「保險業作業委外使用雲端服務自律規範」條文修訂對照表

金融監督管理委員會民國 115 年 6 月 12 日金管保壽字第 1150416699 號同意備查

修正條文	現行條文	說明
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內部作業制度及程序辦法」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。	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。	因「保險業作業委託他人處理應注意事項」於 2026 年 1 月 2 日廢止，及「保險業作業委託他人處理內部作業制度及程序辦法」自 2025 年 12 月 31 日起施行，爰修正本自律規範所援引之法規依據。
第二條 本規範適用之範圍，以保險業依「保險業作業委託他人處理內部作業制度及程序辦法」將作業委託他人處理，並涉及使用雲端服務為限。除本規範另有訂定外，會員公司應按「保險業作業委託他人處理內部作業制度及程序辦法」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	第二條 本規範適用之範圍，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	因「保險業作業委託他人處理應注意事項」於 2026 年 1 月 2 日廢止，及「保險業作業委託他人處理內部作業制度及程序辦法」自 2025 年 12 月 31 日起施行，爰修正本自律規範所援引之法規依據。

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。	機制，充分掌握在臺作業雲端委外事項之控管情形。	
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）。 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	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）。 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	本條內容無調整。

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	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。	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	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	本條內容無調整。

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	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。	對於控管雲端服務風險事項具備充足之資源、專業及權限。	
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	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	本條內容無調整。

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	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。 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。	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。 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。	
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	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	因「保險業作業委託他人處理應注意事項」於 2026 年 1 月 2 日廢止，及「保險業作業委託他人處理內部作業制度及程序辦法」

議，其內容除依「保險業作業委託他人處理內部作業制度及程序辦法」第九條及第十六條規定外，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。 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。	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。 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。	自 2025 年 12 月 31 日起施行，爰修正本自律規範所援引之法規依據。

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。	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。	
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	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	本條內容無調整。

(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密演算法。	(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	(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。	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。	
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。 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。	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。 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。	本條內容無調整。
第九條	第九條	本條內容無調整。

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,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	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,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。	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。	
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	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	本條內容無調整。

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。 (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。	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。 (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。	
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。	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。	本條內容無調整。
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。	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。	本條內容無調整。
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。	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。	本條內容無調整。