金融機構使用雲端服務實務手冊

專案單位：銀行公會金控業務委員會金融科技發展組

撰寫：勤業眾信會計師事務所

日期:113 年 8 月

目錄

總則

一、目的

隨著雲端服務發展逐漸成熟，全球企業持續快速將工作負載轉移到雲端，故本金融機構使用雲端服務實務手冊（以下稱實務手冊）旨在協助金融機構於建置或使用雲端服務時，可依據國際標準及適用法規要求，建構雲端數位轉型策略、檢視與降低使用雲端服務可能帶來之風險，使金融機構能安全且合適地推動雲端數位轉型之策略目標，進而提升金融機構資訊作業效益。本實務手冊係屬建議性質，金融機構可參考本實務手冊執行建置或使用雲端服務，但不以此為限。

二、使用建議

本實務手冊提供金融機構作業使用雲端服務時參考，建議我國金融機構使用雲端服務時，不論是否屬金融機構作業委外使用雲端服務之範疇，皆可因應雲端服務使用情境，建構雲端服務完整風險管理及控管程序。

三、雲端服務之種類、部署模型

依雲端服務業者提供之雲端服務模式，雲端服務可分為三個種類，包含基礎設施作為服務（Infrastructure as a Service, IaaS）、平台作為服務（Platform as a Service, PaaS）及軟體作為服務（Software as a Service, SaaS）。金融機構可依據所需之服務選擇一個或多個服務模式。

(a) 軟體即服務（SaaS）：雲端服務業者提供集中式代管軟體與相關資料，使用者使用軟體，但無需安裝軟體、作業系統、硬體。具備使用簡單、無需安裝、即時更新之特性。

(b) 平台即服務（PaaS）：雲端服務業者提供雲端運算平台解決方案，使用者能於此平台操作其軟體，但不需管理與控制雲端基礎設施（包含網路、伺服器、作業系統或儲存空間）。

(c) 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），使用者能掌控作業系統、儲存空間、已部署的應用程式及網路元件（如防火牆、負載平衡器等），但無需控管或維護基礎運算資源。

第一章、 雲端服務策略發展與治理

一、金融業雲端轉型推動關鍵

目的

金融機構考慮採用雲端服務時，建議謹慎評估以下影響成效的關鍵因素，並適時進行相關領域的評估與更新，以確保最大程度的保護組織利益。

參考指引

金融機構在推動雲端轉型時，可考量下列因素訂定雲端服務採用之策略，並依據雲端技術採用之進程，從準備、發展至優化階段逐步調整策略，邁向以韌性為導向之雲端轉型目標：

(a) 雲端服務供應商提供之雲端服務與新興科技的發展趨勢。
(b) 外在環境，如：市場、主管機關、法規等趨勢。
(c) 雲端服務對於金融機構業務發展方向與趨勢之影響。
(d) 整體資訊系統架構採用雲端服務之影響。
(e) 數據架構與數據應用之需求。
(f) 資訊基礎設施與資訊安全之潛在風險。
(g) 整體資訊作業與服務流程之管控。
(h) 適當的雲端技術人才培訓。

二、雲適性評估

目的

金融機構使用適性評估框架分析現有的企業應用程式組合，以確立雲端服務採用策略及計畫。

參考指引

金融機構以系統化之雲適性評估與遷移路徑分析，檢視現有系統於業務面與技術面之屬性，並針對欲遷移之系統進行財務與雲端服務業者之評估。雲適性評估結果可做為金融機構執行遷移作業時識別最佳遷移路徑之參考資訊，其中最佳遷移路徑可參考 Gartner 發布之 5R 模型，以 Rehost、Refactor、Rearchitect、Rebuild、Replace 做為執行遷移作業之原則。下列係於執行雲適性評估作業時可參考之評估項目示例：

(a) 業務面評估項目： 業務關鍵性、業務支援性、風險監管需求等。
(b) 技術面評估項目： 基礎設施架構、應用架構、網路架構、系統相依性等。
(c) 財務面評估項目：地端資源、雲端資源、執行搬遷作業資源等。

(d) 雲端服務業者評估項目：市場價值、使用者情境支援性、技術相容性與互通性、雲端解決方案社群支援性、雲端服務價格方案、雲端資源服務水準與資訊安全能力等。

金融機構採用雲端服務之策略及目標，可因應金融機構業務發展、技術發展、監理法規要求及利害關係人期待等內、外部議題影響持續更新。考量客戶體驗、營運需求及資訊架構發展各層面之規劃以選擇妥適之雲端服務應用策略推動計畫。

在雲端服務地點選擇時，可綜合考量雲端服務業者提供服務之機房所在國家的政治、經濟與法規之穩定度，以選擇合適之資料處理及儲存地點。評估項目可包含：

(a) 金融機構選用雲端服務之客戶資料處理地及其儲存地時，可考量該地區社會、政治和經濟環境妥適性。
(b) 金融機構可優先考量與可保有其指定資料處理地及其儲存地之權利的雲端服務業者合作。
(c) 如受委託之雲端服務業者其資料處理及儲存地位於境外時，金融機構可選擇指定雲端服務機房應位於當地資料保護法規不低於我國要求之國家。評估各國家之資料保護法規時，可參考委外辦法相關問題問答集第 10 題，已曾經評估屬當地資料保護法規不低於我國要求之國家：德國、法國、荷蘭、奧地利、愛爾蘭、芬蘭等歐盟國家，瑞士、冰島、美國、英國、印度、日本、韓國、香港、菲律賓、馬來西亞、新加坡、澳洲。
(d) 建議金融機構可要求雲端服務業者除在法律不允許之情況下，在當地法律要求其向第三方揭露資料時應通知金融機構。

基於作業風險分散之原則，金融機構可實施多雲或其他分散策略，以適度分散降低對單一雲端服務業者曝險度過高之風險，惟多雲可能使營運複雜性提升，故金融機構可視其對雲端管理技術之熟悉度及服務穩定度，選擇發展單雲或多雲之策略；同時亦可建立雲端服務資料可用性與互通性政策和程序，以降低服務鎖定風險與提高資料可移植性，提前規劃於未來服務結束時，得以將系統遷移或資料遷出雲端服務。

三、雲端服務治理制度

目的

確保金融機構建立完善治理制度，以有效管理其所採用之雲端服務。

參考指引

金融機構建立「雲端服務管理政策」時，以符合金融機構管理其雲端服務之政策及目標為目的，可涵蓋下列項目，並建議每年檢視雲端服務管理政策是否受到下列要素影響，以適時更新：

(a) 市場與雲端服務業者等外部環境。
(b) 金融機構營運策略及利害關係人要求。
(c) 主管機關雲端相關法規、法律等監管規範之要求。
(d) 金融機構組織、資安、風控等政策之影響。
(e) 雲端技術安全風險及威脅。

四、權責劃分

目的

確保金融機構建立內部專責單位以及相關單位之相關權責劃分，以降低角色及權限間相互衝突風險。

參考指引

金融機構可針對雲端服務管理單位、維運單位、使用單位與資訊安全管理單位等，規劃雲端服務使用及管理之相關角色權責與責任劃分，雲端服務之分工及權責可涵蓋以下作業分工：

(a) 雲端服務需求申請：依據業務需求提出雲端服務申請，並對雲端服務進行驗證測試及驗收作業，以確保符合業務所需。
(b) 雲端服務業者評估：評估雲端服務業者提供雲端服務之能力與風險評估，以確保雲端服務業者能履行服務承諾。
(c) 雲端服務安全管理：評估雲端服務之安全性，確保使用雲端服務之過程可以符合金融機構之安全要求，並設計雲端安全控制措施。
(d) 雲端服務管理規範建置及維護：針對雲端服務使用之完整生命週期建立合適之以管理規範，並確保相關人員可清楚瞭解並遵循管理規範要求。
(e) 雲端應用系統開發及維護：負責雲端應用系統之設計、實作及檢視。
(f) 雲端應用系統存取管理：負責雲端應用系統權限及帳號設定與定期審查作業。
(g) 雲端平台維運管理：負責雲端平台之建置、維護與變更等管理，包含系統架構設計、系統部署、雲端平台存取管理及網路管理等作業。
(h) 雲端服務資源管理：瞭解業務對於資源之要求並確保運作不受干擾，使系統具有適當的資源，以便在發生故障或計畫外停機時具有彈性。
(i) 雲端成本管理：負責追蹤雲端服務費用的內部分配。

考量角色及權限間相互衝突之職務，為防止由個人獨自執行潛在衝突的職務。建議金融機構區隔以下職務及責任範圍。下列係可能要求區隔之活動示例：

(a) 啟動、核可及執行變更；
(b) 申請、核可及實作存取權限；
(c) 設計、實作及檢視程式碼；
(d) 設計及查核雲端安全控制措施。

第二章、 雲端風險評估方法

一、以風險基礎方法落實核心原則

金融機構確認、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。依風險基礎方法，金融機構可依其風險胃納評估風險等級，對於較高風險情形採取加強措施，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。

依據ISO 31000風險管理原理及指導綱要，金融機構並非所有部門或活動都適用單一種風險管理的方法，但建立雲端風險評估方法時可以考量與其它的風險管理進行協調整合。因此，金融機構於決定其風險胃納時，可考量金融機構現行之風險評估方法論、組織規模、資源等，決定金融機構整體願意接受之風險程度。風險管理的過程包含以下步驟：

(a) 溝通及諮詢
(b) 確認內部及外部情境
(c) 風險評鑑：包含風險鑑別、風險分析與風險評估流程
(d) 風險處置
(e) 監督與審查

風險管理有助於決策者作出明智的選擇。風險管理有助於確立及選擇方案之判斷。因此，風險管理可以幫助金融機構在進行委外服務前，先行確定雲端服務採用之風險的可接受程度以及風險處理的合理性與有效性。

二、雲端風險評估

目的

識別、評估及管理使用雲端服務之潛在風險。

參考指引

金融機構建立風險評估機制，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：

(a) 建立及維持風險接受、執行雲端安全風險評估之準則。
(b) 確保重複之風險評估產生一致、有效及可比較之結果。
(c) 識別使用雲端服務之潛在風險及其風險擁有者。
(d) 訂定風險處理優先序。

金融機構執行風險評估時，風險評估項目包含但不限於：

(a) 雲端委外作業是否具重大性；
(b) 雲端服務種類與部署模型；
(c) 雲端服務目的與範圍；
(d) 雲端服務使用期限；
(e) 雲端服務所涉及之資料敏感度（包含個人資料）；
(f) 涉及雲端服務之業務或資訊系統重要程度；
(g) 雲端服務提供者之聲譽、可靠性、資訊透明度；
(h) 雲端服務提供者所提供之服務水準協議資訊；
(i) 雲端服務提供者所提供之資安強度；
(j) 雲端服務集中度；
(k) 金融機構對於雲端服務之管理能力與經驗。

金融機構判斷雲端委外作業風險是否具重大性之考量因素，依據委外事項所面臨的情況綜合考量，包含委外範圍是否對金融機構或其客戶具有重大影響，可參照「金融機構作業委託他人處理內部作業制度及程序辦法」相關問題問答集第 4 題舉例如下：

(a) 雲端委外作業是否屬金融機構之關鍵業務，如：雲端服務所涉業務是否對金融機構之營收與獲利有直接影響、所涉業務是否屬於金融機構持續營運管理計畫所列的關鍵營運流程等。
(b) 雲端委外作業對盈餘、償付能力、流動性、籌資能力、資本及風險之潛在影響。
(c) 若雲端服務業者未能提供服務或發生資料保護或資訊安全問題，將對金融機構之聲譽、營運目標之達成、客戶權益、交易對手或整體金融市場造成重大影響等。如：雲端服務所涉業務是否具有時效關鍵性，當雲端服務發生中斷時，金融機構所能容忍的業務恢復時間復原時間目標（Recovery Time Objective, RTO），及是否會直接影響客戶重大權益。
(d) 雲端委外作業之建置成本。
(e) 金融機構若須將雲端服務移回金融機構本身、或尋找其他雲端服務業者提供服務時所衍生之移轉成本。
(f) 金融機構如委託同一家雲端服務業者提供服務，金融機構對該雲端服務業者之總暴險。
(g) 雲端服務業者面臨營運問題時，金融機構仍可維持適當內控制度及符合法規要求之能力。

金融機構可依據個別機構及委外事項所面臨的情況綜合考量，並定期檢視評估結果是否依然妥適，例如原屬不重大之雲端委外事項，可能在同一雲端服務業者之委外作業規模增加或委外事項的性質改變而變得具重大性，以因應風險之變更調整控管要求。

第三章、 雲端服務管理架構

一、盡職調查

目的

確保金融機構為建立盡職調查，幫助識別與監控使用之雲端服務風險。

參考指引

金融機構執行盡職調查時建議評估下列項目，得依據所採用之服務與風險決定針對雲端服務業者之盡職調查的執行強度：

(a) 雲端服務業者之專業能力與資格；
(b) 雲端服務業者之服務水準；
(c) 雲端服務業者之財務狀況；
(d) 雲端服務業者對於我國法規之遵循承諾；
(e) 雲端服務業者是否可配合金融機構及其主管機關辦理實地查核；
(f) 雲端服務業者之備援機制；
(g) 雲端服務業者之資訊安全防護能力，包含者是否已具備資訊安全、資料保護或營運持續相關制度與認證，包含但不限於 ISO 27001、ISO 27701、ISO 27017、ISO 27018、ISO 22301 或 CSA STAR 等；
(h) 雲端服務業者之威脅與弱點管理機制，包含是否允許金融機構針對雲端服務營運環境進行弱點掃描和滲透測試；
(i) 雲端服務業者之資訊安全事件通報責任管理機制；
(j) 雲端服務業者之稽核軌跡留存機制；
(k) 雲端服務業者的業務持續運作機制與災難復原能力；
(l) 雲端服務業者是否提供資料處理及儲存位置之權利；
(m) 雲端服務業者是否具備雲端基礎架構及虛擬化設備安全管理程序；
(n) 雲端服務業者的資料銷毀、資料遺失和資料外洩通報管理機制；
(o) 雲端服務業者支援金融機構營運持續計畫與退場機制之測試或演練。

藉由以上盡職調查項目，金融機構判斷雲端服務業者是否可符合金融機構需求。

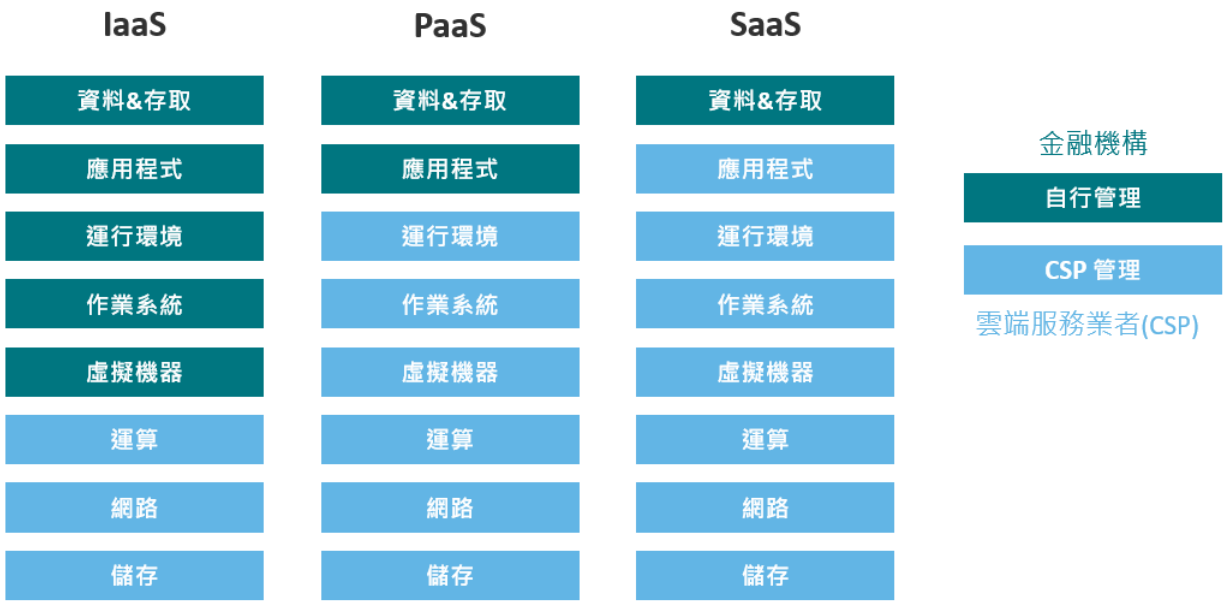
二、共享責任

目的

為確保金融機構使用雲端服務時明確瞭解內、外部角色權責劃分。

參考指引

金融機構於使用不同服務模式時，其雲端安全責任亦有所不同，以下為不同服務模式下金融機構和雲端服務業者之間的責任：



三、契約與協議

目的

金融機構使用雲端服務時，為與雲端服務業者達成服務使用契約或協議，作為權益確認及確保達成雙方期望與認知。契約或協議為做廣義的解釋，除雙方簽署或達成合意之紙本或電子書面外，可包括雲端服務業者單方提供予金融機構之條款、約定、承諾，或其他紙本或電子書面、文件或網頁。

參考指引

金融機構在使用雲端服務前，務必與雲端服務業者建立相關契約或協議以確保金融機構之權利，金融機構使用雲端服務時通常分為二類：

一、與雲端服務業者直接簽約模式：可直接與雲端服務業者擬議以落實委外契約權責之建構，進而履行管理雲端服務業者之義務。

二、透過雲端服務業者合作夥伴（如：經雲端服務業者授權之經銷商）採購雲端服務時之經銷模式：金融機構透過與雲端服務業者合作夥伴擬議，訂閱雲端服務及收取費用，該服務之提供者仍為雲端服務業者，原則上由金融機構與該雲端服務業者達成契約或協議。因此，為建立雲端服務業者對於其所提供服務之履約責任及義務，雲端服務業者可提供(或透過合作夥伴提供)金融服務附加條款「Financial Services Addendum（FSA）」或相關承諾書，以條款、約定、承諾，或其他紙本或電子書面、文件或網頁等方式，敘明其對於委外契約之權利義務關係。

除前二類模式外，金融機構直接訂閱 SaaS 服務時，通常以訂閱制協議為雲端服務業者與雲端服務使用者之間的協議，當金融機構選擇訂閱雲端服務時，可透過訂閱制

協議瞭解雙方之責任及義務後，由雲端服務業者提供商品、服務或數位內容，並由金融機構支付費用，通常此協議具備以下一項或兩項標準：

(a) 為無限期或固定期限之自動續約，除非金融機構採取行動停止協議續約或在到期前終止協議；

(b) 含有免費試用或降價期，期後協議效力持續，金融機構必須支付更高費率，除非金融機構採取行動終止。

不論直接或間接與雲端服務業者簽署協議，相關契約或協議內容可參考「金融機構作業委託他人處理內部作業制度及程序辦法」要求，可區分為法規要求「應記載事項」及雲端服務業者應「協力事項」二類。

「應記載事項」包含委外辦法第十條與第十八條第二項之要求，可參考下表進行約定：

依法應記載事項	**參考範例**
1. 雙方委外事項範圍與權責區分，權責及義務責任，可考量雙方的共同責任模型，包含雲端服務業者及金融機構各自負責管理的項目。	（依實際情形約定）
2. 雲端服務業者所承諾之服務水準，並應包括服務可用性之要求。	乙方提供雲端服務期間，有關服務安全性與可用性等服務水準載明於（文件名稱及存放位置），乙方應依承諾提供服務。
3. 雲端服務業者應確實遵守我國相關法令，不得違反法令強制或禁止規定、公共秩序及善良風俗，對經營、管理及客戶權益，不得有不利之影響，並應確保遵循銀行法、洗錢防制法、個人資料保護法、消費者保護法及其他法令之規定。	乙方應盡善良管理人注意義務依約定履行本合約，且不得違反法令強制或禁止規定、公共秩序及善良風俗，並應遵循保險法、洗錢防制法、消費者保護法、個人資料保護法、金融消費者保護法、保險業作業委託他人處理應注意事項及其他法令之規定。
4. 雲端服務業者應建立客戶資料保密及安全措施，應包括資料區隔要求，以及雲端服務業者向第三方揭露資料之限制。	乙方履行本合約應落實客戶資料保密及安全措施，並同意甲方保有存放於雲端之資料所有權、資料區隔要求。 除在法律不允許之情況下，乙方未經甲方事前書面同意，不得向第三方揭露甲方之資料。 前項所謂事前書面同意，係指乙方於事前以書面方式向甲方提出資料揭露之對象、範圍及內容等說明，並經甲方以書面回覆同意。
5. 雲端服務業者應依金融機構監督訂定之標準作業程序，執行消費者權益保障、風險管理、內部控制及內部稽核制度。	乙方履行本合約應落實消費者權益保障，包括消費者資料保密及安全措施，並同意應依據甲方督導訂定之標準作業程序，執行消費者權益保障及風險管

	理，且應定期或不定期稽核所屬員工有無依據標準作業程序執行本合約相關作業。
6. 雲端服務業者就受託事項範圍，同意主管機關及中央銀行得取得相關資料或報告，及進行金融檢查，或得命令其於限期內提供相關資料或報告，金融機構得視需要自行或委託專業第三人辦理查核作業。	乙方就受委託事項範圍，同意配合甲方之主管機關或其指定查核單位得取得相關資料或報告及進行金融檢查，或得命令其於限期內提供相關資料或報告。 甲方得以本合約作為行使查核權之依據，乙方同意甲方得自行或委託專業第三人對其委託事項範圍辦理查核作業，乙方將配合甲方查核作業，提供必要之協助。
7. 雲端服務業者不得以金融機構名義辦理受託處理事項，包含對外廣告或進行不實廣告。	乙方未經甲方事先書面授權，對外不得以甲方名義辦理本合約約定事項，亦不得以甲方名義對外廣告或進行不實廣告。
8. 金融機構與雲端服務業者應約定消費者爭端解決機制，包括解決時程、程序及補救措施。	甲方使用本雲端服務期間，乙方應提供甲方反應意見之聯絡管道等消費者爭端解決機制，乙方亦得依甲方公告之服務水準協議所載有關解決時程、程序及補救措施內容請求基於消費者保障之權益。
9. 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。	乙方對本合約若有履行困難之虞或乙方對受委託事項有重大異常或缺失，應於相關情事發生時主動通知甲方。 前述通報包括對乙方影響之資訊安全事件，且乙方應配合甲方通報主管機關或通知當事人之程序，並提供必要之書面說明或協助。
10. 金融機構應於契約中要求受委託機構非經金融機構書面同意，不得將作業複委託。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。複委託契約應準用本條規定訂定之。	本合約允許複委託之情形僅限於以下情形，其他非經甲方同意，乙方不得將作業複委託： （明訂複委託之範圍、限制或條件）
11. 如涉及重大性消費金融業務資訊系統委託至境外雲端服務業者處理，應確保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，原雲端服務業者對系統遷移、資料處理之義務，及遷移過程中雲端服務業者對服務中斷之賠償責任。	（涉及重大性消費金融業務資訊系統委託至境外雲端服務業者處理者適用） 本合約期間甲方需將作業移轉至其他雲端服務業者或移回甲方之情況時，乙方於合理的範圍內提供甲方有關系統遷移與資料處理之必要協助。 前述遷移過程若合約尚未中止，乙方應持續遵守服務水準協議等要求。

「協力事項」為法規要求金融機構對雲端服務業者之監督管理責任，金融機構可參考下表約定相關事項：

建議約定項目	參考範例
1. 金融機構保有存放於雲端資料所有權與其指定資料處理地及其儲存地之權利。除非得到金融機構同意，雲端服務業者不得變更金融機構資料存放位置。	甲方保有存放於雲端資料所有權與指定資料處理地及其儲存地之權利，如未經甲方事前同意，乙方無權任意變更甲方之資料存放位置或使用甲方之資料。
2. 雲端服務業者應遵守資料存放雲端位置之相應司法管轄區之資料保護法規。	乙方應遵守雲端資料儲存地相應司法管轄區之資料保護法規。
3. 雲端服務業者違反安全與保密協議時之賠償責任（賠償範圍由雙方依雙方商業協議約定之）。	乙方如有違反我國法令或雙方所約定之安全與保密義務之情形時，甲方得終止委託、要求乙方限期改善、或暫停委託直至確認乙方完成改善為止。 乙方及其受僱人如因違反安全與保密協議致生甲方損害時，甲方並得就前開損害請求損害賠償，包含甲方如因而受行政裁罰及一切其他支出（包括但不限於：律師酬金、訴訟費用等）。
4. 在以下情況下金融機構有權終止契約或協議： (a) 依主管機關通知得終止或解除契約； (b) 雲端服務業者所有權發生變更； (c) 雲端服務業者破產或清算； (d) 雲端服務業者進入受監管或司法管理狀態； (e) 雲端服務業者發生安全或機密性違規； (f) 雲端服務業者履行契約或協議能力顯有困難之虞者。	本合約期間內，如發生不可歸責於甲方之事由致不得繼續履行本合約或使用本合約之服務專案時，甲方得不經預告立即通知乙方終止或解除本合約之全部或一部份，包含： (a) 甲方因法令變更、主管機關命令終止或解除、業務需求改變等原因，須提前終止或解除本合約時。 (b) 乙方違反本合約之條款或未能履行本合約所規定之條款； (c) 乙方重整、聲請或被聲請重整。 (d) 乙方解散或決議解散或被命令或裁定解散。 (e) 乙方合併或決議合併、破產或聲請或被聲請宣告破產。 (f) 乙方主要資產被查封，無法履行本合約，或有相當事實足認有發生履行合約之能力顯有困難之虞者。
5. 終止委外契約時，雲端服務業者允許金融機構提取資料之相關責任，並在退出過程中提供合理及必要之協助。包含當金融機構與雲端服務業者已終止契約或協議造成金融機構無法直接存取資料的情況下，金融機構可確保雲端服務業者已包含	任一方依本合約約定終止或解除本合約後，雙方應無條件配合對方之要求完成對方資產之盤點及返還（持有對方資產者適用）。甲方存放於雲端之資料應由甲方自行處理，乙方承諾於合約終止時，提供甲方服務退出必要之協助。 前項協助包含若當甲方已終止合約致無

於資料刪除流程，相關流程亦經過檢視。	法直接存取資料時，乙方承諾執行資料刪除作業，與在合理範圍內協助甲方辦理退出計畫之測試與執行。

上述建議範本，僅供擬約時參考，金融機構與雲端服務業者可依實務需求調整契約，金融機構應與雲端服務業者依服務模式及權責劃分對實際協議條款內容作出約定。

針對「依法應記載事項」若因實務限制無法滿足時，金融機構可先評估該條款未約定是否可能存在對於其客戶權益與業務運作之風險，若實際應用情境不適用者，則判斷為無顯著影響則無須採行替代措施。若為是否，建議應依據評估結果針對風險較高之項目規劃替代措施，以確保金融機構對雲端服務業者之最終監督義務之執行。

實務建議如下，以在無法透過合約約定的情況下，有效地管理和應對重大異常或缺失。：

(a) 建立明確的溝通機制：建立內部或外部的投訴管道，以及時處理投訴並採取必要的行動，並要求雲端服務業者在發現重大異常或缺失時立即通知金融機構；
(b) 委任獨立監督方：包含委任獨立第三方之監督方、第三方中介機構，以進行監督及仲裁；
(c) 調整定期監督和審查頻率：建立定期監督和審查雲端服務業者的機制，針對雲端服務業者進行定期檢查和評估；
(d) 定期衡量風險之改變：建立完善的風險管理計劃，包括評估、監控和應對異常情況的策略和程序。

四、定期審查與服務監督

目的

為確保金融機構使用之服務維持議定標準。

參考指引

金融機構依風險評估結果建立定期審查與服務監督機制，以確保對第三方進行有效與及時之監督。視使用雲端服務種類之風險考量以下控管：

(a) 指派專責單位或人員負責監督雲端服務業者。
(b) 審查雲端服務水準協議達成情形。
(c) 由雲端服務業者所負責資訊底層架構之查核，可定期審查雲端服務業者出具之資訊安全國際標準認證報告，並追蹤雲端服務業者是否及時修補評估報告中確定為重要的任何威脅、風險或安全議題。
(d) 定義並定期審查雲端服務關鍵績效與風險指標。
(e) 審查對客戶資訊之使用、處理及控管情形
(f) 審查雲端契約或協議與服務水準，確保整體雲端服務有效性與符合相關規範之目的。

(g) 審查雲端服務變更管理控制，包含重大系統變更紀錄、基礎映像檔變更紀錄等，確保變更管理程序之落實。

服務水準協議（Service Level Agreement, SLA）是雲端服務業者與服務使用者對於雲端服務可用性所達成之協議。一般而言，若雲端服務業無法依協議達到承諾的服務水準，會依協議計算且提供給使用者特定的財務承諾，該等承諾亦可能因未達服務水準之程度而有所差異。

常見的雲端服務 SLA 為 99.9%，代表的意義為雲端服務無法使用之時間（Downtime），即時間區間內預期可能發生的總中斷時間的百分比，若以「99.9%」的可用性為例，表示雲端服務業者每年合計可能發生之停機時間容許值為 8.76 小時（如下表）。通常雲端服務業者所承諾的 SLA 內容幾乎都是以服務提供角度所訂定，因此若金融機構期望獲得更高之服務水準時，可考量採用符合需求的服務選項、依需求與雲端服務業者協商更合適之可用性承諾或通過高可用性的架構規劃與設計以達到 SLA 需求，並考量具備公開透明可提供雲端服務運行狀態資訊之雲端服務業者，以得到合乎期待之服務。

服務水準	每年停機時間	每月停機時間	每週停機時間
99%	87.6 小時	7.2 小時	100.8 分鐘
99.9%	8.76 小時	43.2 分鐘	10.08 分鐘
99.95%	4.38 小時	21.6 分鐘	5.04 分鐘
99.99%	52.56 分鐘	4.32 分鐘	1.01 分鐘
99.999%	5.256 分鐘	25.92 秒	6.048 秒

第四章、 雲端人才培訓

一、培訓對象

目的

確保培訓計畫依據金融機構不同角色考量，包含適用新進人員或人員調動至不同要求之新職位或角色人員時之培訓要求。

參考指引

(a) 針對董事會制定包含風險意識培訓之培訓規劃，提升對於雲端使用所涉及風險的認識，並加深對風險管理實踐的理解。
(b) 針對要求特定技能及專業知識之執行團隊（例如：雲端軟體開發人員），制定識別、準備及實作金融機構內採用雲端服務之適切培訓規劃。
(c) 針對負責雲端之部門、團隊及涉及雲端服務相關人員制定相關培訓規劃，確保人員能夠理解和管理金融機構中採用不同雲端服務的技術技能與風險認知。
(d) 針對所有人員制定全面的資訊科技安全意識培訓計畫，確保瞭解有關使用和存取資訊資產的相關法律、法規和指南。

二、培訓內容

目的

確保相關人員具備所需之專業知識與技能，以理解且管理採用雲端之風險，並履行其責任。

參考指引

(a) 以工作職掌或角色進行培訓及證照考取之規劃，確保為雲端使用者提供對應之培訓內容。
(b) 培訓對象與培訓內容可參考以下表格做為制定培訓規劃之基礎：

培訓對象	培訓內容	建議培訓重點
治理及管理階層	著重於瞭解雲端資源最適採用方法，以及管理採用不同雲端服務之風險意識與專業知識。	1. 準備階段：雲端服務基礎概觀。 2. 發展/優化階段：雲端安全性與合規性。
服務監管與使用人員	著重於整體資訊安全意識及其影響、金融機構的資訊科技安全政策和標準，以及個人保護資訊資產的責任，以確保人員瞭解有關使用和	1. 準備階段：雲端服務資源基礎操作和管理。 2. 發展/優化階段：雲

	存取資訊資產的相關法律、法規與規範要求。	端安全性與合規性。
建置及維運執行團隊	著重於應用不同雲端工具之能力、實踐雲端遷移之專業能力，以及雲端安全性與合規性。	1. 準備階段：雲端架構設計。 2. 發展階段：雲端解決方案配置和管理 3. 優化階段：雲端計算與成本管理、雲端自動化設計。

(c) 雲端原廠專業課程及證照訓練之安排，可幫助金融機構初階、中階與專業人員等不同職業領域，因此金融機構可考量人員之角色與責任，從基礎認知到深度專業，以系列課程與證照進行學習。

(d) 可考量透過實體或虛擬管道進行培訓，以保持知識之更新（例如： 課堂教學、遠距學習、網路課程、自訂進度、由專家指導在職訓練、輪調活動）。

(e) 培訓規劃可定期舉行，若內部人員缺少所需技能，應即時採取相關行動並獲取該等技能。

(f) 培訓活動結束時，可就評鑑人員之理解，測試培訓計畫的有效性。

第五章、 雲端服務資安控管

一、加密與金鑰管理

目的

確保金融機構使用雲端服務作業時遵循之加密及金鑰管理機制。

參考指引

金融機構為以風險基礎方法和所採用之雲端服務模式決定其加密與金鑰管理執行強度與項目：

基本項目

(a) 傳輸客戶資料或機敏資料時，採行傳輸加密機制等保護措施，實務作法參考如下：

(1) Azure：使用 ExpressRoute 或站對站虛擬私人網路（VPN ）連線建立私人連線，並使用 HTTPS（TLS 1.2 以上）之通訊協定加密由金融機構向雲端環境之資料傳輸通道，如：Azure Blob Storage 之存取，以確保資料在雲端環境與金融機構端之間傳輸的安全性。

(2) AWS：透過 AWS Virtual Private Cloud（VPC）提供的通道加密技術，如 Site-to-site VPN 連接或 AWS Direct Connect，以實現傳輸安全保護。同時，採用 HTTPS（TLS 1.2 以上） 通訊協定以加密保護金融機構對於 AWS 服務的存取操作及資料傳輸，如：Amazon S3 的服務操作及資料存取。

(3) GCP：使用 Google Cloud VPN 或 Cloud Interconnect 確保資料金融機構與雲端環境之間的傳輸安全。並可通過 Organization Policy 限制僅能使用高強度（TLS 1.2 以上）的通訊加密協定，加密所有由金融機構上傳至雲端服務的資料，如：Google Cloud Storage。

(b) 儲存客戶資料或機敏資料時，採行靜態加密或代碼化等有效保護措施，實務作法參考如下：

(1) Azure：可採用 Azure Storage 服務中的伺服器端加密（SSE），自動加密雲端儲存資料，並利用符合 FIPS 140-2 Level 3 等級的 Azure Key Vault Managed HSM 管理與保護加密金鑰。Azure 支援用戶自行攜帶自己的加密鍵值進行 Azure Storage 服務內資料加密，亦可選擇以自行攜帶之鍵值由硬體加密（HSM） 之 Azure Key Vault 來管理與保護加密金鑰。

(2) AWS：使用 Amazon S3 的伺服器端加密（SSE）功能自動加密儲存於雲端境的資料。同時運用符合 FIPS 140-2 Level 3 等級的 AWS Key Management Service （KMS），透過硬體安全模組（HSM）落實加密金鑰建立、管理和控制機制，以保護金鑰的機密性和完整性。

(3) GCP：在 Google Cloud Storage 中所有儲存的資料均可使用 Customer-supplied encryption key（CSEK）模式或 Customer managed encryption key（CMEK）

金鑰針對伺服器磁碟端進行加密保護。

(c) 加密與金鑰管理政策和程序，涵蓋項目包含：
   (1) 加密工具之管控措施；
   (2) 完整金鑰生命週期（生成、儲存、使用、撤銷、到期、更新）；
   (3) 備份加密金鑰；
   (4) 避免金鑰洩露之方法；
   (5) 金鑰更換程序及時機（包含如發現金鑰暴露的風險時）；
   (6) 金鑰管理權限，符合職責分離之原則。

(d) 使用高安全性演算法（如 AES 256 以上），依用途產生自有之加密金鑰，並評估加解密環境是否符合金融機構設定的安全水準。

進階項目

(a) 評估使用自行管理金鑰（Bring Your Own Key, BYOK）和自行管理加密（Bring Your Own Encryption, BYOE），以提升對金鑰的控制權。
   (1) 自行管理金鑰：金融機構選擇使用自有金鑰進行加密，而不是使用雲端服務業者產生的預設金鑰。
   (2) 自行管理加密：金融機構選擇於應用層使用自己的加密解決方案，而非僅依賴雲端服務業者提供的加密功能。

(b) 金鑰建議採用符合第三方認證 FIPS 140-2 Level 3 以上的硬體安全模組（Hardware Security Module, HSM）為優先，並限制明文匯出功能及要求經存取權限控管。金融機構可依風險評估採用地端硬體安全模組作業。

(c) 加密工具及金鑰可考量儲存於隔離且安全的網路環境，限制存取來源，包含不能從雲端服務業者其他客戶使用的網路或日常員工存取的網路存取。

二、資料安全與隱私管理

目的

確保於雲端環境中處理資料之過程遵守相關法令法規要求，並保護資料之機密性和完整性。

參考指引

金融機構應以風險基礎方法和所採用之雲端服務模式決定其資料安全與隱私管理執行強度與項目：

基本項目

(a) 確保雲端服務業者及金融機構依共同責任模型建立資料銷毀、資料遺失和資料外洩通報管理程序，依據雲端服務使用之目的控管雲端服務存取方式。

(b) 確保遵守客戶資料保密的相關法規要求。

(c) 瞭解雲端服務業者用於資料銷毀的過程。

(d) 為確保資料安全，使用具有高安全性的加密演算法，並避免使用已知不安全的網路協定及版本或採取妥適之補償性控制。

(e) 為確保客戶隱私資料之保護，金融機構可評估參考 ISO/CNS 29100「資訊技術-安全技術-隱私權框架」、ISO/CNS 29191「資訊技術-安全技術-部分匿名及部份去連結鑒別之要求事項」，以及 ISO/CNS 20889「隱私增強資料去識別化術語與技術分類」採行妥適之代碼化或去識別化技術，以有效提升隱私保護能力。

進階項目

(a) 避免使用營運資料執行雲端服務測試與驗證。

(b) 監控與定期查核雲端資料使用情形，預防客戶隱私及營運機密外洩。

(c) 如由地端透過傳輸服務或相關工具將資料上傳至雲端環境時，應使用安全控管措施，如：身分識別與存取控制或 HMAC-SHA 簽章等安全性機制。

(1) Azure：使用 Azure File Sync 服務來同步地端檔案伺服器與 Azure Files 共享。此方法允許在保持地端存取的同時，利用 Azure 的全球網路將資料安全上傳至雲端。在傳輸過程中，Azure 會自動加密資料，Microsoft Entra ID (舊名 Azure AD) 和角色型訪問控制(Azure Role-Based Access Control, RBAC) 功能，確保只有經過授權認證的用戶才能存取或傳輸資料。Microsoft Entra ID 和 RBAC 提供豐富的存取控制策略和細粒度的權限管理，能夠實施基於角色的存取控制和最小權限原則。此外，透過設定網路安全性群組（NSG）和相關防火牆服務，可以對存取來源的 IP 範圍進行限制，並實施對內外網的存取控制，從而支持零信任安全模型的實施。而 Microsoft Entra ID 身分驗證所使用之簽章採用 HMAC-SHA256。

(2) AWS：使用 AWS Storage Gateway、DataSync 等服務將檔案傳輸至雲端環境，除利用 HTTPS （TLS 1.2 以上） 加密保護網路傳輸資料內容，並將資料儲存於 已啟用伺服器端加密（SSE）之 Amazon S3 或 FSX 等儲存服務中，並結合 AWS Identity and Access Management（IAM）確保只有授權者可存取或傳輸資料。

(3) GCP：使用 Google Cloud Storage Transfer Service 將大量資料上傳至 Google Cloud Storage 時，提供資料加密傳輸與加密儲存之保護外，同時可配置 Identity and Access Management（IAM）策略，以確保只有授權者可執行資料傳輸。此外 GCP 提供 VPC-SC 的應用程式介面（ Application Programming Interface, API）服務執行檢查作業，以限制資料僅能由指定之 IP 位置或裝置執行上傳，以實現零信任防護。

三、身分識別與存取控制

目的

確保雲端環境中之資源和資料受適當保護，且僅有授權之人員可以存取必要資源和

資料。

參考指引

金融機構以風險基礎方法和所採用之雲端服務模式決定其身分識別與存取控制執行強度與項目：

基本項目

(a) 針對有調整雲端服務組態設定權限之員工及擁有特權帳號之員工實施多因子身分驗證。

(b) 變更預設存取憑證並限制對金融機構存放於雲端之資料及資源存取權限。

(c) 對雲端服務業者提供的應用程式介面（API）以及由金融機構建置和實施的 API 設定適當存取權限。

(d) 確保登入憑證與存取管理系統之安全性，並與其雲端服務業者的控制保持一致，參考雲端服務業者所提供之設置及最佳實務建議：

(1) 登入憑證：多重要素驗證（ Multi-Factor Authentication, MFA）、密碼複雜度、服務帳號金鑰管理、整合 OpenID Connect 或輕型目錄存取協定（Lightweight Directory Access Protocol, LDAP）等單一登入（SSO）機制。

(2) 存取管理系統：在非必要的情況避免人員對於資料的直接存取、最小權限、以角色為基礎之存取管理政策、保留稽核軌跡（Audit Logs）與監控存取行為等。

(3) 基於資料之機密性建立存取授權之限制，如：多因子認證、存取時間或存取位置等。

四、稽核軌跡與監控

目的

金融機構使用雲端服務時負有監督和記錄之責任，以確保雲端環境之安全性、合規性及服務可用性。

參考指引

金融機構應以風險基礎方法和所採用之雲端服務模式決定其稽核軌跡與監控執行強度與項目：

基本項目

(a) 留存金融機構人員對於雲端服務平台操作之稽核軌跡，稽核軌跡至少保留六個月。

(b) 根據 SLA 對關鍵服務進行監控，並由金融機構定期審查，以識別使用異常。若是在複合 SLA 的情況下，即為涉及多個供應鏈層級（tier）及條款要求，以因應複雜之業務需求或雲端服務業者之多個服務，金融機構應加強其執行強度。

(c) 金融機構為監控和審查主機或服務容量使用率，並針對可能有風險之主機或服

務進行確認。

(d) 針對雲端安全事件制定監控與分析之關聯規則，例如：異常資料下載行為、異常權限變更、異常登入位置警報等。

(e) 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。

(f) 啟用雲端平台環境中儲存空間的加密功能，可使用雲端服務業者預設之金鑰，或使用金融機構在雲端平台上建立之金鑰。

進階項目

(a) 針對已蒐集之稽核軌跡與監控資料，考量集中管理，即不建議與地端資料分開管理，以確保完整性和一致性，並避免遺漏或重複之情形。因應人力、技術學習曲線、成本等，可考量依發展期程及雲服務複雜度實施不同作法：

(1) 採用單一雲平台：除留存在雲端環境一份原有的稽核軌跡並使用其原生地監控與告警功能之外，建議同時整合地端共用地端的稽核軌跡與監控管理機制。雲端平台之應用系統的監控機制，建議仍以雲原生工具為優先選擇。

(2) 如採用多雲平台者，可選擇適當的環境中建立一致的整體監控機制進行所有環境的統一監控及管理。因複雜度極高，建議熟悉各雲平台的技術後，再選定具體方案。

五、基礎架構安全

目的

為確保使用服務時負有保護其基礎架構安全之責任，遵循基礎架構安全之規定。

參考指引

金融機構以風險基礎方法和所採用之雲端服務模式決定其基礎架構安全執行強度與項目：

基本項目

(a) 建置基礎架構、設定環境安全性和應用程式維運之管理或控制之角色，應實施職責分離，以避免過度授權。

(b) 集中管理基礎架構變更的權限，並密切監控環境配置以防止未經授權的變更。

(c) 監視營運環境之變更，並觸發自動警報以向安全或基礎架構團隊發出警報。

六、威脅與弱點管理

目的

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，以確保資訊資產安全性和系統正常運作，並定期進行弱點掃描及定期評估網路安全

防禦措施之有效性。

參考指引

金融機構以風險基礎方法和所採用之雲端服務模式決定其威脅與弱點管理執行強度與項目：

基本項目

(a) 建立威脅與弱點檢測及管理流程，可考量：
  (1) 在雲端和金融機構的本地環境之間以及入口或出口點實施控制，以減輕此類威脅。
  (2) 持續蒐集與關注資安（包含雲端）相關威脅與弱點，並評估相關威脅與弱點對金融機構之影響。蒐集來源可包含 TW-Cert、FISAC、主管機關發布之警訊、供應商等。

(b) 確保雲端服務業者有定期評估系統相關威脅與風險、執行安全檢測並及時對弱點與事件進行處置。

(c) 採 IaaS 與 PaaS 部署者，可定期對應用程式及其運行環境進行弱點掃描與修復，以降低安全風險。其他項目可藉由評估雲端服務業者提供之弱點及威脅評估結果，並評估高風險以上之弱點是否可能影響金融機構資訊環境之安全性。

進階項目

(a) 網路存取和安全設定採取預防措施，例如：配置防火牆、邊界保護、東西向流量監控、配置檢測及防止惡意流量及活動工具、網路服務強化設定。

(b) 除一般威脅防護控制，如入侵偵測系統（Intrusion Detection System, IDS）、入侵防禦系統（Intrusion Prevention System, IPS），考量在安全網段中實施進階威脅防護控制，如持續性威脅（Advanced Persistent Threat, APT）防禦策略，保護對雲端環境的存取。

(c) 針對資料洩露及跨服務攻擊進行管控，以確保不同服務及用戶之間的資源能夠得到適當的隔離。

第六章、 雲端服務維運控管

一、資訊資產管理

目的

確保金融機構在雲端環境中之資訊資產有適當之控管，以期於雲端技術或內外環境發生重大異動時，能確保雲端資訊資產之機密性、完整性與可用性

參考指引

金融機構對於雲端環境中與業務相關之雲端資訊資產，負有管理之權責。

基本項目

(a) 建立雲端資訊資產盤點及分級管理機制，識別雲端服務中，金融機構所屬之相關資訊資產，包含運算資源、軟體、網路、儲存空間及衍生資料，其中衍生資料包括雲端運算過程中所產生的資料，如：系統監控紀錄、統計分析資料等。

(b) 針對雲端資訊資產之類別及安全分級採取妥適之管控，以防止資產遭受破壞而影響金融機構業務之運行。

(c) 指派資訊資產擁有者、保管者及使用者，依角色授予資產之存取權限，以確保只有經授權的使用者能夠存取特定資產。

(d) 定期檢視資產清單及存取控制政策，以確保資訊資產管理的有效性和安全控制的適切性。

(e) 定期對資訊資產進行風險評估，識別可能的安全威脅，並採取相應的風險降低措施。

(f) 資訊資產生命週期結束，應確保經刪除或銷毀的敏感資料無法回復以避免資訊外洩。

進階項目

(a) 建立自動化資產管理機制，以主動識別及管理雲端資訊產使用情形。

二、服務部署與監控

目的

確保金融機構在雲端環境中之系統及應用程式安全性、可用性、可靠性及運行效能，並透過監控工具及時發現及解決問題。

參考指引

確保金融機構使用雲端資源部署應用服務，能夠針對各種部署模式的安全需求進行管理。

基本項目

(a) IaaS 部署時應注意事項：
   (1) 透過虛擬私人網路（VPN）、子網路（subnets）、及防火牆規則等資源，強化應用程式的保護。
   (2) 根據業務需求分配適當的資源，並根據需求進行適時調整，以優化資源使用。
   (3) 管理虛擬機器映像檔的安全性，並定期進行升級或更新作業系統，以保障系統安全。
   (4) 制定虛擬機之遷移政策與計畫，以確保環境移轉時之資料完整性、系統安全性及最小化服務中斷時間。

(b) PaaS 部署時應注意事項：
   (1) 應對 PaaS 平台提供的資通系統基礎環境介面（Application Infrastructure Interfaces）進行評估，以確保其能夠滿足平台互通性及擴展性需求。
   (2) 開發團隊應評估程式語言與開發工具，以確保開發品質及可維護性。
   (3) 開發團隊應對組件（Component）執行單元及整合測試，以確保在編譯階段的軟體函式庫（Software library）與執行階段的呼叫函式都能夠符合預期的功能和性能。
   (4) 應用程式應具備必要的通訊安全功能（如：傳輸加密、端點安全性驗證、網路層安全策略），以確保資料及通訊安全。
   (5) 執行應用程式版本控制及審查，以確保應用程式安全性。
   (6) 使用持續整合（CI）和持續部署（CD）工具，以滿足自動化測試及部署需求。
   (7) 將機敏資訊、環境變數與程式碼分離配置。

(c) SaaS 部署時應注意事項：
   (1) 確保只有經過授權的使用者能夠存取 SaaS 應用程式，並採用最小權限原則限制使用者能夠存取的資源及資料。
   (2) 依據安全基準進行 SaaS 應用程式配置，防止配置錯誤導致的安全漏洞。
   評估並監控 SaaS 服務的安全措施和合規性狀態，確保雲服務供應商遵守國際與產業安全標準。

進階項目

(a) 建立自動化部署流程，確保不同環境連續部署的可靠及一致性，以降低因人為操作錯誤。

(b) 建立自動化監控機制，確保對雲端服務的部署、運作狀態和效能具有透明度和可見性。

三、變更管理與組態管理

目的

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對其組態進行管理。

參考指引

金融機構以風險基礎方法和所採用之雲端服務模式決定其變更管理與組態安全執行強度與項目：

基本項目

(a) 依據雲服務提供者和雲服務使用者間的變更管理責任協議，建立組態設定管理機制，以確保系統的穩定性及追蹤能力，內容包括：
   (1) 建立組態變更流程，以確保組態變更可能的風險均經詳細評估。
   (2) IaaS 部署時參照雲端服務提供者或產業公開的指引（如政府組態基準、金融業系統組態基準、CIS Benchmarks）所提供的組態配置建議進行管理，以確保虛擬機、儲存與網路配置符合安全最佳實踐，以保障基礎架構的安全。
   (3) 記錄組態變更，如變更的時間、變更前後的組態設定、變更執行者及變更原因，並妥善存留組態變更記錄。
   (4) 建立組態監控機制，確保組態設定與既定的標準模板保持一致，並及時識別並處理任何偏差或未經授權的變更，以保障系統安全及營運穩定。

(b) 確保只有獲得授權的人員才能進行組態設定的變更，以防止任何未經授權的存取或修改，保障系統的安全與穩定。

進階項目

(a) 評估採用基礎架構即程式碼（Infrastructure as Code）機制，以實現變更的版控、變更管理、核准流程、自動部署及便於回復或遷移等操作。

(b) 建立變更回復（Rollback）機制，以便在變更失敗或錯誤時能夠快速還原至先前的已知良好狀態。

四、應用系統開發與維護

目的

確保金融機構在雲端環境中之雲端應用系統生命週期相關管理規則和程序。

參考指引

金融機構實施明確的雲端應用系統生命週期管理政策和流程，包括系統開發、測試、部署、監控、更新和退役等方面的規則。在雲端應用系統的生命週期各階段進行風險估及管理，以符合相關的法規和合規性要求。

基本項目

(a) 落實應用需求管理，以確保應用系統開發符合業務目標、使用者需求與安全規範要求（如：電子銀行業務安全控管作業基準、PCI DSS、GDPR、ISO 與 SOC

等）。

(b) 依循安全設計原則，於設計階段即應考慮資料保護與隱私問題，預防潛在安全風險。

(c) 定期對程式碼進行檢測，識別和修補安全漏洞，以有效提高程式碼的品質和安全性。

(d) 透過完整的測試流程（如單元測試、整合測試、系統測試及安全測試），透過多維度的測試以確保應用系統的穩定性與安全性。

(e) 透過正式的變更管理流程控制風險，以確保任何修改或更新均不會對系統穩定性和安全性造成負面影響。

(f) 使用版本控制系統管理程式碼版本，以促進團隊協作並追踪程式碼的變更。

(g) 採用 DevSecOps 方法，確保在部署過程中執行有效的安全措施，保障生產環境不受潛在威脅侵害。

五、資源管理

目的

確保金融機構在雲端環境中資源有效運用，並符合安全性與成本效益。

參考指引

金融機構檢核各類雲端服務（例如 virtual private network、container、virtual machine 等）之申請、授權、啟用之妥適性，並訂定管控機制，以維持雲端資源之有效運用。

基本項目

(a) 依據現行業務需求及使用量推估，制定資源規劃策略（如硬體、軟體、人力及財務等資源），以確保有足夠資源達成業務目標。

(b) 監控並及時辨識及處理系統效能問題，以確保系統之穩定性與可用性。

(c) 設定監控閥值以監控資源使用情況，以便及時調整配置或進行故障排查，確保系統穩定運行。

(d) 定期對資源進行評估和更新，包括硬體、軟體及其他關鍵技術，以確保業務持續運用最新和最高效的技術方案。

(e) 依據退場策略制定雲端服務終止時處理資源及資料之方法。

進階項目

(a) 實施自動化監控和警報系統，即時追蹤資源狀態和服務指標，確保在出現異常時迅速執行應對措施。

第七章、 雲端服務查核

一、查核執行方式

目的

為確保使用服務符合金融機構的安全策略和標準以及避免其違反任何法律、法規或契約義務，可設立定期查核時間與奠定查核模式的標準。

參考指引

金融機構以「金融機構作業委託他人處理內部作業制度及程序辦法」要求及其使用的雲端服務模式決定合適的查核內容、時間及方式。

(a) 查核頻率可參考以下表格決定：

分級	查核頻率
雲端委外作業涉及重大性消費金融業務資訊系統委託至境外處理	每年至少辦理一次一般性查核及一次專案查核
具重大性之境外雲端委外作業	每年至少辦理一次查核
不具重大性之境外雲端委外作業	每兩年辦理一次查核或依據組織資源決定查核頻率
境內雲端委外作業	

(b) 金融機構為定期審查其資訊系統的設計及架構安全，評估潛在弱點及威脅可使用靜態（如白箱測試）、動態（如黑箱測試）或分散式負載測試，執行安全評估檢視。

(c) 鑒於雲端科技具相當專業複雜度，金融機構對受託機構進行查核，可自行或與其他金融機構（不限業別、不限同一家金控下之金融機構）聯合委託具資訊專業之獨立第三人查核為之。

(d) 金融機構指定窗口擔任金融機構、雲端服務業者、及查核人員的統一聯絡窗口，以溝通安排查核行程。

(e) 金融機構確認雲端服務業者有針對查核後所發現之問題事項在合理時間範圍內作出相對應的解決方案。

二、查核人員資格

目的

確保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。

參考指引

金融機構為評估查核人員之獨立性、資格與專業性。資格建議可包含下列任一經驗或證照：

(a) 具備執行查核所需之專業知識和技能，可要求人員具備雲端安全相關證照，如：
  (1) 資訊安全及雲端國際標準證照，如：ISO 27001、ISO 27017、CCSP、CCSK、CISSP 等。
  (2) 雲端平台基礎專業技術證照，如：AWS CCP、Azure AZ-900、GCP Cloud Digital Leader 等。
  (3) 雲端平台進階專業技術證照，如：AWS Certified Security Specialty、Azure AZ-500、GCP Professional Cloud Security Engineer 等。
(b) 具備雲端安全查核相關經驗。
(c) 獨立於涉及該委外或負責雲端服務之單位。

三、查核重點項目

目的

於規劃查核項目時，確保金融機構依其使用雲端服務模式之安全性需求差異及責任模型，決定其查核項目。

參考指引

金融機構對雲端服務之查核可以區分為：一、對於由雲端服務業者所負責資訊底層架構之查核，可依雲端服務業者出具之資訊安全國際標準認證報告辦理。二、個別金融機構仍就其各自之委外項目及雲端服務應用情形，依風險基礎方法進行查核並分別出具查核報告。

雲端服務模型大致可區分為基礎架構即服務（IaaS）、平台即服務（PaaS）、軟體即服務（SaaS）三種，基於不同雲端服務模式對安全性有不同要求，例如 IaaS 模式下，金融機構需額外關注基礎設施之安全性， SaaS 模式則需關注應用程式之安全性，而 PaaS 模式則需關注開發之安全性。因此，查核項目可根據所選擇之雲端服務模式進行調整。

對於具重大性之雲端委外服務，金融機構之查核重點項目可包含：

(a) 雲端服務所在機房之實體安全控管機制。
(b) 雲端服務業者處理作業相關之重要系統及控制環節。
(c) 盡職調查過程中雲端服務業者所提供之報告內容。
(d) 雲端平台資料刪除與災難復原流程。
(e) 雲端服務業者之營運持續性控制措施。
(f) 確認雲端服務作業內容執行之妥適性（例如：是否遵循服務水準之要求）及符合本會相關規範（例如：金融機構作業委外使用雲端服務自律規範）及國際資訊安全標準（例如：ISO 27001、ISO 27017）。

於規劃查核項目時，除上述項目，可根據共同責任模型及風險基礎方法考量以下領

域及範圍，金融機構可依國際或產業標準（例如：ISO 27001、ISO 27017、SOC 2）及特定作業委外所涉風險，進行雲端服務委外查核，或參考下列建議選擇與目前所使用之雲端服務項目相關領域及議題進行查核：

領域	**查核項目**
加密及金鑰管理	・ 確認加密金鑰由雲端服務業者或受信任的金鑰管理供應商維護。 ・ 確認具備金鑰管理控制措施，針對其金鑰之產製、傳遞、管理及銷毀等生命週期進行控管。 ・ 確認金鑰設置負責之管理人員，並與雲端服務資訊維運管理人員具備權責分離之設計。 ・ 確認針對傳輸及儲存之資料進行加密，加密強度需符合主管機關法規之要求，以防止資料外洩之威脅。
虛擬化安全	・ 確認實施網路控制措施，以確保資料在營運環境和非營運環境之間的公共雲端部署中保持隔離。 ・ 確認虛擬網路上的網路流量在實體網路上的安全保護設備中受監控（如：入侵防禦系統或防火牆）。 ・ 確認實施資安控制措施（例如：防火牆控制、入侵偵測或深度package分析等），以偵測和及時阻擋異常進入或流出的流量模式（例如：嘗試存取高風險IP、對外進行挖礦、IP/Port掃描等攻擊行為）或阻斷式服務攻擊（DDoS）。
營運持續管理	・ 依金融機構該項雲端作業委外所需的營運韌性，確認雲端服務業者可提供之營運韌性控制（例如：RTO、RPO、MTPD）。 ・ 確認雲端服務具備復原程序，或提供高可用性建置架構。 ・ 確認雲端服務維運人員具備持續營運管理能力、經驗、知識以利進行復原。 ・ 確認於備援或復原情境下具備確保資料之正確性與完整性控制措施。 ・ 確認定期測試雲端服務之營運持續計畫。 ・ 確認雲端服務在無法預料的中斷情況下，確保操作的連續性並持續遵守法規義務。提供及時的通知，告知服務中斷事件及其適當的補救措施。 ・ 確認雲端服務為客戶提供具有地理位置彈性的託管選項。
實體安全	・ 確認雲端服務機房人員進出具備控制措施，若外部人員進入機房需授權之人員陪同，並定期覆核其記錄。 ・ 確認雲端服務機房之空間具備監視器（CCTV）進行監控，且未有死角，其記錄至少需保存適當期間。 ・ 確認雲端服務機房具備環境控制措施，當發生環境異常事件（如：電力異常）會即時告警機房管理人員進行處理。 ・ 確認雲端服務機房具備電力持續營運之機制（如：不斷電系統或是發電機）。

	・ 確認雲端服務機房定期針對電力、消防、空調、監視器等設備進行維護。 ・ 確認雲端服務機房之作業操作區域無法連線網際網路。
威脅與弱點管理	・ 確認所有虛擬操作系統、虛擬網路和防火牆配置層保持最新的安全修補（Security Patch）和系統強化要求（System Hardening）。 ・ 確認弱點掃描和滲透測試之結果，並針對弱點掃描或滲透測試之結果進行修補作業。 ・ 若無法或無須進行修補，確認其進行說明或施以補償性控制措施。
事件監控與數位鑑識	・ 確認具備監視雲端服務資訊維運人員針對所有平台對基礎資源的存取。任何存取具備正當理由並獲得批准。 ・ 確認事件管理流程之有效性，包含資安日誌和事件管理系統，並啟用相關記錄以進行詳細的分析和告警。 ・ 確認提供雲端服務管理日誌、應用程式日誌及系統活動日誌。 ・ 確認雲端服務日誌記錄和監視框架可允許將事件集中收集至特定租戶。 ・ 確認當發生危機事件時，具備通報程序，並能配合金融機構之調查作業進行相關證據保全之作業。
雲端供應鏈管理	・ 確認是否有將雲相關服務複委託給其他供應廠商。 ・ 確認選擇該供應廠商是否有進行盡職調查，如： 公司營運狀況、業務承接能力或是資訊安全控管強度等。 ・ 確認是否針對該供應廠商合約內容包含資訊安全控管相關要求和服務水準。 ・ 確認該供應廠商於雲端服務之相關存取權限是否依循其權責具備妥適性。 ・ 確認是否定期針對該供應廠商進行服務水準之監控，以確保服務之品質。 ・ 確認當發生危機事件時，該供應廠商立即通知以確保事件之掌握與處理。
變更管理	・ 確認具備雲端服務變更管理流程及控制，其包含變更至營運環境之前如何有效地測試和批准變更作業。 ・ 確認相關作業有依據其雲端服務變更管理流程進行，並留存相關記錄。 ・ 確認變更作業已進行評估，以確認其是否具有風險，並針對其風險實施處理因應計畫以防制威脅之發生。 ・ 確認變更作業包含回復機制，以確保其變更異常時回復至正常營運。 ・ 若為重大或緊急變更作業，確認其告知機制，並於變更後完成其程序。
身分辨識和存取管	・ 確認具備結構化角色的存取控制，用來適當地限制特

理	權用戶的權限。 ・ 確認提供使用系統位置的功能來作為身分驗證因素（例如基於IP地址的來源來限制存取）。 ・ 確認為所有存取租戶資料的人員提供資安意識教育訓練，告知相關人員使用雲端之安全操作要求。 ・ 確認訂定雲端存取政策，該政策為雲端服務實施存取控制。包括新用戶存取權限、用戶存取權限的修改和存取權限的撤銷（joiner/mover/leaver controls）、用戶註冊、特權帳戶管理、密碼和用戶密碼管理的使用、對用戶存取權限的定期審核以及外部用戶的身分驗證連接…等內容。 ・ 確認支援雙因子認證來實施身分驗證作業，包括用戶名稱、密碼、OTP等，若採行固定密碼，符合金融機構之密碼原則。
風險治理與管理	・ 確認進行雲端服務之風險評估，並針對超過其風險可接受水準之項目訂定風險改善計畫加以因應。 ・ 確認提供足夠的人力和資源以監督和管理雲端服務並執行正在進行的風險管理活動。 ・ 確認提供雲端服務退出計畫、程序或控制措施，不會因此造成對營運功能和服務提供的不當中斷，以及對法規義務的遵守。 ・ 確認定期檢視其管理職責和雲端服務安全架構。 ・ 確認接受金融機構或其委託第三方及主管機關進行雲端服務之查核作業。
應用程式與 API 安全	・ 確認依據環境及業務的性質，雲端服務的整體開發流程之安全性，如原始碼掃描、安全組態設定、風險評估等。 ・ 確認開發測試環境免於未經授權的取用。 ・ 確認原始碼或其他重要資料（例如：Compiled codes、Libraries 或 Runtime modules）與系統組態設定之控管措施，以確保其機密性和正確性。 ・ 確認前項資料不會被未經授權地在雲端開發測試環境上被移除。 ・ 確認雲端服務發布至營運環境之軟體，於發布前已完成必要之功能及安全測試。 ・ 於合約結束後，確認就金融機構儲存於雲端服務之原始碼或其他相關資料做適當移除。
人員管控安全	・ 確認負責開發和發布解決方案的團隊符合職責分離。 ・ 確認雲端服務業者已要求相關人員同意保密責任。
資料安全	・ 確認使用專用的安全網路來提供管理存取權限給雲端服務基礎架構，而那些基礎架構是和客戶（租戶）生產基礎架構及雲端服務業者共享服務基礎架構分開的。 ・ 確認具有將客戶資料的儲存限制在特定地理區的能力。

	• 確認提供可能會處理資料的地理列表，以及與現有資訊保護措施有關的資訊。 • 確認其雲端服務之資料備份機制，並針對其備份媒體進行資料回存測試以確保其完整性及有效性。

第八章、 雲端服務韌性管理

一、營運衝擊分析

目的

確保雲端服務中斷期間，金融機構之資訊及其他相關聯之系統或服務的回復優先順序及資源分配。

參考指引

營運持續計畫（BCP）係確保營運持續管理及資訊安全管理的關鍵要素，以確保在任何雲端服務中斷期間，皆能維持金融機構的運作目標。而營運持續計畫的基礎為營運衝擊分析（BIA）的結果。金融機構於執行 BIA 的過程中，可考量：

(a) 使用衝擊型式和準則，評估隨著時間推移，由於雲端服務活動中斷而產生的衝擊。

(b) 評估這些衝擊的幅度和期間，並確定指定金融機構上傳至雲端服務之資料或資訊系統連接雲端服務功能的韌性能力和有效性，如 RTO 及復原時間點（ RPO ）。

(c) 透過 BIA 確定支援優先活動所需的資源，同時確定這些資源的韌性能力和有效性，如 RTO 及 RPO。

二、雲端服務之資訊安全事件通報與管理機制

目的

建立及時、一致及有效事件通報機制。

參考指引

雲端服務之資訊安全事件通報與管理機制包含定義人員角色和職責，並與金融機構內外部相關單位進行有效溝通。

雲端服務之資訊安全事件通報機制可考慮以下幾點：

(a) 建立一個通報雲端服務之資訊安全事件的管道；

(b) 建立雲端服務之資訊安全事件管理程序，包括管理、記錄、檢測、分類、定義優先順序、分析、溝通和協調相關單位；

(c) 建立雲端服務之資訊安全事件回應流程，以提供金融機構評估、回應和學習雲端服務之資訊安全事件的能力；

(d) 金融機構應只允許有關人員處理雲端服務之資訊安全事件。並向此類人員提供相關處理程序文件且定期舉行相關教育訓練。

(e) 金融機構所有員工和雲端服務使用者意識到其有責任在發現雲端服務之資訊安全事件時立即通報，以防止或盡量減少雲端服務之資訊安全事件的影響。且金

融機構為向員工和雲端服務使用者提供雲端服務之資訊安全事件通報程序，及通報對象。

(f) 經評斷為重大雲端服務之資訊安全事件之事件立即通報於內部平台和作業中心，使相關人員立即應對。

雲端服務之資訊安全事件管理機制可考慮以下幾點：

(a) 根據構成雲端服務之資訊安全事件的標準評估雲端服務之資訊安全事件；
(b) 監視、檢測、分類、分析和報告雲端服務之資訊安全事件和雲端服務之資訊安全事故（透過人工或自動方式）；
(c) 根據雲端服務之資訊安全事件的類型和類別，管理雲端服務之資訊安全事件；
(d) 與監管部門、外部利益團體、雲端服務業者和客戶等內部和外部相關單位協調；
(e) 紀錄雲端服務之資訊安全事件管理活動；
(f) 處理雲端服務之資訊安全事件證據；
(g) 建立分析根因的程序；

對經常發生之雲端服務之資訊安全事件變成系統問題時，執行減緩措施及處理流程。

三、營運持續計畫

目的

確保雲端服務中斷期間，金融機構之資訊及其他相關聯之系統或服務的可用性。

參考指引

營運持續計畫（BCP）可以由一個或多個解決方案組成，並根據雲端服務特質以制定、實施和測試計畫，以確保滿足所需的雲端服務可用性水準，並符合在關鍵過程中斷或失效後的時限要求。

金融機構可檢視雲端服務業者所提供 BCP 以確保以下事項：

(a) BCP 得以應對、減緩和回應雲端服務中斷之情形，並由具有必要責任、權限和專業能力之人員支援。
(b) 金融機構可透過參閱第三方檢核報告（例如 SOC 2 報告）瞭解雲端服務業者之營運持續計畫。

金融機構可依據雲端服務業者 BCP 之共同責任模型規劃管理金融機構 BCP 因應雲端服務中斷時之回應及復原程序。金融機構考量單點及區域性等雲端服務連線異常之情境，評估雲端服務對於企業營運韌性之影響，以訂定對應備援機制及應變程序，並考量將雲端服務業者通報金融機構之流程納入金融機構營運持續計畫（BCP）中，針對通報及伺服器切換機制進行共同演練。

(a) 金融機構之 BCP 可包括以下雲端服務持續資訊：

(1) 符合營運衝擊分析（BIA）中規定的營運持續要求、目標績效，以及容量規格等。
(2) 資料備份方式及備份地點。
(3) 雲端服務及相關資訊資產之業務復原指標，及復原優先序及相依性。

(b) 金融機構定期進行 BCP 演練或測試。
(c) BCP、演練計畫與測試結果由管理階層核可。
(d) 雲端服務業者可提供就災難復原（Disaster Recovery）與營運持續（Business Continuity）所需要功能，包含提供保存相關關鍵資料庫或紀錄系統之快照等相關功能。

金融機構確保雲端服務業者已針對資通安全事件或天然災害等可能造成雲端服務異常或中斷之事件訂定災難復原計畫（DRP），DRP 可包含如雲端服務業者需切換伺服器導致雲端服務中斷時雲端服務業者通報金融機構之機制。事件類型包含：

(a) 人為或天然災害（如：地震、水災、火災、風災等）。
(b) 地緣政治風險。
(c) 內部控制不良之舞弊案或作業發生重大缺失情事。
(d) 實體安全維護方面（如：機房或設備遭破壞或遭恐嚇等）。
(e) 資通安全事件（如：惡意程式或勒索軟體攻擊等），包含涉及金融機構客戶資料安全事件，或對金融機構及其客戶權益有重大影響者。
(f) 其他可能導致雲端服務業者正常營運之重大財物損失事件。

針對各類可能造成金融機構使用雲端服務中斷或異常之災害情事，金融機構可考量於契約或協議中訂定金融機構與雲端服務業者之營運持續職責。金融機構營運持續之責任包含但不限於，針對使用雲端服務之業務制定人工作業程序或替代作業程序或建立雲端服務備援機制，以確保雲端服務業者未能及時回復雲端服務功能時，保障金融機構業務不中斷。雲端服務業者之營運持續之責任包含但不限於，及時告知金融業者雲端服務功能異常。

四、營運持續計畫之測試或演練

目的

確保營運持續計畫（BCP）規劃及實施有效性，以能於雲端服務中斷期間，有效將金融機構之資訊及其他相聯之系統或服務損失與災害最小化。

參考指引

針對營運持續計畫（BCP）之有效性驗證，金融機構可確保以下事項：

(a) 驗證 BCP 的測試或演練準確性、完整性和回復程序之有效性。
(b) 金融機構為將該通報流程納入金融機構 BCP 中，針對通報機制在情況允許下進行

共同演練。

(c) 參與測試或演練的金融機構與雲端服務業者相關人員，應熟悉 BCP 及演練程序要求，以踐能力。

(d) 依據雲端服務涉及的業務及資訊組件，設計不同測試或演練場景。

五、轉移策略及計畫

目的

確保於雲端服務終止時，有效將金融機構之資訊服務影響最小化。

參考指引

金融機構為確保安全終止與雲端服務業者關係，考量以下事項：

(a) 取消雲端服務業者存取權限；

(b) 妥善處理金融機構資訊；

(c) 雲端服務業者變更時資料可轉移性；

(d) 紀錄管理；

(e) 歸還資產；

(f) 安全處理資訊和其他相關聯之系統或服務；

(g) 持續的保密要求；

金融機構之雲端服務退出計畫可包含事前評估、事中處理與事後管理階段之規劃及後續資料刪除與銷毀紀錄之管理，金融機構刪除相關資料時可考慮以下事項：

(a) 依據業務需求選擇刪除方式（電子覆蓋或加密刪除）；

(b) 紀錄刪除結果；

(c) 使用外部資訊刪除服務時，向刪除服務之業者取得刪除證據。

當金融機構規劃將雲端服務委外作業移轉至其他雲端服務業者或移回金融機構之方案時，可考量雲端服務對金融機構持續營運的潛在影響，擬訂退場計畫各階段辦理事項如下：

階段	退場要項
事前評估	• 評估遷移所需資源退場事前調查。並確認既有資源是否足夠應對遷移過程及未來營運所需。 • 盤點應返還、移轉之資料及資源。 • 規劃暫時性替代工具，以及評估系統遷移或資料遷出之費用。
事中處理	• 進行移轉系統環境部署、測試與導入。 • 搭配雲端服務業者提供之機制進行資料移轉，並進行資料完整性驗證測試。 • 執行使用者測試以蒐集回饋資訊。
事後確認	• 替代方案之工具、系統、服務進行測試、驗證與導入。 • 確認完成系統遷移或資料遷出。

	• 確認及測試移轉後之雲端服務並取得使用者執行回饋意見以持續調整作業流程。

第九章、 其他說明

一、外國銀行在臺分支機構之適用說明

目的

外國銀行在臺分（子）行通常由總（母）行、集團或區域總部統籌辦理雲端服務，包含採用集團自建雲端服務或複委託第三方提供雲端服務之情形，通常皆係依循其總（母）行所訂定之管控措施辦理，惟為符合本國法規之要求，外國銀行在臺分（子）行除就其在臺業務建立妥適內部控制制度及風險管理機制外，針對實務手冊各章要求，建議可衡量國內所負之管理責任及風險調整相關作法。

參考指引

當外國銀行總（母）行受託處理外國銀行在臺分（子）行之資料，總（母）行為處理該資料與雲端服務業者簽訂協議，則屬複委託關係，總（母）行與雲端服務業者簽訂之契約應符合「金融機構作業委託他人處理內部作業制度及程序辦法」之要求。

若外國銀行在臺分（子）行如僅為雲端服務使用單位，未直接管理或負雲端維運之責時，針對雲端服務之管理建議如下：

(a) 可由總（母）行、集團或經其授權之區域總部負責辦理該雲端服務之單位擔任雲端服務專責單位，負責監督雲端服務業者，監督項目可參考本手冊第三章、雲端服務管理架構之四、定期審查與服務監督。外國銀行在臺分（子）行為指派專責人員或單位作為接洽窗口。

(b) 盡職調查及定期審查可援用其總（母）行、總機構或經其授權之區域總部負責統籌辦理並提供相關報告與資料。

(c) 協議約定事宜可由總（母）行、總機構或區域總部負責統籌辦理，契約或協議建議約定項目可參考本手冊第三章、雲端服務管理架構之三、契約與協議。

(d) 雲端人才培訓可考量以使用雲端服務之風險管理作為雲端人才培訓重點。

(e) 雲端服務查核可援用其總（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或其獨立單位查核報告。外國銀行在臺分（子）行為評估援用之查核人員獨立性、資格與專業性，評估方式可參考本手冊第六章、雲端服務查核之二、查核人員資格。

二、雲端委外自律規範適用說明

金融機構對於涉及營業執照所載項目或客戶資訊委外作業涉及雲端服務之範圍，不論其直接委託雲端服務業者，或由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，除非屬金融機構作業委外使用雲端服務之範疇者，皆應遵循「非屬金融機構作業委外使用雲端服務」。

判斷原則如下：

(a) 金融機構是否為本國銀行、外國銀行在臺分行、信用合作社、票券金融公司及信用卡業務機構？

(b) 委外作業是否涉及營業執照所載項目或客戶資訊相關作業？

(c) 是否由雲端服務業者提供資料處理或儲存服務？

前段非屬金融機構作業委外使用雲端服務之範疇，包含以下情境，建議亦可衡量雲端服務之風險執行妥適之風險管理及控管程序：

(a) 市場資訊服務及交易暨通訊平台採用雲端服務平台提供金融機構服務。

(b) 金融機構於雲端建置之環境或資訊系統無涉客戶資訊之儲存或處理者，如：無客戶資訊之開發或測試環境、官方網站、公開資訊網站或下載平台、教育訓練平台。

(c) 金融機構使用雲端服務辦理數位廣告投放作業或辦理數位行銷活動時，未涉及利用直接或間接識別客戶身分者，如以下場景：

  (1) 提供非個人化之廣告投放或活動資訊；

  (2) 利用雲端服務收集瀏覽者的數位軌跡時，未與當事人個人資料進行整合，或採用匿名化蒐集用戶資料；

  (3) 資料由雲端服務業者產生之識別碼，回傳至金融機構進行資料比對；

  (4) 金融機構提供亂數產生、無法直接識別個人之識別碼予雲端服務業者。

(d) 金融機構使用雲端視訊開會軟體及相關之通訊服務工具。

(e) 金融機構就其內部營運或行政事項之作業委外使用雲端服務之數位辦公協作軟體（如：視訊會議工具），但該作業委外並未涉及營業執照所載業務項目。為免爭議，若符合上述情事，即使金融機構之內部營運或行政事項涉及蒐集、處理、利用或國際傳輸金融機構之客戶資料（例如內部郵件內提及金融機構之客戶資料加以傳輸或處理），仍非屬金融機構作業委外使用雲端服務之範疇。

以數位行銷為例，金融機構利用雲端服務收集瀏覽者的數位軌跡時，若未與當事人個人資料進行整合時，而非屬金融機構作業委外使用雲端服務之範疇。金融機構仍應持續關注雲端服務業者對隱私資料保護之要求，包含以下要點：

(a) 金融機構須確保符合個人資料保護法要求，如對資料應用的告知責任與是否應取得當事人同意：

  (1) 金融機構應向個人資料當事人明確告知個人資料使用之目的、範圍、對象及方式；

(2) 金融機構應取得個人資料當事人明確的同意始得使用其資料；
(3) 依據目標受眾定位，僅蒐集、處理與利用必要之資料。

(b) 資料分析與傳輸時，可評估採行代碼化或去識別化等機制保護處理中之資料，以降低資料被識別之風險。
(c) 資料傳輸時，可使用雜湊演算法（SHA256）以確保資料傳輸安全。
(d) 金融機構監測消費者回應與反饋，以即時修正廣告投放策略和行銷活動內容
(e) 活動結束後，或個人資料當事人提出資料刪除請求時，金融機構應協同雲端服務業者刪除其個人資料。

三、個人資料去識別化說明

所謂個人資料包含任何可以直接或間接識別出個人的資料，皆屬於個人資料。所謂直接識別的個資，就是單憑該資料就足以識別出特定個人，例如身分證號碼、護照號碼、指紋等；而間接識別資料依個資法施行細則第 3 條規定，係指保有該資料之公務或非公務機關僅以該資料不能直接識別，須與其他資料對照、組合、連結等，始能識別該特定之個人之資料，例如：車牌號碼與其他相關車輛資料對照、組合、連結後，仍可識別特定當事人者，即屬間接識別個人資料，基本上，應該已經可能據此推定出來某一個特定的個人但如果是查詢困難、需耗費過鉅或耗時過久始能特定到個人的資料，則非屬之。

個人資料去識別化（de-identification）即指「透過一定程序的處理，使個人資料不再具有直接或間接識別性」，因此，採取一組合理之步驟，移除直接或間接識別資料與資料主體間之關聯的過程即稱之為去識別化。個人資料是否達成去識別化主要可從以下要素判定：

(a) 是否仍可能識別當事人？
(b) 是否仍可能與其他個人資料相連結？
(c) 是否仍可能推論出該資料與特定人相關？

個人資料去識別化常見的技術方法如下表所示，建議可綜合考量資料使用目的、資料欄位、重新識別攻擊發生之可能性等因素後，決定去識別化方法。

去識別化技術	說明
統計工具	進行隨機抽樣將增加資料集之不確定性。或屬性值之組合，以提供較廣泛之資訊而非選取詳細觀察聚合相關屬性或值。
密碼式工具	通過加密演算法，保證個人資訊不可還原。常見的加密方式包含確定性加密、次序保留加密等。
抑制技術	通過遮罩部分資訊，或局部抑制、記錄抑制，避免定位到個人。
假名化技術	為各資料當事人建立間接識別資料，替換資料當事人識別資料。
解析	藉由將資料集區分成不同表格，將識別資料與資料其餘部分解除關聯。
概化技術	利用概括、捨入、編碼等方式，對資料進行泛化處理，如取整，截零、範圍約定等。
隨機化技術	修改屬性值，使其新值以隨機方式與其真值不同。通過雜訊添加、置

	換、微聚集等技術，改變資料內容。
合成資料	疊加一定的特徵資料或校驗資訊，演算法不可逆。

四、中小型企業上雲案例分享

以下列舉一些常見的案例，可減少中小型企業對於資訊硬體和基礎設施的投資，提高資源靈活性和擴展性，在增加彈性的同時，也可以同步增加對雲端技能操作之熟悉度：

一、網站和應用系統託管：將對外服務網站和對外公開之應用系統遷移到雲端平台，尤其針對可用性需求較高之網站，以兼具資源可用性及安全性需求。

二、數位辦公工具及文件協作：使用雲端郵件服務管理和共享電子郵件、日曆、文件和其他協作工具，以提高員工之間的協作效率，並減少管理和維護工作量。

三、人力資源管理系統：以雲端人力資源管理平台，進行人力資源管理、招聘、員工培訓、薪酬管理等功能。

四、數位學習平台：以外部訓練課程平台擴大課程主題與資源，或藉由雲端影音串流平台提供更即時的線上培訓課程，提昇員工培訓的效率和效果。

五、客戶關係管理系統：使用雲端 CRM 平台管理客戶資料、銷售流程和客戶互動，以提高銷售和行銷之效率，並提供更好的客戶服務。

六、財務和會計系統：使用雲端財務和會計管理系統，管理發票、支付和財務報告。以提高財務流程的效率，並提供更即時和準確的財務資訊。

七、雲端備份及備援服務：透過雲端備份重要資料，以強化營運韌性的同時，並確保可符合法規要求。

八、雲端開發及測試環境：以雲端實驗場域進行開發及測試，以快速回應需求，並提高市場競爭力。

九、客戶服務與行銷工具：以雲端影音串流平台提供如：市場分析資訊、行銷活動直撥、線上即時諮詢等功能，以增加受眾之參與度和互動性，並提高活動的吸引力和效果。

附件

附件 1 專有名詞英中對照表
附件 2 使用雲端服務建議檢核表

附件 1 專有名詞英中對照表

英文名稱	縮寫	中文名稱
-A-		
Advanced Persistent Threat	APT	持續性威脅
Application Infrastructure Interfaces		資通系統基礎環境介面
Application Programming Interface	API	應用程式介面
Audit Log		稽核軌跡
-B-		
Business Continuity	BC	營運持續
Business Continuity Plan	BCP	營運持續計畫
Business Impact Assessment	BIA	營運衝擊分析
Bring Your Own Key	BYOK	自行管理金鑰
Bring Your Own Encryption	BYOE	自行管理加密
-C-		
Closed-circuit Television	CCTV	監視器
Cloud Service Provider	CSP	雲端服務業者
Compiled Code		編譯程式碼
Component		組件
Container		容器
Customer-Managed Encryption Key	CMEK	客戶自行管理金鑰
Customer-Supplied Encryption Key	CSEK	客戶自行攜帶金鑰
-D-		
Distributed Denial-of-Service Attack	DDoS	阻斷式服務攻擊
De-Identification		個人資料去識別化
Disaster Recovery	DR	災難復原
Disaster Recovery Plan	DRP	災難復原計畫
Downtime		服務無法使用時間
-F-		
Financial Services Addendum	FSA	金融服務附加條款
-H-		
Hardware Security Module	HSM	硬體安全模組
-I-		
Identity and Access Management	IAM	身分識別與存取管理
Infrastructure as a	IaaS	基礎設施作為服務

Service		
Infrastructure as Code	IaC	基礎架構即程式碼
Internet Protocol	IP	網際網路協定位址
Intrusion Detection Systems	IDS	入侵偵測系統
Intrusion Prevention Systems	IPS	入侵防禦系統
-J-		
Joiner Control		用戶存取權限的新增
-K-		
Key Management Service	KMS	金鑰管理服務
-L-		
Leaver Control		用戶存取權限的撤銷
Library		函式庫
Lightweight Directory Access Protocol	LDAP	輕型目錄訪問協定
-M-		
Mover Control		用戶存取權限的修改
Multi-Factor Authentication	MFA	多重要素驗證
-O-		
One Time Password	OTP	一次性密碼
-P-		
Platform as a Service	PaaS	平台作為服務
Port		埠
-R-		
Recovery Time Objective	RTO	復原時間目標
Recovery Point Objective	RPO	復原時間點
Rehost		Gartner 5R 模型:原封不動的遷移至雲端
Refactor		Gartner 5R 模型:重新設計架構適用雲環境
Rearchitect		Gartner 5R 模型:包含少量修改的遷移
Rebuild		Gartner 5R 模型:拋棄現有技術，從頭開始開發
Replace		Gartner 5R 模型:現有應用退役，採用替代解決方案
Rollback		回滾機制
Runtime Modules		運行環境模組
-S-		
Security Patch		安全修補
Service Level Agreement	SLA	服務水準協議

Software as a Service	SaaS	軟體作為服務
Software Library		軟體函式庫
Single Sign-On	SSO	單一登入
Subnet		子網路
System Hardening		系統強化要求
-T-		
Tier		層級
-V-		
Virtual Machine	VM	虛擬機
Virtual Private Cloud	VPC	虛擬私有雲
Virtual Private Network	VPN	虛擬私有網路

附件 2 使用雲端服務建議檢核表

階段	領域	子領域
日常執行與控管	雲端服務治理制度	雲端服務管理政策
		專責單位及相關單位角色權責劃分
		風險評估機制
		監控機制
		轉移策略及計畫
	人才培訓	雲端技術知識與能力培訓計畫與執行
	資安控管	加密與金鑰保護
		資料安全與隱私管理
		身分識別與存取控制
		稽核軌跡與監控
		基礎架構安全
		威脅與弱點管理
		變更管理與組態安全
使用前評估	風險評估與控管	客戶資料處理及儲存地之資料保護法規
		營運衝擊分析
		雲端服務可用性與互通性
		管理能力與經驗
	雲端服務業者評估	盡職調查程序
		資料保護
		防護能力與資源區隔
		日誌紀錄保存機制
	契約或協議	委外事項範圍及雲端服務業者之權責
		客戶資料保密及安全措施

		與雲端服務業者終止委外契約之重大事由
		查核之要求
		重大異常之通報
使用中評估	監督及審查	服務水準協議達成情形
		雲端資源
		安全防護
		雲端委外查核
	業務持續性管理	營運衝擊分析
		營運持續管理計畫
		雲端資料備份
		測試或演練計畫
		雲端服務之資安事件通報與管理機制
使用後	服務終止	資料刪除
		服務/資料移轉