金融機構作業委外使用雲端服務自律規範總說明

本會113年4月25日第14屆第15次理監事聯席會議通過
金管會 113 年 7 月 4 日金管銀外字第 1130138523 號函修正後洽悉

因應金融機構運用導入雲端運算、雲端儲存等新興技術的多樣化，以提升數位轉型及金融服務敏捷彈性。爰依金融監督管理委員會（以下稱金管會）「金融資安行動方案」要求，強化金融機構建構完整風險管理及控管程序等，訂定「金融機構作業委外使用雲端服務自律規範」（以下稱「本規範」），以提升金融機構使用雲端服務管控措施。

本規範參酌金管會「金融機構作業委託他人處理內部作業制度及程序辦法」、中華民國銀行商業同業公會全國聯合會「金融機構資通安全防護基準」、新加坡ABS「Cloud Computing Implementation Guide 2.0」、新加坡金融管理局 MAS「Advisory on Addressing the Technology and Cyber Security Risks Associated with Public Cloud Adoption」與「TRM Guideline」、美國聯邦金融機構檢查委員會（FFIEC）「Security in a Cloud Computing Environment」、美國網路安全暨基礎設施安全局（CISA）「Cloud Security Technical Reference Architecture」、美國財政部「The Financial Services Sector's Adoption of Cloud Services」日本金融業資訊系統中心（FISC）「Security Guidelines on Computer Systems for Banking and Related Financial Institutions」、日本經濟產業省「雲端服務使用資訊安全管理指南」、香港金融管理局（HKMA）「Guidance on Cloud Computing」、香港政府資訊科技總監辦公室「雲端運算保安實務指引」與「採購雲端服務的實務指南」、雲端安全聯盟「Cloud Control Metrix」與德國「Cloud Computing Compliance Controls Catalog」等國際法令規範等，爰經參考各國作法，擬具本規範，以維護金融機構使用雲端服務之資訊安全。

本規範共十條，其要點如下：

一、 說明本規範之立法意旨。（第一條）
二、 說明本規範之適用範圍。（第二條）
三、 明訂本規範提及之名詞解釋。（第三條）
四、 明訂治理政策及風險管理。（第四條）
五、 明訂管理架構。（第五條）
六、 明訂人才培訓要求。（第六條）
七、 明訂資安控管要求。（第七條）
八、 明訂雲端服務查核要求。（第八條）
九、 明訂業務持續性管理要求。（第九條）
十、 說明本規範之核可實施。（第十條）

金融機構作業委外使用雲端服務自律規範	
條　文	說　明
第一條 中華民國銀行商業同業公會全國聯合會(以下稱本會)為確保金融機構依「金融機構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，並依風險基礎方法實施雲端委外治理機制及風險管理措施，以達成妥適使用雲端服務之目標，特訂定本規範。	說明本規範訂定目的與立法意旨。
第二條 本規範適用之金融機構，包括本國銀行（不含其國外分行)、外國銀行在臺分（子）行。 本規範適用之範圍，以金融機構對於涉及營業執照所載業務項目或客戶資訊之相關作業委外，並涉及使用雲端服務為限。除本規範另有訂定外，金融機構應按「金融機構作業委託他人處理內部作業制度及程序辦法」辦理。 提供電子銀行服務者，應符合本會制定之「金融機構辦理電子銀行業務安全控管作業基準」規定。 外國銀行在臺分(子)行辦理作業委外涉及雲端服務，如係透過總（母）行、集團或區域總部辦理者，可依總（母)行所訂管控措施辦理，惟須不低於本自律規範之規定，外國銀行在臺分(子)行仍應就其在臺業務建立妥適內部控制制度及風險管理機制，充分掌握對在臺作業雲端委外事項之控管情形。	一、說明本規範訂定適用範圍。 二、第二條第二項爰參照「金融機構作業委託他人處理內部作業制度及程序辦法」明定適用對象，金融機構辦理作業委外涉及使用雲端服務應遵循「金融機構作業委託他人處理內部作業制度及程序辦法」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、第二條第三項爰依據「金融機構運用新興科技作業規範」第二條第十五款規定，提供電子銀行服務者，應符合本會制定之「金融機構辦理電子銀行業務安全控管作業基準」規定。 四、第二條第四項爰參考「銀行防制洗錢及打擊資恐注意事項範本」，並依據外國銀行運作實務擬訂外國銀行在臺分支機構適用範圍。
第三條 本規範用詞定義如下:	一、第三條第一項第一款係參照「金融機構運用新興科技作業規範」

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。 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）：金融機構應確認、評估及瞭解其使用雲端服務之風險，採取適當控制措施，以有效降低此類風險。依該方法，金融機構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，並以適當且有效之方法，降低經其確認之使用雲端服務風險。 四、互通性：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金融機構。	第二條第一項第二款及國家資通安全研究院定義明定雲端服務之定義。 二、第三條第一項第二款係參照「金融機構作業委託他人處理內部作業制度及程序辦法」第十九條所採用之名稱，並參照新加坡銀行公會（The Association of Banks in Singapore, ABS）與香港金融管理局（Hong Kong Monetary Authority, HKMA）明定雲端服務業者之定義。 三、第三條第一項第三款係依據「金融機構防制洗錢辦法」第二條第一項第九款之明定風險基礎方法之定義。 四、第三條第一項第四款係參酌「金融機構作業委託他人處理內部作業制度及程序辦法」第十八條第二項第六款用字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。
第四條 金融機構作業委外使用雲端服務應建立使用雲端服務治理制度，規劃並確認以下事項： 一、應制訂雲端服務管理政策，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，以評估使用雲端服務之潛在風險。	一、本條爰依據訂明金融機構於使用雲端服務作業時應規劃及注意之治理制度與風險管理事項，包含董事會及專責單位權責、風險管理、委外管理及雲端管理策略。 二、鑑於金融機構使用雲端服務時應設立完善之治理制度並實施相關管理機制，參酌新加坡 TRM Guideline 等規範，於第四條第一項明訂金融機構於使用雲端服務時應規劃事項。

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、定期舉辦或參加雲端人才培訓，以確保金融機構具備管理雲端技術風險之知識與能力。 六、以風險基礎方法實施資訊安全控管要求。 七、建立雲端服務查核及業務持續性管理要求。 前項第二款之專責單位應包含雲端財務、成本或資源管理之角色。 第一項第三款所稱風險評估機制係指金融機構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，評估項目可包含： 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、金融機構對於雲端服務可用性與互通性之要求； 四、金融機構對於雲端服務之管理能力與經驗。 董事會應認知及監督金融機構作業委外使用雲端服務之風險，確保金融機構對於控管雲端服務風險事項具備充足之資源、專業及權限。外國銀行在臺分行，得由總機構或經其授權之區域總部負責及辦理。 金融機構使用雲端服務與控管其風險事項應注意以下事項： 一、金融機構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、金融機構如將作業項目委託	三、第四條第一項第一款係依據「金融機構運用新興科技作業規範」第二條第一項第四款要求訂定。 四、第四條第一項第二款專責單位為總經理或更高層級所指定之單位，依據「金融機構作業委託他人處理內部作業制度及程序辦法」第四條第二項第二款要求內部作業規範應載明專責單位及相關單位對委外事項控管之權責分工，爰於第四條第一項第二款明訂為金融機構應建立專責單位及相關單位之分工。 五、第四條第一項第三款、第四條第三項爰依據「金融機構作業委託他人處理內部作業制度及程序辦法」第四條規定。 六、第四條第二項爰參照美國 FFIEC IT Examination Handbook 及新加坡 ABS Cloud Computing Implementation Guide 2.0，說明專責單位應包含雲端財務、成本或資源管理之角色。 七、為確保金融體系之穩定性，透過建立風險管理機制確保金融機構識別和評估使用雲端服務之潛在風險，第四條第三項爰依據新加坡 ABS Cloud Computing Implementation Guide 2.0 說明金融機構應具備風險評估機制，採取風險基礎方法。 八、為保障組織整體利益及提升治理水平，確保金融機構能夠有效管理和應對各種風險，第四條第四項爰依據「金融機構作業委託他人處理內部作業制度及程序辦法」第四條第二項第一款訂定董事會應確保金融機構作業委外使

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，金融機構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、金融機構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、金融機構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。	用雲端服務之風險得到全面監督與審核。 九、為完善金融機構採用雲端服務之管理策略，參酌美國 FFIEC Security in a Cloud Computing Environment、香港 Guidance on Cloud Computing、香港雲端運算保安實務指引及 FISC Security Guidelines on Computer Systems for Banking and Related Financial Institutions、英國 FG16/5: Guidance for firms outsourcing to the cloud and other third party IT services 及新加坡 ABS Cloud Computing Implementation Guide 2.0，爰於第四條第五項各款明訂金融機構於使用雲端服務時，風險控管應注意事項。 十、第四條第五項第二款係依據「金融機構作業委託他人處理內部作業制度及程序辦法」第十九條第一項第六款第二目、「金融機構運用新興科技作業規範」第二條第一項第十一款及「金融機構作業委託他人處理內部作業制度及程序辦法相關問題適用解說問答集（委外問答集）」第十題訂定。 十一、 為降低金融機構供應商鎖定之風險及確保資料之可移植性，參照新加坡 MAS Advisory on Addressing the Technology and Cyber Security Risks Associated with Public Cloud Adoption 及 ABS Cloud Computing Implementation Guide 2.0，爰依據「金融機構作業委託他人處理內部作業制度及程序辦法」第八條第一項第三款要求，於第四條第五項第三款、第五

	款明訂金融機構於使用雲端服務時，應考量雲端服務資料可用性與互通性要求。 十二、 依據「金融機構作業委託他人處理內部作業制度及程序辦法」第十九條第一項第一款與「金融機構運用新興科技作業規範」第二條第一項第五款要求，爰於第四條第五項第三款明訂金融機構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。惟參照新加坡 ABS Cloud Computing Implementation Guide 2.0 採用多雲或其他分散策略時，雖可避免過度集中，應考量與組織內部的技術、管理能力達到平衡。 十三、 第四條第五項第四款係參照美國 Cloud Security Technical Reference Architecture、新加坡 Advisory on Addressing the Technology and Cyber Security Risks Associated with Public Cloud Adoption 及 Cloud Computing Implementation Guide 2.0，爰明訂金融機構於使用雲端服務時，應建立涉及雲端服務之系統監控機制，如監控雲端資源使用情況、服務可用性，並應注意是否已執行完成所有作業程序，以避免影響正常交易等。
第五條 金融機構使用雲端服務時，應依所使用之雲端服務模式執行盡職調查及定期審查程序： 一、應評估雲端服務業者之專業	一、本條訂明金融機構於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、契約應載明之項目與雲端服務業者之責任。

知識與資源、財務健全、內部控制及資安管理機制及符合法規要求。 二、金融機構執行盡職調查時，應以風險基礎方法決定其執行強度。評估項目宜包含： （一）金融機構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金融機構受託作業之客戶資料處理地及其儲存地之司法管轄區，是否可能對金融機構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金融機構需求。 （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	二、鑑於盡職調查為簽屬委外契約前之關鍵任務，參酌香港 Guidance on Cloud Computing，爰於第五條第一項明訂金融機構於使用雲端服務時，應執行盡職調查及定期審查程序，並參照「金融機構作業委託他人處理內部作業制度及程序辦法」第八條、第十八條及第十九條要求，爰於第五條第一項定義金融機構對於業者盡職調查之要項。 三、考量針對雲端服務業者有跨國佈署雲端資源之風險，參考香港 Guidance on Cloud Computing 與英國 FG 16/5 Guidance for firms outsourcing to the 'cloud' and other third party IT services 等規範，爰於第五條第一項第二款第一目規範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，評估當地監管機構調閱金融機構資料之風險。 四、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，爰於第五條第一項第二款第二目要求雲端服務業者應實施相關控管，金融機構得參照雲端問答集第 4 題說明，依據雲端服務業者提供服務之內容、範圍及性質等要求其採用適合之國際資訊安全標準，如國際標準組織之 ISO27001、ISO27002 、ISO27017、ISO27018 、ISO27701 以及雲端安全聯盟（CSA）STAR 驗證等，以評估是否已建立妥適之資訊安全控管措施。 五、依據「金融機構作業委託他人處

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金融機構資安需求。 三、外國銀行在臺分（子）行經由總（母）行、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，得援用其總（母）行、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。 金融機構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，並符合以下要求： 一、契約或協議內容依「金融機構作業委託他人處理內部作業制度及程序辦法」第十條及第十八條規定，應確認涵蓋下列事項： （一）委外事項範圍及雲端服務業者之權責，應包括金融機構與雲端服務業者間之責任區分及雲端服務水準； （二）客戶資料保密及安全措施，應包括金融機構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； （三）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； （四）雲端服務業者就受託事項範圍，同意金融機構、	理內部作業制度及程序辦法」第四條第三項要求，因雲端服務營運持續性及有效性係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採用雲端服務之金融機構。經參照香港 Guidance on Cloud Computing，爰於第五條第一項第二款第四目，明訂金融機構針對雲端服務業者之災難復原及營運持續能力評估規範。 六、考量金融機構與雲端服務業者之間應以契約或協議作為權益保證，依據「金融機構作業委託他人處理內部作業制度及程序辦法」第十條第一項第一款、第三款、第七款、第八款及第十款，以及同法第十八條第二項第六款、第十九條第一項第五款之要求，第五條第二項第一款爰明訂契約或協議內容應確認涵蓋事項及應符合事項。 七、依據「金融機構作業委託他人處理內部作業制度及程序辦法」第十九條第一項第二款，金融機構對雲端服務業者負有最終監督義務，故應確保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符合相關規範之要求，第五條第二項第二款爰要求金融機構對契約或協議內容評估及監督之責任。 八、考量雲端服務業者修訂契約或協議之實務限制，第五條第二項第二款爰明訂如契約或協議內容無法符合應採行適當評估，並依據風險規劃及採行妥適之替代措施，如經適當評估認為不符合之

主管機關或其指定之人查核之要求； （五）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金融機構，包括對於影響金融機構之資訊安全事件通報責任； （六）如涉及重大性消費金融業務資訊系統委託由雲端服務業者處理，應包括委外作業移轉至其他雲端服務業者或移回金融機構之情況，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。 二、前揭契約或協議內容如無法符合本項第一款要求，應採取適當評估，並依風險規劃替代措施，以確保金融機構對雲端服務業者之最終監督義務之執行。 三、外國銀行在臺分（子）行經由總（母）行、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，得由總（母）行、總機構或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項第一款及第二款之要求。 金融機構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	情形並不影響風險（例如：依實際應用情境於前款事項有不適用者），則無須採行替代措施。 九、考量金融機構應確保雲端服務業者提供之服務符合期待，參考「金融機構運用新興科技作業規範」第二條第十三款第四目，第五條第三項爰明訂金融機構應監督及定期審查服務執行情形，包含服務水準報告與操作紀錄等，並參酌香港 Guidance on Cloud Computing 要求金融機構在使用雲端服務時應依據風險程度與對營運影響程度調整其審查與監督頻率。 十、依據雲端問答集第一題之說明，委外辦法所定金融機構將作業委託他人處理涉及雲端服務之範圍除金融機構直接委託雲端服務業者，亦包括金融機構之受委託機構複委託予雲端服務業者處理之情形，爰於第五條第三項第二款明訂適用範圍。並參照「金融機構作業委託他人處理內部作業制度及程序辦法」第十條第二項要求，委外契約中應針對複委託情形，訂明複委託之範圍、限制或條件。為避免適用之疑義，金融機構使用非自有雲端平台之雲端服務業者所提供之應用軟體服務、工具或解決方案者（SaaS 服務），應與 SaaS 服務商依前項規定達成服務使用契約或協議，而雲端平台業者尚無本條複委託之適用，併予敘明。 十一、 鑑於雲端服務業者負責雲端服務基礎設備維護之操作，參考「金融機構運用新興科技作業規

以輔助其監督作業： 一、金融機構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、金融機構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、金融機構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、金融機構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。	範」第二條第一項第十三款第五目，爰於第五條第三項第三款明訂金融機構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之相關資料遷移及刪除事宜。
第六條 為確保金融機構相關人員具備應有之專業知識與技能，金融機構於使用雲端服務期間，應依以下規定定期辦理人才培訓： 一、專責單位應針對負責雲端之部門、團隊及涉及雲端服務相關人員提供適當之訓練與資源，以提升人員對雲端服務導入、使用及管理之能力，並能以風險為基礎方法做出適當之決策與監督。 二、應針對培訓對象之角色與權責，依職能提供包含資訊安	一、本條訂明雲端能力之訓練及能力、人力提升計畫。 二、依據「金融機構作業委託他人處理內部作業制度及程序辦法」第四條第三項第二款要求，金融機構應確保具備充足之資源與專業，考量金融機構應確保相關人員具備應有之專業知識與技能來理解並管理採用雲端之風險，且有鑑於培訓規劃重點應持續更新，並定期檢視其有效性，參考新加坡 TRM Guidelines、美國 Cloud Security Technical Reference Architecture 及 FFIEC IT

全、風險認知和雲端知識技能等內容，確保相關人員具備足夠之專業知識與技能。 三、應確保培訓資源與培訓政策的持續更新，並驗證培訓之有效性。	Examination Handbook InfoBase，爰於第六條第一項明訂人才培訓之內容範疇及更新時機。 三、第六條第一項第二款所稱之培訓對象可包含負責雲端運作之高階管理人員、服務監管人員、執行團隊及其他涉及雲端服務相關操作與管理人員。
第七條 金融機構應建立雲端服務資安控管機制，依風險基礎方法採取適當之控管措施，以確保使用雲端服務符合金融機構資訊安全政策等相關規範要求。 一、加密與金鑰管理 （一）傳輸及儲存客戶資料或機敏資料時，應採行資料加密或代碼化等有效保護措施，並遵循加密金鑰管理程序要求。 （二）如保管加密金鑰，應妥適注意其儲存安全。 二、資料安全與隱私管理 （一）金融機構對於雲端服務業者處理之資料應保有完整所有權，除執行指定作業外，金融機構應確保其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。 （二）雲端服務存取應使用加密通訊協定。 （三）宜依據雲端服務使用之目的控管雲端服務存取方式。 三、身分識別與存取控制	一、本條訂明金融機構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、數據及隱私資料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酌美國 CSA Cloud Control Matrix v4.0 架構，惟金融機構應針對所使用之雲端服務模式設計控制措施，並以風險基礎方法決定資安項目執行強度與項目之必要性。 三、依據「金融機構作業委託他人處理內部作業制度及程序辦法」第十九條第一項第四款要求，金融機構傳輸及儲存客戶資料至雲端服務業者，應訂定妥適之加密金鑰管理機制，參酌新加坡 ABS Cloud Computing Implementation Guide 2.0 及美國 FFIEC Security in a Cloud Computing Environment 和 NIST FIPS 140-2，爰於第七條第一項第一款明訂金融機構於使用雲端服務時，應進行之加密與金鑰管理之規定，金鑰管理機制如：租用硬體安全模組或由金融機構自行管理金鑰（Bring Your Own Key, BYOK）。 四、第七條第一項第一款第一目係依據「金融機構運用新興科技作業

（一）應基於最小權限原則、角色和權限管理原則，建立雲端資源和資料之存取權限授權政策。 （二）應針對特權帳號實施多因子身份驗證機制，如：具備調整雲端服務組態設定權限之帳號。 （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。 四、稽核軌跡與監控 （一）應留存金融機構人員對於雲端服務平台操作之稽核軌跡。 （二）宜針對雲端安全事件場景制定監控與分析之關聯規則，以即早發現潛在資安風險。 （三）宜考量集中管理稽核軌跡與監控資料。 （四）應避免雲端平台之稽核軌跡內容含有未加密之營運或客戶重要資料。 （五）如金融機構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。 五、基礎架構安全 （一）應定期評估雲端服務之基礎架構安全管理機制。 （二）應採取適當措施管理金融機構使用中的虛擬機和容器之映像檔。	規範」第二條第一項第九款要求訂定。 五、第七條第一項第一款第二目金鑰應遵循本會相關規範辦理，注意其儲存安全，宜考量與虛擬映像檔等雲端關鍵資訊資產分開儲存。 六、為確保於雲端環境中處理資料之過程得以遵守相關法令法規要求，並保護資料之機密性和完整性，參照新加坡 ABS Cloud Computing Implementation Guide 2.0 及美國財政部 The Financial Services Sector's Adoption of Cloud Services 與美國 Cloud Security Technical Reference Architecture，爰於第七條第一項第二款明訂金融機構於使用雲端服務時，應遵守之資料安全與隱私管理要求。 七、第七條第一項第二款第一目係依據「金融機構運用新興科技作業規範」第二條第十款要求訂定。 八、雲端環境中之資源和資料應受適當保護，同時應確保僅有授權之人員可以存取必要資源和資料，參照新加坡 TRM Guidelines、Advisory on Addressing the Technology and Cyber Security Risks Associated with Public Cloud Adoption、ABS Cloud Computing Implementation Guide 2.0、德國 Cloud Computing Compliance Controls Catalogue （C5）及香港 Guidance on Cloud Computing，爰於第七條第一項第三款明訂金融機構應遵循之身分識別與存取控制規範。 九、考量雲端服務如開放透過網際網

六、威脅與弱點管理 （一）針對金融機構自行管理之雲端環境，應有威脅與弱點檢測及管理流程，以定期評估網路安全防禦措施之有效性。 （二）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金融機構之影響。 七、變更管理與組態安全 （一）應確保實施雲端服務組態管理機制，包含組態變更前後之評估，並妥善管制對雲端服務組態之變更紀錄。 （二）應建立對基礎映像檔之標準變更管理流程，為確保採用可信任來源之映像檔，宜執行完整性檢查。	路直接存取之風險，第七條第一項第三款第三目要求應建立身分識別與存取控制等安全控制措施，包含強化身分、設備或來源IP識別等。 十、金融機構使用雲端服務時應負有監督和記錄之責任，以確保雲端環境之安全性及合規性，參酌新加坡 ABS Cloud Computing Implementation Guide 2.0 及美國 Cloud Security Technical Reference Architecture，爰於第七條第一項第四款明訂金融機構於使用雲端服務時，應進行雲端環境安全之監控及稽核軌跡管理之相關規定。 十一、 鑑於金融機構使用雲端服務時應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，參考新加坡 ABS Cloud Computing Implementation Guide 2.0 及美國 FFIEC IT Examination Handbook InfoBase – IT Booklet: Management 與 Cloud Security Technical Reference Architecture，爰於第七條第一項第五款明訂金融機構於使用雲端服務時，應遵循之基礎架構安全之規定。 十二、 為確保金融機構及時發現應用程式和系統中之弱點和漏洞，以有效防範潛在攻擊，且考量金融機構應於雲端環境中能夠積極應對各種威脅和弱點，以確保資訊資產安全性和系統正常運作，參酌新加坡 ABS Cloud Computing Implementation Guide 2.0，爰於第七條第一項第六款明

	訂金融機構使用雲端服務時，應遵循之威脅與弱點管理規定。 十三、 為確保金融機構在雲端環境中對系統進行變更時，能夠以受控且安全之方式進行，且考量金融機構使用雲端服務時應對其組態進行管理，參照新加坡 ABS Cloud Computing Implementation Guide 2.0，爰於第七條第一項第七款明訂金融機構使用雲端服務時，應進行之變更及組態管理要求。
第八條 金融機構應就雲端服務規劃雲端服務委外查核作業，包含規劃查核之時機、內容與查核執行方式： 一、對於具重大性之境外雲端委外服務，應每年至少辦理一次查核。 二、其他非屬重大性境外雲端委外服務，應依風險基礎方法規劃雲端服務查核頻率，並依風險變化調整查核頻率。 金融機構應評估查核人員之獨立性、資格與專業性，包含其是否具備執行查核所需之專業知識和技能，或具備雲端安全相關證照。 對於重大性委外雲端服務，金融機構對雲端服務之查核重點項目宜包含： 一、雲端服務所在機房之實體安全控管機制。 二、雲端服務業者處理作業相關之重要系統及控制環節。 三、盡職調查過程中雲端服務業者所提供之報告內容。 四、雲端平台資料刪除與災難復原流程。	一、本條訂明金融機構於執行雲端服務查核時應遵循之事項。 二、為確保有限之查核資源聚焦於金融機構最重要之風險和控制點，以達到更有效之風險管理，參考美國 FFIEC IT Examination Handbook InfoBase - IT Booklet: Audit、FFIEC IT Examination Handbook InfoBase - IT Booklet: Business Continuity Management 、德國 Cloud Computing Compliance Controls Catalogue （C5）及日本雲端服務使用資訊安全管理指南，爰於第八條第一項明訂金融機構應就雲端服務委外重大性及依風險基礎方法選擇查核之時機、內容與查核執行方式。 三、依據「金融機構作業委託他人處理內部作業制度及程序辦法」第十八條第二項第四款要求，金融機構辦理涉及重大性消費金融業務資訊系統委託至境外處理，應每年至少辦理一次一般性查核及一次專案查核。除法規已有規定外其他雲端委外作業，爰於第八條第一項第一款明訂具重大性之境外雲端委外

五、雲端服務業者之營運持續性控制措施。 六、確認雲端服務作業內容執行之妥適性及符合相關本會規範及國際資訊安全標準。 金融機構應持續追蹤雲端服務業者之查核改善情形，確保其採取適當和及時之替代性措施。 外國銀行在臺分（子）行經由總（母）行、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，可援用其總（母）行、總機構或經其授權之區域總部負責統籌辦理並提供第三方查核報告。	服務查核之頻率為每年一次，並於第八條第一項第二款其他非屬重大性境外雲端委外服務，應依風險基礎方法規劃雲端服務查核頻率，並依風險變化調整其頻率。 四、依據「金融機構作業委託他人處理內部作業制度及程序辦法」第十九條第一項第三款要求，金融機構應評估查核人員適格性，鑑於金融機構之雲端服務查核作業日漸普遍，考量查核品質及結果之可靠性和查核人員之專業性、獨立性和客觀性，參酌新加坡 ABS Cloud Computing Implementation Guide 2.0 及香港採購雲端服務的實務指南，爰於第八條第二項明訂查核人員應具備之資格。 五、考量雲端服務委外重大性並採風險基礎方法決定查核項目，爰參考新加坡 ABS Cloud Computing Implementation Guide 2.0、美國 Cloud Security Technical Reference Architecture 及日本 FISC Security Guidelines on Computer Systems for Banking and Related Financial Institutions，於第八條第三項各款明訂對於重大性委外雲端服務，金融機構宜考量之查核重點項目。 六、為提供安全、可靠且合規之雲端服務，爰參考新加坡 ABS Cloud Computing Implementation Guide 2.0，於第八條第四項明訂金融機構應持續追蹤雲端服務業者之查核改善情形。 七、考量外國銀行在臺運作實務，依據「金融機構運用新興科技作業規範」第二條第一項第十一款及「金融機構作業委託他人處理內部作

	業制度及程序辦法相關問題適用解說問答集（雲端問答集）」第十二題說明，於第八條第五項明訂其可援用其總（母）行、總機構或經其授權之區域總部相關查核資源。
第九條 金融機構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、規劃營運持續管理計畫，應考量雲端服務所涉及資產、資源與資料所在位置，以及雲端服務業者可提供之復原能力。 三、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，確保資訊之可用性及防止未授權存取。 四、金融機構規劃具重大性委外業務持續運作之測試或演練計畫時，應以風險基礎方法，決定測試或演練執行頻率與方式。宜考量與雲端服務業者共同合作擬訂建立使用雲端服務之業務持續運作測試或演練計畫，並得於情況允許下與雲端服務業者進行聯合測試或演練。 金融機構應建立使用雲端服務之資訊安全事件通報與管理機制。 金融機構應於採用雲端服務前，建立終止使用雲端服務之轉移策略及計畫，應包含以下事項： 一、終止雲端服務時資料處置方式，包含但不限於刪除、將資料移回金融機構自行處理，	一、本條訂明營運持續管理相關規範，包含使用雲端服務之資訊安全事件通報，以及終止委託之轉移機制。 二、考量金融機構使用雲端服務時，將須依其對既有資訊系統與業務產生之影響，分配所需資源，參照「金融機構資通安全防護基準」第十七條營運持續管理說明，並參酌美國 FFIEC IT Examination Handbook InfoBase - IT Booklet: Business Continuity Management、德國 Cloud Computing Compliance Controls Catalogue （C5）及日本雲端服務使用資訊安全管理指南，爰於第九條第一項第一款明訂金融機構於使用雲端服務時，應遵循之營運衝擊分析及評估規定。 三、依「金融機構作業委託他人處理內部作業制度及程序辦法」第八條第一項第二款第五目要求，爰於第九條第一項第四款要求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，避免因重大異常或事項影響金融機構正常營運或對客戶權益有重大影響。 四、為確保金融機構有效應對使用雲端服務之資訊安全風險及確保業務穩定運作，同時遵循相關法令法規要求，爰於第二項明訂金融機構應建立使用雲端服務之資訊

或將其移轉至其他雲端服務業者。 二、金融機構應確保終止委外契約或終止使用雲端服務時，刪除雲端服務業者留存之資料，並留存刪除或銷毀之紀錄。前述資料包含但不限於電子資料、應用程式及備份資料等。	安全事件通報與管理機制。 五、依據「金融機構作業委託他人處理內部作業制度及程序辦法」第八條第一項第三款要求，金融機構應訂定終止委託之移轉機制，鑑於金融機構對雲端服務管理機制，除應建立有效之緊急應變程序及營運持續計畫，與雲端服務業者終止服務契約或協議，或終止使用雲端服務時，應確保能順利移轉至其他雲端服務業者或移回自行處理，並確保原受委託機構留存之資料全數刪除或銷毀，並留存刪除或銷毀之紀錄，爰於第九條第三項明訂終止委託之移轉機制要求。
第十條 本自律規範經本會理監事會議通過並報請金融監督管理委員會備查後施行；修正時亦同。	本條說明本規範之施行及修正程序。