附件2

委外辦法修正草案外部意見回應彙整表

草案條次及內容摘要	外部意見	意見回應
第2條第2項 關於委外辦法適用之金融機構，包括本國銀行及其國外分行、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。	建議委外辦法之適用應擴及金控集團、保險公司、證券業。	1. 委外辦法係依銀行法第45條之1授權訂定，適用之金融機構尚不包括金融控股公司(下稱金控公司)，且金控公司並未辦理金融業務，爰非委外辦法之適用範疇。 2. 目前本會保險局及證期局刻分別就保險業及證券業之委外業務研訂相關規範，爰金控下之保險公司及證券業等亦有該業別適用之委外規範。
第4條第5項 關於重大性之定義為對金融機構之業務營運及客戶權益有重大影響之情形。	建議主管機關於委外辦法常見問答集中，提供金融機構據以評估重大性之「要素」。	1. 現行委外辦法雲端問答集已參考國際規範，提供金融機構據以評估重大性之要素。 2. 本會將參酌相關建議，於問答集中增列金融機構判斷委外作業是否具重大性之相關例示，如時效關鍵性等，以利金融機構判斷。

第5條 關於新型態委外之首案核准	1. 首案核准後，函示公告之程序。 2. 過去金管會已公告核定之「企業客戶商務信用卡盜刷監控作業」及「企業客戶洗錢防制交易監控作業」委外，是否屬修正草案之「已經核定為得委外之作業項目」？	1. 本會前於101年發布金管銀外字第10100302791號函，核定金融機構辦理「企業客戶商務信用卡盜刷監控作業」及「企業客戶洗錢防制交易監控作業」委外處理係屬委外辦法」第3條第1項第20款其他經主管機關核定得委外之作業項目。 2. 本會將整理過往依第20款核准案例列入問答集外，未來經本會核定得委外之作業項目，除發布函示公告周知外，也將配合更新問答集。
第8條第2款 風險管理測試演練	測試或演練是否可由受委託機構辦理並提供測試或演練結果	**將於問答集說明：** 金融機構得參酌受託機構之測試或演練結果，但仍應考量作業委外之風險管理屬金融機構與受託機構之共同責任，金融機構仍應就其管理部分進行測試或演練範圍。
第17條 跨境委外之認定	針對第17條及第18條所稱「境外」應如何認定？另指定之境外資料儲存、處理地，擬新增或變更時，應如何辦理？	**將於問答集說明：** 1. 依第17條規定，金融機構將內部作業委託至境外處理，應充分掌握受託機構對客戶資料使用之情形、確保受託機構處理之金融機構客戶資訊應能及時提供予主管機關及金融機構等，爰第17條及第18條所稱「境外」應以受託機構實際辦理受託作業之地點為準，尚非以受託機構公司註冊地為判斷。 2. 承前點，金融機構應充分瞭解及掌握受委託機構對客戶資訊之使用、處理及

		控管情形，若委外作業屬同一事由且受託機構不變者，僅境外資料儲存、處理地變更時，則金融機構應就擬新增或變更之國家對客戶資訊保護之情形另為評估，並應依第3條所定方式更新作業委外項目之申報資訊。
第18條第1項 須申請核准之委外事項	建議調整第18條第1項之**應向主管機關申請核准範圍**，若「**受委託機構為同集團總機構或國外分支機構，且金管會先前已核准**該受託機構所在地之其他委外作業」，可排除適用，**無須申請核准**。	**不參採。** 有關建議外國金融機構依第18條申請核准範圍，如受託機構所在地業經核准，可排除適用一節，本次修法已明定金融機構應依風險基礎方法管理委外風險，且放寬須向本會申請核准之項目為「委託至境外之重大消費金融資訊系統」，考量該等機構辦理如將重大性消費金融業務資訊系統委託至境外辦理，對客戶權益影響重大，仍須依委外辦法規定辦理。
	建議18條申請書件中「董（理）事會決議之議事錄」，得於董（理）事會已通過相關分層授權規則時，該有權簽署人員出具之同意書代替。	考量金融機構將重大性消費金融業務資訊系統委託至境外辦理對客戶權益影響重大，董事會應明確瞭解擬辦理之重大性委外事項內容，並承擔相關責任，以落實公司治理
	需向主管機關申請核准之重大消費性金融資訊系統，**建議應排除已匿名化或加密後的數據**，因其已無法輕易推斷客戶身分。	**不參採。** 1. 憲法法庭111年8月12日111年憲判字第13號判決(健保資料庫案)，意旨略以： (1) 個資若經處理，依其資料型態與資料本質，客觀上仍有還原而間接識別當事人之可能時，無

		論還原識別之方法難易，若以特定方法還原而可間接識別該個人者，其仍屬個資。當事人就此類資料之自主控制權，仍受憲法資訊隱私權之保障。 (2) 反之，經處理資料於客觀上無還原識別個人之可能時，即已喪失個資本質，當事人就該資訊自不再受憲法第22條個人資訊隱私權之保障。 2. 故金融機構辦理作業委外涉及客戶資訊，應依委外辦法第7條第1項第1款辦理，至是否屬個人資料的認定，應依個人資料保護法及參照上開憲法法庭判決意旨審慎辦理。
	金融機構之核心資料保全如採雲端備份或於境外雲端建置備援系統，如涉及消費金融業務客戶資料，是否須事先核准？	**已於立法說明補充說明：** 1. 如金融機構為僅將客戶資料或其程式、資料庫與作業系統之備份檔案儲存於境外公有雲進行冷備份加密儲存(無法在雲端中直接使用，須在特定系統環境中還原方可應用)，並不涉及「資訊系統」之運作或資料還原運用，對於系統之正式、備援環境的運行並無影響，無須依第一項規定向主管機關申請核准。惟金融機構仍應依該資料境外備份事項是否具重大性，採適當管控措施。 2. 如於境外雲端建置備援系統，具有雲端還原機制及

		回復業務運作功能，尚屬「重大性消費金融業務資訊系統委託至境外處理」，應依第18條申請核准。
第18條 須申請核准之委外事項	建議**新增**第4項條文如下： 「**委外作業如涉及將雲端環境作為內部網路環境之延伸，使資料在傳輸、使用和儲存時，均得在可控管之雲端封閉架構下進行，並對個人資料有相關之安全控制程序者，不適用前三項之規定。**」	**不參採。** 本次修法已明定金融機構應依風險基礎方法管理委外風險，且放寬須向本會申請核准之項目為「委託至境外之重大消費金融資訊系統」，金融機構應依內部控管及風險管理評估，如系統無涉上述重大性消費金融業務委託至境外處理，尚無須適用該條規定申請核准。
第18條 須申請核准之委外事項	建議**新增**第5項條文如下： 「**同一金融機構就雲端架構設計首次申請核准後，嗣後再就同一雲端架構設計重複運用於其他應用系統時，免申請核准；就原已被核准之應用系統，如有不涉及雲端架構設計之應用系統增減修改者，亦同。**」	**不參採。** 1. 同一雲端架構運用於不同應用系統所涉及客戶資料庫及安全控管仍有不同。 2. 本次修法已明定金融機構應依風險基礎方法管理委外風險，且放寬須向本會申請核准之項目為「委託至境外之重大消費金融資訊系統」，金融機構應依內部控管及風險管理評估，如系統無涉及上述重大性消費金融業務委託至境外處理，尚無須適用該條規定申請核准。
第19條第1款及第4款 關於委外事項涉及使用雲端服務，應依規定辦理之事項。	建議於問答集增列更細緻「依客戶資料之分級分類暨相對應加密或代碼化等保護措施」監理所認可之技術與標準等之相關闡釋。	**不參採。** 本項建議提供技術與標準等之相關闡釋，係屬銀行執行技術層面，若未來金融機構於實務執行上有需求，可於銀行公會相關會議提出討論。

第19條第3款 關於規範金融機構委託獨立第三人查核之查核報告符合相關國際資訊安全標準。	考量隱私資料的運用與管理之重要性，建議第19條第3款第2目修正為「符合相關國際資訊安全**及隱私保護**標準。」	**參採**，修正第19條第3款第2目。
	建議**新增**第3款第4目條文如下：「（四）本辦法下適用於雲端服務業者提供及控制之基礎設施、硬體及軟體之查核、稽核及檢查要求，得以取得相關雲端服務業者之雲端服務資訊安全國際標準認證證明處理。」	**將於問答集說明：** 基於雲端基礎架構為雲端業者所建置及管理，因雲端運用不同型態而有差異。爰針對上述雲端架構之查核可依雲端業者出具關於雲端基礎架構的資訊安全國際標準認證報告辦理。惟個別金融機構仍應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。
第19條第4款 關於規範金融機構傳輸及儲存客戶資料至雲端服務業者，應採行客戶資料加密或代碼化等有效保護措施。	有關草案第19條第4款「客戶資料加密」，建議應採 E2EE (End-to-end encryption，端到端加密)。	**不參採。** 1. 金融機構及雲端業者係依自身成本、效益及風險基礎方法等評估採行合適之加密技術標準。 2. 金融機構對於作業委外仍須負最終責任，應就委外事項之風險程度、重大性及對營運及客戶權益影響進行評估，依風險基礎方法採取適當之控管措施。