款、第六款、第七款、第八款、第十一款；第十六點第二項第六款；第十八點第一項第五款與「金融機構作業委外使用雲端服務自律規範」第五條第二項第一款之內容，明定契約或協議內容應確認涵蓋或符合之事項。

條文	訂定說明
三、客戶資料保密及安全措施，應包括各會員公司存放於雲端資料所有權，以及雲端服務業者向第三方揭露資料之限制。 四、與雲端服務業者終止委外契約之重大事由，應包括服務終止之資料處理責任。 五、雲端服務業者就受託事項範圍，同意各會員公司、主管機關或其指定之人查核之要求。 六、雲端服務業者針對受託事項若有重大異常或缺失應立即通知各會員公司，包括對於影響各會員公司之資訊安全事件通報責任。 七、如涉及自然人客戶相關資料之重大性業務資訊系統委託至境外處理，應包括委外作業移轉至其他雲端服務業者或移回各會員公司之情況，原雲端服務業者有關系統遷移、資料處理之義務，及雲端服務業者服務中斷之賠償責任。 前揭契約或協議內容如無法符合本條第一項要求，應採取適當評估，並依風險規劃替代措施，以確保各會員公司對雲端服務業者之最終監督義務之執行。 外國保險業在臺分支機構經由國外總機構或經其授權之區域總部複委託第三方提供雲端服務之情形，得由國外總機構或經其授權之區域總部負責統籌協議約定事宜，且服務使用協議應符合本條第一項及第二項之要求。	三、第六條第一項第一款係依據 CSA「Cloud Controls Matrix」 Supply Chain Management, Transparency, and Accountability（供應商管理、透明與可歸責性）以及「金融機構作業委外使用雲端服務自律規範」第五條第二項第一款第一目之內容，明定服務使用契約或協議應包含委外事項範圍及雲端服務業者之權責。 四、第六條第一項第二款係依據 EIOPA「Guidelines on outsourcing to cloud service providers」Guideline 10，以及 FCA「FG 16/5 Guidance for firms outsourcing to the 'cloud' and other third-party IT services」 Exit plan，明定各會員公司應確保契約中載明，雲端服務業者提供的資料備份機制及資料刪除機制。 五、第六條第一項第三款係依據「保險業作業委託他人處理應注意事項」第十八點第一項第四款、第五款與「金融機構作業委外使用雲端服務自律規範」第五條第二項第一款第二目之內容，明定各會員公司應確保契約中載明客戶資料保密及安全措施。 六、第六條第一項第四款係依據「保險業作業委託他人處理應注意事項」第十六點第二項第六款與「金融機構作業委外使用雲端服務自律規範」第五條第二項第一款第三目之內容，明定契約內容應載明服務終止後雲端服務業者的資料處理責任。 七、第六條第一項第五款係依據「保險業作業委託他人處理應注意事項」第九點第一項第七款規定與「金融機構作業委外使用雲端服務自律規範」第五條第二項第一款第四目之內容，明定雲端服務業者就受託事項範圍，同意各會員公司、主

條文	訂定說明
	管機關或其指定之人查核之要求。 八、第六條第一項第六款係依據「保險業作業委託他人處理應注意事項」第九點第一項第十一款與「金融機構作業委外使用雲端服務自律規範」第五條第二項第一款第五目之內容，明定雲端服務業者對委外事項若有重大異常或缺失應立即通知各會員公司。 九、第六條第一項第七款係依據「保險業作業委託他人處理應注意事項」第十二點第二項第六款與「金融機構作業委外使用雲端服務自律規範」第五條第二項第一款第六目之內容，明定各會員公司應確保契約中載明於委外作業移轉至其他受委託機構或移回各會員公司之情況。 十、第六條第二項係依據「保險業作業委託他人處理應注意事項」第十八點第一項第二款與「金融機構作業委外使用雲端服務自律規範」第五條第二項第二款之內容，明定各會員公司對契約或協議內容評估及監督之責任。 十一、第六條第三項係依據「保險業作業委託他人處理應注意事項」第四點第二項、第三項之規定與「金融機構作業委外使用雲端服務自律規範」第五條第二項第三款之內容，明定外國保險業在臺分支機構執行「保險業作業委託他人處理應注意事項」第四點第二項所規定之辦理事項時，得由總機構或經其授權之區域總部負責及辦理，爰明定外國保險業在臺分支機構經由國外總機構或經其授權之區域總部複委託第三方提供雲端服務之情形，得由國外總機構或經其授權之區域總部負責統籌協議約定事宜。
第七條 各會員公司應依風險基礎方法規劃適當之資安控管機制及建立相關程序，並考量下	一、本條明定各會員公司於使用雲端服務作業時應遵循之資安控管事項，包含雲端環境之安全控管、身分識別管理、資料

條文	訂定說明
列事項： 一、雲端環境之安全控管 (一)如採用虛擬機和容器之映像檔進行部署，應建立映像檔管理機制，以確保其完整性及安全性。 (二)應控管雲端環境與地端環境之間的連線，並使用加密通訊協定或專線。 (三)應依雲端服務之正式及非正式區進行適當區隔。 (四)應定期評估雲端服務之基礎架構安全管理機制。 二、身分識別管理 (一)應依最小權限原則及職責分離原則管理雲端系統及機敏資訊之存取權限。 (二)使用特權帳號應採取適當控管機制（如多因子身分驗證或特權帳號管理系統），並定期辦理帳號清查。 (三)如開放透過網際網路直接存取雲端服務者，應建立身分識別與存取控制等安全控制措施。 三、資料傳輸及儲存之加密管理 (一)傳輸及儲存客戶資料至雲端環境者，應採行資料加密或代碼化等有效保護措施。 (二)宜依據雲端服務之使用目的實施存取控制措施。 (三)會員公司對於雲端服務業者處理之資料應保有完整所有權，除執行指定作業或經會員公司同意之作業外，應確保雲端服務業者不得有存取客戶資料之權限，不得為指定範圍以外之利用，並遵守資料保密的相關法規要求。 四、金鑰管理機制 (一)應根據資料的分類、相關風險及加密技術的可用性，使用安全且合適的加	傳輸及儲存之加密管理、金鑰管理機制等。 二、本條領域之拆分方式係參照雲端安全聯盟(Cloud Security Alliance, CSA)「Cloud Controls Matrix」之架構，各會員公司應依風險基礎方法和所使用的雲端服務模式規劃資安控管機制。 三、第七條第一項第一款係依據ABS「Cloud Computing Implementation Guide 2.0」第四章 Key controls recommended when entering into a cloud outsourcing arrangement、CSA「Cloud Controls Matrix」Infrastructure & Virtualization Security(基礎架構與虛擬化安全)與「金融機構作業委外使用雲端服務自律規範」第七條第一項第五款之內容，明定各會員公司應遵守之安全控管規定，以確保雲端服務之安全性與可用性。 四、透過網段區隔可以有效地提高系統的安全性、效能和管理性，依據ABS「Cloud Computing Implementation Guide 2.0」第四章 Key controls recommended when entering into a cloud outsourcing arrangement，於第七條第一項第一款第三目明定應在正式及非正式區之間實施網段區隔，可確保隔離不同環境之間的資源和資料，防止非正式環境的事件對正式環境造成影響。 五、各會員公司使用雲端服務時負有保護其基礎架構安全之責任，且基礎架構安全為保障雲端服務基本安全之關鍵，依據ABS「Cloud Computing Implementation Guide 2.0」第四章 Key controls recommended when entering into a cloud outsourcing arrangement與FFIEC IT Examination Handbook，於第七條第一項第一款第四目明定應定期評估雲端服務

條文	訂定說明
密演算法。 (二)應區隔加密金鑰儲存位置並設置適當存取安全控管措施。 五、若涉及自行管理之雲端環境（如採用IaaS 或 PaaS 雲端服務模式者），除前述一到四款管控，應再考量下列事項： (一)稽核軌跡與監控： 1. 應留存會員公司對於雲端服務平台操作之稽核軌跡，宜考量集中管理稽核軌跡與監控資料，及避免稽核軌跡留存未加密之客戶資料。 2. 宜針對雲端安全事件場景制定監控規則，將相關事件日誌納入資訊安全事件之監控管理機制範圍，以及早發現潛在資安風險。 3. 如各會員公司之雲端服務係採與其地端資訊環境介接之雲地混合模式，宜考量雲地間邊際防護，並建立日誌與監控分析相關機制。 (二)威脅與弱點管理： 1. 應定期執行系統弱點掃描，依掃描結果進行修補，或完成補償性控制措施，並記錄處理情形及追蹤改善。 2. 應持續關注雲端服務相關威脅與弱點，評估相關威脅與弱點對各會員公司之影響。 (三)變更管理與組態安全： 1. 應規劃雲端服務變更管理機制，並留存變更紀錄。 2. 應依據雲端環境、運作效能、資訊安全等面向規劃合適之組態並進行管理與監控。	之基礎架構安全管理機制。 六、 應控管使用者對雲端資源及機敏資訊的存取方式，並確保使用者僅擁有必要的權限來存取資源及機敏資訊，以防止未經授權的存取，依據 ABS「Cloud Computing Implementation Guide 2.0」第四章 Key controls recommended when entering into a cloud outsourcing arrangement、CSA「Cloud Controls Matrix」Identity & Access Management（身份與存取控制）與「金融機構作業委外使用雲端服務自律規範」第七條第一項第三款之內容，於第七條第一項第二款明定各會員公司應遵循之身分識別管理規範。 七、 各會員公司於雲端環境處理、儲存、傳輸與使用資料時，應實施資料存取控制措施，並遵守相關法令之要求，依據 ABS「Cloud Computing Implementation Guide 2.0」第四章 Key controls recommended when entering into a cloud outsourcing arrangement、CSA「Cloud Controls Matrix」Data Security and Privacy Lifecycle Management（資料安全和隱私生命週期管理）、保險業運用新興科技作業原則第貳條第七項與「金融機構作業委外使用雲端服務自律規範」第七條第一項第一款與第二款之內容，於第七條第一項第三款明定各會員公司使用雲端服務時，應遵守之資料傳輸及儲存之加密管理要求。 八、 第七條第一項第三款第一目係依據「保險業作業委託他人處理應注意事項」第十八點第一項第四款要求訂定。 九、 第七條第一項第三款第三目係依據「保險業作業委託他人處理應注意事項」第十八點第一項第五款要求訂定。

條文	訂定說明
	十、 第七條第一項第四款係依據 ABS「Cloud Computing Implementation Guide 2.0」第四章 Key controls recommended when entering into a cloud outsourcing arrangement 、 CSA 「 Cloud Controls Matrix」Cryptography, Encryption & Key Management（密碼學、加密和金鑰管理）、保險業運用新興科技作業原則第貳條第七項與「金融機構作業委外使用雲端服務自律規範」第七條第一項第一款之內容，明定各會員公司使用雲端服務時，應制定金鑰管理機制，加密演算法之選擇應基於資料的保密性需求以及相應的安全性考量，採用主管機關認可之加密演算法或被廣泛認可之加密標準。 十一、 應注意加密金鑰存放之安全，考量與加密或代碼化工具分開儲存，參照 ABS「 Cloud Computing Implementation Guide 2.0 」第四章 Key controls recommended when entering into a cloud outsourcing arrangement，於第七條第一項第四款第二目明定加密金鑰應區隔儲存並設置適當存取安全控管。 十二、 第七條第一項第五款第一目係參照 ABS「Cloud Computing Implementation Guide 2.0 」第四章 Key controls recommended when entering into a cloud outsourcing arrangement、CSA「Cloud Controls Matrix」Logging and Monitoring（記錄與監控）、保險業辦理資訊安全防護自律規範第十七條與「金融機構作業委外使用雲端服務自律規範」第七條第一項第四款之內容，明定各會員公司採用 IaaS 或 PaaS 雲端服務模式時，應監控雲端環境並管理稽核軌跡。 十三、 為確保各會員公司及時發現雲端環境中之弱點及漏洞，並針對不同風險訂定

條文	訂定說明
	適當措施及追蹤改善，依據 ABS「Cloud Computing Implementation Guide 2.0」第四章 Key controls recommended when entering into a cloud outsourcing arrangement 、 CSA 「 Cloud Controls Matrix 」 Threat & Vulnerability Management（威脅與弱點管理）、保險業辦理資訊安全防護自律規範第十四條與「金融機構作業委外使用雲端服務自律規範」第七條第一項第六款之內容，於第七條第一項第五款第二目明定採用 IaaS 或 PaaS 雲端服務模式時，應遵守之威脅與弱點管理要求。 十四、 各會員公司可以根據雲端服務之特性和運作效能對雲端環境進行調整，確保系統效能達到最佳狀態，從而提高服務可靠性，依據 ABS「Cloud Computing Implementation Guide 2.0」第四章 Key controls recommended when entering into a cloud outsourcing arrangement、CSA「Cloud Controls Matrix」Change Control and Configuration Management（變更管理和設定管理）與「金融機構作業委外使用雲端服務自律規範」第七條第一項第七款之內容，於七條第一項第五款第三目明定採用 IaaS 或 PaaS 雲端服務模式時，應規劃雲端服務變更管理機制並對組態進行管理。
第八條 各會員公司應定期執行人力培訓與人力提升規劃，以確保具備足夠之專業知識與資源。相關內容包含： 一、專責單位應依據使用雲端服務之範圍，規劃適當人力與資源，以確保組織擁有足夠之資源進行雲端服務維運與管理，並能以風險為基礎方法做出適當之決策與監督。	一、本條明定各會員公司應定期執行人力培訓與人力提升規劃並定期檢視。 二、依據「保險業作業委託他人處理應注意事項」第七點第一項第二款、 ISO 27002 #5.23 以及「金融機構作業委外使用雲端服務自律規範」第六條之內容，各會員公司對於雲端服務應具備足夠之專業知識與資源，故於第八條明定人力培訓之相關規範。

條文	訂定說明
二、依據涉及雲端服務之人員角色權責，規劃適當教育訓練並提供必要之資源（包含資訊安全、風險認知和雲端知識技能等內容），以提升相關人員對於雲端服務導入、使用以及監控等面向的管理能力。 三、應檢視人力培訓之規劃及機制，以維持教育訓練的有效性。	三、第八條第一項第一款係依據美國聯邦金融機構檢查委員會（Federal Financial Institutions Examination Council，FFIEC）IT Examination Handbook「Management」以及「金融機構作業委外使用雲端服務自律規範」第六條第一項第一款之內容，明定各會員公司應依據使用雲端服務之範圍，規劃適當人力與資源。 四、第八條第一項第二款係依據 ABS「Cloud Computing Implementation Guide 2.0」第四章 Key controls recommended when entering into a cloud outsourcing arrangement、CSA「Cloud Controls Matrix」Human Resources（人力資源）以及「金融機構作業委外使用雲端服務自律規範」第六條第一項第二款之內容，明定依據人員角色權責，規劃適當教育訓練。 五、第八條第一項第三款係依據 FFIEC IT Examination Handbook 「Architecture, Infrastructure, and Operations 」以及「金融機構作業委外使用雲端服務自律規範」第六條第一項第三款之內容，明定會員公司應定期檢視人力培訓之規劃及機制。
第九條 各會員公司應針對雲端服務業者規劃雲端服務查核作業。相關內容包含： 一、查核頻率 (一)雲端服務涉及自然人客戶相關資料之重大性業務資訊系統委託至境外處理時，每年至少應辦理一次一般性查核及一次專案查核。 (二)辦理非屬上述類型之雲端服務委外事項時，應依據風險基礎方法規劃與調整查核頻率。 二、得委託具資訊專業之獨立第三人協助進行查核，並應評估獨立第三人之適格性，	一、本條明定各會員公司應規劃雲端服務查核作業。 二、依據「保險業作業委託他人處理應注意事項」第十八點第一項第三款與「金融機構作業委外使用雲端服務自律規範」第八條之內容，各會員公司應對雲端服務業者進行查核，並參照 ABS「Cloud Computing Implementation Guide 2.0」第三章 Activities recommended as part of due diligence 、CSA 「Cloud Controls Matrix」Audit & Assurance（稽核確保）與新加坡金融管理局(Monetary Authority of Singapore, MAS ）「Guidelines on

條文	訂定說明
評估內容包含執行查核所需的專業知識、專業技能與獨立性。 三、針對查核時所發現的缺失項目，應追蹤改善情況並依實際情況採取合適的補償性措施。 四、對具重大性之雲端服務委外事項執行查核時，其執行重點宜包含： (一)確認雲端服務作業內容執行之妥適性，與是否符合本國相關規範及國際資訊安全標準。 (二)評估資料中心實體安全控制之充足性。 (三)雲端服務業者之營運持續性控制措施。 (四)雲端服務業者處理作業相關之重要系統及控制環節。 (五)盡職調查過程中雲端服務業者所提供之報告內容。 (六)雲端平台資料刪除與災難復原流程。 外國保險業在臺分支機構得交由國外總機構或經其授權之區域總部稽核單位辦理，相關單位並應提供相關雲端查核報告予該外國保險業在臺分支機構。	Outsourcing （Financial Institutions other than Banks）」5.2、5.8、5.12，於第九條明定查核之相關規範。 三、「保險業作業委託他人處理應注意事項」第十六點第二項第四款已明定，當雲端服務涉及自然人客戶相關資料之重大性業務資訊系統委託至境外處理時，每年至少應辦理一次一般性查核及一次專案查核，而針對非屬上述類型之雲端服務委外事項，於本自律規範第九條第一項第一款第二目中明定會員公司應依風險基礎方法自行規劃與調整查核頻率。 四、依據「保險業作業委託他人處理應注意事項」第十八點第一項第三款，保險業得自行委託，或與委託同一雲端服務業者之其他保險業聯合委託具資訊專業之獨立第三人查核，並應評估第三人之適格性，又參照 ABS「Cloud Computing Implementation Guide 2.0」第三章 Activities recommended as part of due diligence 以及「金融機構作業委外使用雲端服務自律規範」第八條第二項之內容，於第九條第一項第二款明定對獨立第三人之評估項目。 五、第九條第一項第三款係依據 ABS「Cloud Computing Implementation Guide 2.0」第三章 Activities recommended as part of due diligence 以及「金融機構作業委外使用雲端服務自律規範」第八條第四項之內容，明定追蹤與改善查核缺失並依實際情況採取合適的補償性措施。 六、第九條第一項第四款係依據 ABS「Cloud Computing Implementation Guide 2.0」第四章 Key controls recommended when entering into a cloud outsourcing arrangement 、 MAS 「 Guidelines on Outsourcing （Financial Institutions other

條文	訂定說明
	than Banks）」5.4、5.7、歐洲保險和職業養老金管理局（European Insurance and Occupational Pensions Authority , EIOPA）「Guidelines on outsourcing to cloud service providers」Guideline 10 以及「金融機構作業委外使用雲端服務自律規範」第八條第三項之內容，明定各會員公司對具重大性之雲端服務委外事項執行查核時可參考的執行重點。 七、第九條第二項係依據「保險業作業委託他人處理應注意事項」第十七點第一項第四款與「金融機構作業委外使用雲端服務自律規範」第八條第五項之內容訂定。
第十條 各會員公司應將下列要求納入業務持續性管理機制： 一、應針對涉及雲端服務使用之資訊系統辦理營運衝擊分析，評估雲端服務之韌性及復原能力。 二、依據風險基礎方法考量雲端服務之重要性，規劃適當之營運持續管理機制。 三、規劃雲端服務事件管理與應變流程，包含重大風險事件的發現與通報、緊急應變處理、以及事件管理等程序，並載明與雲端服務業者之權責劃分。 四、辦理具重大性之雲端服務委外事項時，應依據風險基礎方法決定執行測試或演練的頻率、情境以及範圍。 五、建立雲端資料備份機制，並留存備份清冊，備份媒體或檔案應妥善防護，確保資料可用性及防止未授權存取。 六、於使用雲端服務前，規劃終止雲端服務委託之移轉機制。相關內容包含： (一)規劃合適之雲端服務移轉方式，可選擇將系統與資料移轉回會員公司或移轉至其他雲端服務業者等。	一、本條明定業務持續性管理機制之相關規範。 二、各會員公司使用雲端服務時，應了解其對既有資訊系統與業務產生之影響，並分配所需資源，依據 FFIEC IT Examination Handbook、ABS「Cloud Computing Implementation Guide 2.0」第三章 Activities recommended as part of due diligence 以及「金融機構作業委外使用雲端服務自律規範」第九條第一項第一款之內容，於第十條第一項第一款明定針對涉及雲端服務使用之資訊系統辦理營運衝擊分析。 三、營運持續管理機制可確保各會員公司在面對自然災害、技術故障或其他意外事件時，能不受影響並維持營運，依據 ABS「Cloud Computing Implementation Guide 2.0」第三章 Activities recommended as part of due diligence、CSA「Cloud Controls Matrix」Business Continuity Management and Operational Resilience（營運持續管理與營運彈性）、MAS「Guidelines on Outsourcing（Financial Institutions other

條文	訂定說明
(二)會員公司應確保雲端服務契約終止或系統移轉時，刪除留存於雲端服務之資料，並留存刪除或銷毀之紀錄。	than Banks）」5.7、EIOPA「Guidelines on outsourcing to cloud service providers」Guideline 7 以及「金融機構作業委外使用雲端服務自律規範」第九條第一項第二款之內容，於第十條第一項第二款明定應依據風險基礎方法規畫適當之營運持續管理機制。 四、雲端服務事件管理與應變流程可有效解決雲端服務事件並減少對各會員公司營運的影響，依據 ABS「Cloud Computing Implementation Guide 2.0」第四章 Key controls recommended when entering into a cloud outsourcing arrangement、CSA「Cloud Controls Matrix」Security Incident Management, E-Discovery, & Cloud Forensics（資安事件管理，數位取證與雲端鑑識）、MAS「Guidelines on Outsourcing（Financial Institutions other than Banks）」4.2、ISO 27002 #5.23 以及「金融機構作業委外使用雲端服務自律規範」第九條第二項之內容，於第十條第一項第三款明定各會員公司應規劃雲端服務事件管理與應變流程，且考量到雲端服務的特性，各會員公司還需載明與雲端服務業者之權責劃分，使雙方於事件發生時可有效合作並迅速處理。 五、依據「保險業作業委託他人處理應注意事項」第七點第一項第二款第五目，各會員公司辦理具重大性之委外事項依風險情境進行定期或不定期測試或演練，又參照 ABS「Cloud Computing Implementation Guide 2.0」第四章 Key controls recommended when entering into a cloud outsourcing arrangement、CSA「Cloud Controls Matrix」Business Continuity Management and Operational Resilience（營運持續管理與營運彈性）、

條文	訂定說明
	ISO 27018 #A.11.3 以及「金融機構作業委外使用雲端服務自律規範」第九條第一項第四款之內容，於第十條第一條第四款明定依據風險基礎方法決定執行測試或演練的頻率、情境以及範圍。 六、資料備份機制可在發生系統故障或被惡意破壞時，有效防止資料損失並迅速恢復資料以維持營運，依據 ABS「Cloud Computing Implementation Guide 2.0」第三章 Activities recommended as part of due diligence、第四章 Key controls recommended when entering into a cloud outsourcing arrangement；CSA「Cloud Controls Matrix」Business Continuity Management and Operational Resilience（營運持續管理與營運彈性）；EIOPA「Guidelines on outsourcing to cloud service providers」Guideline 8、12 以及「金融機構作業委外使用雲端服務自律規範」第九條第一項第三款之內容，於第十條第一條第五款明定會員公司應建立雲端資料備份機制。 七、依據「保險業作業委託他人處理應注意事項」第七點第一項第三款，各會員公司應訂定緊急應變計畫及終止委託之移轉機制，又參照 ABS「Cloud Computing Implementation Guide 2.0」第三章 Activities recommended as part of due diligence、CSA「Cloud Controls Matrix」Interoperability & Portability（互通性及可移植性）、MAS「Guidelines on Outsourcing（Financial Institutions other than Banks）」5.7、EIOPA「Guidelines on outsourcing to cloud service providers」Guideline 15、ISO 27002 #5.23、ISO 27017 #CLD.8.1.5、保險業運用新興科技作業原則第貳條第十一項以及「金融機構作業

條文	訂定說明
	委外使用雲端服務自律規範」第九條第三項之內容，於第十條第一條第六款明定會員公司應規劃終止雲端服務委託之移轉機制的相關規範。
第十一條 各會員公司應將本自律規範內容，納入內部控制及內部稽核制度中，並定期辦理查核。	本條明定本自律規範應納入各會員公司之內部控制及內部稽核制度中。
第十二條 各會員公司如有違反本自律規範之情事，經查證屬實且違反情節較輕者，得先予書面糾正；如情節較重大者，提報經各所屬公會理事會通過後，處以新台幣伍萬元以上，貳拾萬元以下之罰款。	本條明定各會員公司如違反本自律規範之罰則。
第十三條 本自律規範由中華民國人壽保險商業同業公會與中華民國產物保險商業同業公會共同訂定，經各該公會理事會決議通過報主管機關備查後施行，修正時亦同。	本條明定本自律規範之核定層級。