論著與分析

金融機構資訊（含雲端）作業委外風險之金融監理探討

林緯政

壹、前言

早在 2005 年國際清算銀行（Bank for International Settlements ，下稱 BIS）發布之「金融服務之委外（Outsourcing in Financial Services）」即指出，金融機構[註1]作業委外有日漸增加，其中尤以資訊服務委外及跨境委外領域增加趨勢最為明顯，相關風險也同時衍生，包括金融機構未能有效監督服務提供者或缺乏專業能力監督受託機構、受託機構未遵守個人資料保護法規、受託機構法律遵循或控制措施不足、缺乏合適退場策略等。此外，跨境委外使得業務連續性計畫（Business continuity planning）變得更加複雜，使金融機構難以即時向主管機關提供相關監理資料。前揭問題於當時已引起許多金融主管機關之重視，並為此陸續修訂金融機構作業委外相關規範[註2]。

本文作者林緯政為金管會銀行局專員。本文為作者個人意見，不代表本公司立場。

時至今日，產業創新發展及新冠疫情更催化了數位服務的使用，透過隨身裝置進行轉帳、借貸及投資等金融服務已是稀鬆平常，金融從業人員也可以遠端工作，數位服務已改變了人們的日常生活。

金融業為加速金融服務效率及控制成本，對於資訊服務業者之依賴日漸加深，特別是在雲端服務應用領域。致使各國金融主管機關聚焦於相關議題，並於近年陸續修訂金融機構作業委外之監理規範，或修正發布相關文件。如歐盟於 2022 年通過「數位營運韌性法案」（Digital Operational Resilience Act，下稱 DORA），以及英國於 2023 年修正「金融服務及市場法」（Financial Services and Markets Act 2023，下稱 FSMA 2023）等。

此外，美國財政部亦於 2023 年 2 月發布「金融業採用雲端服務」報告（The Financial Services Sector's Adoption of Cloud Services），探討金融機構採用雲端服務之機會、挑戰與未來監理措施之規劃[註3]，並於同年 5 月組成工作小組，成員包括銀行、證券、保險主管機關與民間部門，由公私部門合作共同強化金融機構採用雲端服務之相關配套。

觀諸前述主要國家之政策方向，可得知其監理方針已有所轉變，在賦予金融機構權限之同時，亦評估將提供金融機構服務之關鍵第三方服務提供者（Critical Third Party，簡稱 CTP）納入金融監管之框架。

我國亦相當重視金融機構雲端服務委外議題，金融監督管理委員會（下稱金管會）甫於 2023 年 8 月 25 日發布修正「金融機構作業委託他人處理內部作業制度及程序辦法」（下稱委外辦法），修正金融機構（包含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等）委外使用雲端等外部服務之規範；而證券商、證券投信顧問事業、期貨業及保險業之委外規範亦同步修正。本次修正參酌國際監理規範，簡化金融機構申請辦理作業之規定，並強化金融機構內部風險控管相關之規定，後續金管會將持續關注實務執行情形及國際發展，滾動檢討相關規範[註4]。

考量國際金融監理發展向來為我國政策制定之重要參考，本文將探討近期國際監理政策之重點發展，並簡介我國委外監理政策變化，據以提出未來政策研擬可以考量之因素。

貳、金融業作業「委外」之定義

根據 BIS 於 2005 年所提出之定義，「委外（outsourcing）」係指「受監管金融機構於現在或未來，利用第三方（集團內的附屬實體或集團外部的實體）執行通常由金融機構辦理的活動。不論係由金融機構委託第三方，或是已委託第三方之事項再由受託之第三方委託另一服務提供者之「複委託（subcontracting）」，或是受託機構為同一集團之其他金融機構或非金融機構，均在此一範疇（註 5）。

而「委外」與「採購契約（purchasing contracts）」之範疇仍有不同，儘管金融機構均須確保所購買之服務或商品符合其採購目的，但委外係指涉及「移轉金融機構與其客戶有關的非公開機敏資訊或與其業務活動相關的其他資訊」（註 6）之行為。

BIS 所提出之委外定義，廣泛影響各地區金融主管機關，如歐洲銀行監理總署（European Banking Authority，下稱 EBA）所發布之監理文件係以「金融機構與服務提供者間藉由任何形式之安排，由服務提供者透過該安排執行原應由金融機構執行之流程、服務或活動（註 7）」作為委外之定義，並明確列舉非屬委外之活動範疇（註 8）。

類似之作法亦可以見於新加坡金融管理局（Monetary Authority of Singapore，下稱 MAS）（註 9）及國際證券管理機構組織（International Organization of Securities Commissions，簡稱 IOSCO）（註 10）所發布之監理文件，我國金管會委外辦法問答集，亦已整理非屬委外之範疇（註 11），以利金融機構遵循辦理。

參、國際委外監理近期重點發展

一、歐盟「數位營運韌性法案（DORA）」

歐盟理事會（European Council）於 2022 年 11 月 28 日通過「數位營運韌性法案」（Digital Operational Resilience Act, DORA），預計於 2025 年 1 月 17 日起施行。該法案聚焦於強化數位服務的營運韌性，特別是金融機構提供的數位服務。

該法案指出資訊及通訊科技（Information and Communication Technology, ICT）事件和缺乏營運韌性有可能危及整個金融體系之穩健性，遂要求金融機構

應落實執行對 ICT 相關事件的保護、監測、遏制及恢復能力，並提出全面 ICT 風險管理框架，要求所有金融機構依循該框架有效地管理「資訊及通訊科技」風險，其適用對象涵蓋銀行、證券、保險、電子支付機構及虛擬資產服務提供商等金融業者。

該框架已就 ICT 風險管理、事件報告、營運韌性測試及 ICT 第三方風險監控制定規範，以防止相關風險對金融穩定、消費者保護及整個經濟體系產生重大影響。而針對 ICT 之監理框架可以分兩個層次，一是金融機構對於 ICT 服務提供商之管理，二是歐盟主管機關對於關鍵（Critical）ICT 第三方服務提供商之直接監督（Oversight），以下將就此兩部份進行說明。

(一)金融機構對 ICT 第三方服務提供商之管理

DORA 法案要求金融機構對其所有的 ICT 第三方服務提供商（包括雲端服務提供商）進行評估及風險管理，以確保金融機構充分理解其業務和數位基礎架構的運作方式，及 ICT 服務提供商遵守所有相關規範，特別是在數據隱私和安全方面。

在治理層面，金融機構內部應設立管理單位（management body）（註 12）執行風險管理工作，並由管理單位承擔金融機構 ICT 風險之最終責任，以及設定權責分工、審批及監督 ICT 業務連續性政策及災害復原計畫、分配及審查金融機構資源之安排等（註 13）。

金融機構應定期評估其 ICT 之第三方風險策略，並填報登記表（Register）向主管機關說明相關資訊，包含使用 ICT 服務之數量、服務提供者之類別、契約之性質及該服務性質等資訊。此外，金融機構應於 ICT 委外契約或是外包之業務轉為具重大性時，即時通知主管機關，而主管機關應有權取得具重大性服務相關資訊（註 14）。

服務契約條款方面，DORA 法案明確規範金融業者與 ICT 業者簽訂契約應包含之內容，包括：

- 對於服務清晰且完整之說明；
- 是否允許對重要功能進行複委託，如允許複委託，應說明複委託之條件；
- 資料儲存地，如有變更應通知金融機構；

- 個人資料的可訪問性、可用性、完整性、安全性和保護之條款，以及在 ICT 服務提供商業務停止之資料處理機制；
- ICT 向金融機構通報重大影響事件之期限及報告義務；
- 金融機構及其指定之第三方有權對 ICT 服務提供商進行查核，且 ICT 服務提供商應承諾將盡力協助金融機構所進行之現場查核，以及詳細說明遠端查核（remote audits）之範圍、方式和頻率；
- ICT 服務提供商有義務與金融主管機關及其指定人員充分合作；
- 服務終止之退場策略等（註 15）。

以上金融機構對於 ICT 服務提供商之風險管理框架並非 DORA 首創，EBA 所發布之委外指引（Guidelines on outsourcing arrangements）或新加坡 MAS 之委外監管制度（註 16）亦係採取類似之監理框架，要求金融機構從事前評估，訂定嚴謹之服務契約，持續監督受託機構，以落實相關風險管控。

(二)金融主管機關對關鍵 ICT 第三方服務提供商之監督

針對「關鍵 ICT 第三方服務提供商（Critical ICT Third Party Provider，下稱 CTPP）」之監理作法，主要係規範於 DORA 法案之第 28 條至第 38 條，旨在於降低 CTPP 對金融機構造成的風險，確保金融服務的穩定性和連續性。DORA 強化金融主管機關對第三方服務提供商之直接監管權限，係目前金融監理上較為嶄新之作法。

為此，歐洲監管機構（European Supervisory Authorities，簡稱 ESAs）（註 17）將建立一個監督平臺（Oversight Forum），以協調各機關之監督行動，並推廣具一致性的風險監控實務作法。此外，該平台須評估 ICT 服務提供商，並指定對金融業有重大影響之業者為 CTPP。

而 ESAs 係透過以下標準，評估 ICT 服務提供商是否屬 CTPP，說明如下：（1）若該 ICT 服務提供商發生大規模運營失敗，將對金融服務的穩定性、連續性或品質產生潛在系統性影響；（2）依賴該 ICT 服務提供商之金融機構的系統重要性；（3）金融產業對該 ICT 服務之依賴程度；（4）ICT 服務提供商的可替代程度；（5）該 ICT 服務在全球提供服務之

國家數量；（6）該 ICT 服務在全球提供金融業者服務之國家數量。

如一 ICT 服務提供商被認定屬 CTPP，則該其應於歐盟地區設立營業據點，否則金融機構不得使用該項 ICT 服務（註 18）。此外，ESA 將為每個 CTPP 指定一主管機關擔任「首席監督員（Lead Overseer）」，而首席監督員之職責，係評估 CTPP 已依相關規範落實執行全面而有效的風險管理措施，並審查其 ICT 服務之安全性、可用性、連續性、可擴展性和服務品質。

此外，首席監督員有權向 CTPP 要求提供相關資料或文件傳喚 CTPP 人員說明、訪查相關人士進行一般調查（General investigations）或是實地檢查（On-site inspections）。亦可提出建議要求 CTPP 改善其 ICT 風險管理措施，並在必要時可對 CTPP 處以罰鍰。

因授權 ESAs 更多權力監督 CTPP，衍生出人力規模擴充、資訊系統成本、檢查費用及翻譯費用等資源需求，預計 2022 年至 2027 年將增加 30.19 億歐元（約新臺幣 1,000 億元）之經費，以滿足相關監理成本支出所需（註 19）。若未來我國政策上擬參考 DORA 規範強化監理職權，應考量相關監理資源之安排，以及對於整體產業之影響，使相關政策得以有效推動。

目前 DORA 法案之執行仍有許多具體及細部規範或標準待制定，為此 ESAs 於 2023 年 6 月 19 日就相關技術標準啟動公眾諮詢，盼能提高制度明確性以利實務運行（註 20）。ESAs 另於 2023 年 9 月 23 日發布新聞稿，將其對於 ICT 評估標準及向 CTPP 收取監管費用之標準等相關建議送歐洲議會，以作為後續政策研訂之參考（註 21）。

二、英國對第三方及新興科技之監理規範發展

英國央行之審慎監理總署（Prudential Regulation Authority, PRA）及金融行為監管局（Financial Conduct Authority, FCA）於 2022 年 7 月就關鍵第三方業者（CTP）之監理框架發布政策諮詢文件（註 22）。該政策諮詢文件指出 CTP 提供受監理之金融機構與金融市場基礎建設公司（FMIs）服務，卻同時具高度集中特性，亦即多數金融機構可能集中與少數幾家第三方業者合作，如該特定第三方業者運

作失靈將危及消費者權益。為避免未受到監理之部門對金融穩定產生重大影響，該政策諮詢文件提出幾個潛在政策措施說明如下：

(一)建立 CTP 監管清單：監管機構將根據第三方業者對金融服務業的影響、其提供的服務的關鍵性以及其在市場中的地位，確定哪些業者需要進行監管。

(二)制定 CTP 的最低營運韌性標準：監管機構將制定 CTP 必須遵守的最低營運韌性標準，例如風險管理、災難恢復和應急計劃。

(三)開發 CTP 的韌性測試工具：監管機構將開發工具，幫助金融服務業評估其 CTP 的韌性。

而英國財政部（HMT）於 2023 年 6 月修正金融服務市場法（FSMA 2023），賦予主管機關直接監督 CTP 之權力[註 23]。在英國政府辨識系統性 CTP 後，PRA 可要求 CTP 遵循相關義務，可能監理措施包括就 CTP 提供金融機構及 FMIs 之服務，要求其參與跨機關及部門之演練、資安韌性測試及員工專業技能檢核，以進行壓力測試，並瞭解其在不同情境發生下可如何因應。

然而 FSMA 未訂有詳細而具體之 CTP 監管標準，仍有待相關主管機關進一步完備相關監管機制，並將對外公開諮詢[註 24]。雖然英國政府所提出之監管框架與歐盟 DORA 相近，兩者均強化金融主管機關對於金融業之關鍵第三方業者之直接監管權限，由主管機關指定對整體金融業有重大影響關鍵第三方業者，並對該等業者進行風險評估及查核，以確保該等業者能提供符合監理期待之服務，但英國金融主管機關考量要求 CTP 在地化將提高 CTP、金融機構及 FMI 之法令遵循成本，並未如歐盟 DORA 法案制定相關服務應在地化之監理要求[註 25]。

此外，為推動競爭與創新，並保護消費者與企業，英國政府刻正修訂「數位市場、競爭與消費者法案」（Digital Markets, Competition and Consumers Bill）[註 26]，該法案將對被指定為「戰略市場地位（Strategic Market Status）」的數位科技公司提出額外遵循規範，並加強競爭及市場管理局（Competition and Markets Authority, CMA）收集資訊和採取執法行動的能力[註 27]。

三、美國財政部對金融機構使用雲端之風險監理規劃

為瞭解雲端服務對金融業營運韌性之影響，美國財政部與銀行資訊基礎設施委員會（The Financial and Banking Information Infrastructure Committee，簡稱FBIIC）[註28]，於訪談金融產業、雲端服務業者（Cloud Service Providers，簡稱CSPs）等利害關係人，及研究美國及國際規範後，於2023年2月8日發布「金融業採用雲端服務（The Financial Services Sector's Adoption of Cloud Services）」報告。

該報告並未提出額外監理規範，而係蒐集整理金融產業運用雲端服務現況、意見回饋及監理規範，據以提出監理立場及未來規畫。根據美國銀行公會之調查，美國銀行業2021年使用IaaS（Infrastructure As A Service；基礎架構即服務）、PaaS（Platform As A Service；平台即服務）、SaaS（Software As A Service；軟體即服務）[註29]之比率分別為91%、43%及29%，預估將持續增長，且24%受訪銀行已將部分核心服務遷移至雲端[註30]。政府及民間組織均有制定使用雲端服務之技術標準，俾利相關業者參酌，以評估雲端服務之風險及建立控管機制[註31]。

雖然美國金融業運用雲端服務之情形已相當普及，然而業者在訪查過程中，仍表示使用雲端服務具有以下挑戰[註32]：

(一)雲端服務透明度不足：CSPs未能即時提供導致其系統中斷事件之詳細資訊，限制金融機構充分瞭解與雲端服務相關風險及監控之能力。

(二)專業人才及工具之不足：金融機構表示缺乏專業人力和工具以有效利用雲端技術，因此建議CSPs增加支援金融機構之專家人才，並改進支援性技術工具及雲端導入的架構。

(三)源自於CSPs的資安風險：單一CSPs資安事件可能會對整體金融業產生連鎖影響，致金融機構面臨來自CSPs技術漏洞的風險，且實務上不容易透過分散供應商減輕相關風險。

(四)產業高度集中之潛在影響：CSPs產業呈現高集中度，並導致資安問題等事故影響甚鉅。然而主管機關卻缺乏足夠資訊，評估集中度對金融機構之潛在影響，未來應加強公私合作以進一步探討前述影響及推動安全演練。

(五)契約談判不易：CSPs 通常具有較強的議約能力，可能會限制金融機構爭取到理想之雲端服務契約條件的可能性，而明確之法規要求則有助於強化金融機構議約能力。

(六)各國監管制度不一致：各國監理制度的不一致，使得美國金融機構無法在全球採行一致的雲端服務架構，並因此提高使用成本及風險。此外，外國法規變化可能使 CSPs 受到外國金融監管機構的直接監管，並衍生監管衝突，將對其所提供雲端服務品質及安全性產生負面影響。

為解決前揭挑戰，美國財政部及相關主管機關業於 2023 年 5 月 25 日成立「雲端執行指導小組」，旗下並有多個工作小組，將透過公私部門合作，制定採用雲端服務之最佳實務，並致力於提高雲端服務之透明度，以及加強監理資源之合作及協調。此外，該小組將關注實務發展，確認金融監理部門對 CSPs 之監管權限是否足以應對潛在之系統性風險（註 33）。

四、小結

觀察國際委外監理政策之發展，可發現近期主管機關對於金融機構委外風險之主要關注重點，係雲端產業集中特性對於金融產業系統性之潛在影響，而歐盟、英國及美國分別採取不同程度的監理政策應對。歐盟 DORA 賦予金融主管機關對於關鍵雲端服務提供商直接監管之權限，並要求此類業者應在歐盟境內設有據點。英國雖同樣賦予主管機關監管之權限，但未訂有在地化規範。美國主管機關目前並未積極強化主管機關對雲端服務提供商之直接監理權限，而是透過公私部門合作，進一步探討供應商集中度對金融產業之具體影響，及進行跨部門安全演練，並將強化相關監理規範之明確性及與國際監理制度之一致性。

前揭歐盟、英國及美國之政策框架雖已發布，惟修正後之規範均未實際施行，目前尚難評估其成效，仍有待施行後金融業者、第三方服務提供者及監管方共同合作探索最佳運作模式。

肆、我國金融機構作業委外法規之發展

我國金融機構作業委外監管法規最早起源於 1999 年 12 月由財政部金融局制

定之「銀行作業委託他人處理應注意事項」，而後於 2001 年 12 月修正為「金融機構作業委託他人處理應注意事項」，將適用範圍拓展至信託投資公司、票券金融公司、信用合作社、農漁會信用部及經營信用卡業務機構。

為實踐金融監理一元化目標，金管會於 2004 年 7 月成立，財政部金融局改制為金管會銀行局，隨著國際監理趨勢變化、信用卡及消費性貸款相關金融糾紛事件頻傳，金管會廢止舊有委外應注意事項，於 2006 年 9 月發布「金融機構作業委託他人處理內部作業制度及程序辦法」，強化信用卡發卡業務、消費性貸款業務之行銷及應收債權催收委外之監管要求，以及考量跨國委外之監理執行困難，明定跨境委外應取得主管機關核准。

金管會於 2012 年 2 月修正之委外辦法，係考量消費金融業務對我國客戶權益及財產權影響重大，為降低資訊系統集中境外及資料國際傳輸衍生之風險，並強化客戶個人資料之保護，明定本國銀行不得將消費金融相關資訊系統之登錄、處理、輸出等事項委託至境外辦理，並增訂跨境委外應遵循之規定。雖當時規範未使用「雲端」一詞，但將消費金融資料系統委託至境外處理委託之境外處理多涉及私有雲或公有雲應用，我國在當時對雲端應用係採取較為審慎之態度。

為配合我國推動與其他國家建立自由貿易協定之整體政策，又於 2014 年 5 月修正委外辦法前揭消費金融相關資訊系統不得跨境委外之規定，改為符合相關條件之金融機構，應提交相關申請書件，取得主管機關核准後始得辦理。

為因應金融科技發展趨勢，適當導入雲端服務有助於金融機構經營效率之提升及節省成本，且各國金融主管機關已陸續開放作業委託雲端服務業者處理，爰金管會於 2019 年 9 月再次修正委外辦法，增訂金融機構將作業委託他人處理涉及使用雲端服務應遵循規範，要求金融機構注意作業委託雲端服務業者適度分散，金融機構得自行委託或委託具資訊專業之獨立第三人進行查核並出具報告，對委託雲端服務業者處理之資料應保有完整所有權，金融機構須保有其指定資料處理及儲存地之權利，境外當地資料保護法規不得低於我國要求。金融機構在規劃使用雲端服務前，若委外事項具重大性或涉及委託至境外，應向主管機關申請核准，若不具重大性或跨境，則應向主管機關提出備查。

另金管會並於 2020 年 4 月 17 日核備中華民國銀行商業同業公會全國聯合會

（簡稱我國銀行公會）修正之「金融機構運用新興科技作業規範」，該規範參酌委外辦法之規定，研訂金融機構委外使用雲端服務應落實之安全控管重點。

在前次委外辦法修正後，隨著數位金融及科技金融發展，以及新冠疫情對金融服務及遠距工作帶來的變革，金融機構運用雲端服務之情形也日漸普及，金管會於 2023 年 8 月修正委外辦法，本次修法重點摘述如下：

一、參酌國際作法，以風險為基礎之方法（Risk-Based Approach, RBA）為主軸，明定金融機構對作業委外負最終責任，應就作業委外建立妥適之政策及原則，強化委外前、中、後階段之風險控管機制，以作為金融機構辦理作業委外事項之控管基礎（第 4 條）。

二、過往應向主管機關申請核准或備查之跨境委外及雲端委外，相關程序簡化為「涉及重大性消費金融業務資訊系統委託至境外處理應向主管機關提出申請」，向主管機關申請之應備文件亦有相當簡化，從舊法跨境雲端委外之 9 至 12 項文件簡化為 6 項申請文件（第 18 條）。

三、金融機構應訂定使用雲端服務之政策及原則，注意作業委託雲端服務業者適度分散。涉及重大性消費金融業務資訊系統之客戶資料儲存地以位於我國境內為原則，如位於境外，除經主管機關核准者外，客戶重要資料應在我國留存備份等。（第 19 條）

為確保金融機構依前揭委外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，金管會於 2023 年 10 月請銀行公會研訂金融業使用雲端服務的自律規範，重點包括訂定治理政策及風險管理、對雲端業者的管理框架和人才培訓等[註 34]，惟至本文截稿時（2024.2.28），該自律規範尚未發布。

縱觀我國金融機構作業委外之法規修訂，可以發現委外法規修正與我國實務發展現況密切相關，隨著實務需求變化而靈活調整，監管重點最早係關注債權催收和消費性貸款行銷委外，於 2012 年強調消費金融相關資訊系統跨境委外之監理，於 2019 年開始起則係著重於雲端委外監理制度之完備。此外，歷次修法之總說明或條文修正說明多有提及參酌國際規範之內容，國際監理趨勢之變化亦係我國委外法規之修正重要參酌標的。我國目前金融業雲端服務之使用仍在發展階段，雲端服務之採用普及程度尚不及美國及歐洲金融業，隨著產業逐漸導入雲端

服務，可預見我國金融業也應會碰到與歐美金融產業類似之挑戰，如集中於少數雲端服務業者及相關人才或工具不足等挑戰，若能利用他國發展經驗以強化相關風險控管機制，將有助於我國享用技術優勢而減少潛在之負面影響。

伍、結論與建議

金融產業實務發展及國際監理趨勢變化影響我國監理政策之制定，面對雲端服務之發展浪潮，各國主管機關陸續提出相關監理政策因應。目前我國金融業採用雲端服務仍在發展階段，惟考量近年來我國金融業實務發展及逐漸對關鍵第三方服務提供者（CTP）之需求增加，可參酌歐盟及英國作法，及早思考未來金融監理方向，將有助於金融業及主管機關即時採取因應措施。因此以下列舉主管機關擬拓展金融監管權限至 CTP 應考量之面向：

一、金融主管機關之間接地位

對於金融機構作業委外之風險控管，各國多採取由金融機構依風險基礎方法建立全面之控管措施，金融機構應要求受託機構在契約關係下，落實內部管理。而主管機關未直接參與金融機構與受託機構間契約關係，若受託機構服務瑕疵影響金融機構運作或客戶權益，仍有待金融機構評估影響範圍及效果，主管機關須透過金融機構間接瞭解實際服務之運作情形。主管機關在欠缺第一手完整資訊之前提下，如何能直接對 CTP 採取即時有效之監理，仍有待探討。主管機關、金融機構及 CTP 三者間應如何建立明確之權責區分及有效的溝通架構，亦須進一步思考。

二、與「資通安全管理法」管理模式接近

我國數位發展部於 2023 年 9 月提出「資通安全管理法」修正草案，該法定義「關鍵基礎設施」為「行政院公告之關鍵領域中，該領域服務所依賴之系統或網路之實體或虛擬資產，其功能一旦停止運作或效能降低，對國家安全、社會公共利益、國民生活或經濟活動有重大影響之虞者」（草案第三條）。該法要求中央目的事業主管機關應擬訂關鍵基礎設施提供者之指定清單（草案第十九條），並

定期稽核關鍵基礎設施提供者之資通安全維護計畫之實施情形（草案第二十條），以確保相關資通安全無虞[註 35]。

「資通安全管理法」雖與歐盟 DORA 或英國 FSMA 2023 同樣專注大型科技公司對產業之影響，但其性質更接近英國「數位市場、競爭與消費者法案」，因英國「數位市場、競爭與消費者法案」目前仍在修訂中，未來該法與 FSMA 2023 在實務執行上如何相互搭配，亦為政策觀察重點。目前我國對關鍵基礎設施提供者雖已有相關管理法制，為降低金融機構資訊（含雲端）作業委外風險，未來我國金融主管機關若對金融機構資訊作業委外之第三方服務提供業者加強監理或直接監理，可通盤考量與其互相搭配，以強化金融穩定之目標。

三、 跨境服務的監管挑戰

雲端服務之特性，使服務提供者無須在我國設有實體機房或辦公單位，即可自境外提供服務予我國內業者，然而對於來自境外之服務提供者，我國主管機關如何有效對此類業者行使行政職權，亦為一大挑戰。歐盟 DORA 要求關鍵 ICT 服務提供商，應於歐盟地區設立營業據點，否則金融機構不得使用該項 ICT 服務[註 36]，然而英國卻未採取 CTP 在地化要求[註 37]，以我國之市場規模及國際影響力，恐不易採取 DORA 做法強制業者在我國設立據點。未來如我國金融業者集中委託特定境外機構，應思考如何使監理措施有效執行，避免對於境內與境外之業者採取之監理要求不一，產生監理套利之情形。

四、 強化主管機關、金融機構與第三方服務業者之實務合作機制

在我國金融機構採用雲端服務過程中，其面臨之潛在挑戰並非單靠金融監管法規修訂可解決，許多實務問題需要雲端服務業者及金融機構共同協調，如前揭美國財政部報告所指出，金融機構運用雲端服務之挑戰包括雲端服務透明度不足、專業人才及工具之不足、使用雲端服務之資安風險以及雲端服務產業高度集中等，面對該等挑戰，需仰賴金融業及雲端服務產業共同努力，而主管機關在強化監管規範前，亦應瞭解產業面臨之實務挑戰，因此美國於 2023 年 5 月成立「雲端執行指導小組」，透過公私部門合作，制定採用雲端服務之最佳實務，並致力

於提高雲端服務之透明度，以及加強監理資源之合作及協調。

目前我國金融業採用雲端服務仍在發展階段，委外法規甫於 2023 年 8 月修正，許多金融機構仍在探討如何將雲端服務導入其業務流程，建構相關機制使雲端服務得以符合其業務需求及法規遵循。

在此前提下，主管機關如驟然修訂相關規範恐使業者在遵循上有所困難，因此本文建議在現階段與其採取歐盟或英國金融主管機關之更高強度監管法規，更亟需強化主管機關、金融機構與第三方服務業者之資訊交流與合作機制，透過該交流及合作機制研訂金融業採用雲端服務之自律規範及實務操作手冊，並就實務應用之挑戰尋求可行作法。使金融機構可借鑑同業之經驗以提升應用雲端服務之知識與工具，並得與雲端服務業者有更衡平之議約能力，主管機關也得以掌握產業之需求，在正確的時間採取合適監管措施，第三方服務業者在拓展業務過程中能兼顧各方需求，達成產業多贏之局面。

註釋

註 1： 本文探討之金融機構定義範圍較「金融機構作業委託他人處理內部作業制度及程序辦法」第二條所列舉金融機構範圍更廣，主要外國文獻所提及之金融機構多涵蓋銀行業、證券業及保險業。而我國證券業與保險業之委外規範主要係參考銀行業「金融機構作業委託他人處理內部作業制度及程序辦法」修訂，考量本文主要係關注國際規範對於我國監理政策之啟發，不於本文就我國證券業及保險業之委外規範發展與差異進行展開。

註 2： *See* Bank for International Settlements, *Outsourcing in Financial Services*, at 11 (2005).

註 3： U.S. Department of the Treasury, Opportunities, Challenges Facing Financial Sector Cloud-Based Technology Adoption, *available at* https://home.treasury.gov/news/press-releases/jy1252 (last accessed Dec 7, 2023).

註 4： 金融監督管理委員會，2023.8.4 新聞稿「金管會修正發布金融機構作業委託他人處理內部作業制度及程序辦法」，最後瀏覽日期 2023.11.4。

註 5： *See* Bank for International Settlements, supra note 1, at 10. “Outsourcing is defined in this paper as a regulated entity’s use of a third party (either an affiliated entity within a corporate group or an entity that is external to the corporate group) to perform activities

on a continuing basis that would normally be undertaken by the regulated entity, now or in the future". Outsourcing can be the initial transfer of an activity (or a part of that activity) from a regulated entity to a third party or the further transfer of an activity (or a part thereof) from one third party service provider to another, sometimes referred to as "**subcontracting**." In some jurisdictions, the initial outsourcing is also referred to as subcontracting.".

註 6： *See id*. at 10.

註 7： *See* EBA, *Guidelines on Outsourcing Arrangements*, at 19 (2019).

註 8： *See id*. at 26.

註 9： *See* MAS, *Guidelines On Outsourcing*, at 28 (2018).

註 10：See International Organization Of Securities Commissions (IOSCO), *Principles on Outsourcing Final Report*, at 14 (2021).

註 11：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」相關問題適用解說問答集（112 年 10 月版）第 1 題。

註 12：即有權決定金融機構之戰略、目標、總體決策之高階管理單位，具體定義請見 points（7）and（8）of Article 3（1）of Directive 2013/36/EU。

註 13：European Union, Digital Operational Resilience Act, Article 4.

註 14：European Union, Digital Operational Resilience Act, Article 25.

註 15：European Union, Digital Operational Resilience Act, Article 27.

註 16：*See* MAS, supra note 9.

註 17：成員包含歐洲銀行監理總署（EBA）、歐洲證券和市場管理局（ESMA）、歐洲保險和職業養老金管理局（EIOPA）。

註 18：European Union, Digital Operational Resilience Act, Article 28.

註 19：European Union, Digital Operational Resilience Act, at 7.

註 20：EBA, ESAs Joint Committee Technical standards under the Digital Operational Resilience Act (DORA), 2023.6.19, https://www.eba.europa.eu/esas-joint-committee-technical-standards-under-digital-operational-resilience-act-dora

註 21：ESMA, ESAs specify criticality criteria and oversight fees for critical ICT third-party providers under DORA, *available at* https://www.esma.europa.eu/press-news/esma-news/esas-specify-criticality-criteria-and-oversight-fees-critical-ict-third-party (last

accessed Dec 7, 2023).

註 22：Bank of England, DP3/22 – Operational resilience: Critical third parties to the UK financial sector, *available at* https://www.bankofengland.co.uk/prudential-regulation/publication/2022/july/operational-resilience-critical-third-parties-uk-financial-sector (last accessed Dec 7, 2023).

註 23：Financial Services and Markets Act 2023, CHAPTER 3 Critical third parties.

註 24：Bank of England, Cyber risks and operational resilience: getting prepared - speech by Elisabeth Stheeman, 18 October 2023, *available at* https://www.bankofengland.co.uk/speech/2023/october/elisabeth-stheeman-speech-at-the-london-school-of-economics-conference (last accessed Dec 7, 2023).

註 25：*See* Bank of England, supra note 22, at 22. “the potential measures would be agnostic about the location of CTP”.

註 26：UK Parliament, Digital Markets, Competition and Consumers Bill, *available at* https://bills.parliament.uk/bills/3453 (last accessed Dec 7, 2023).

註 27：Competition and Markets Authority, New bill to stamp out unfair practices and promote competition in digital markets, *available at* https://www.gov.uk/government/news/new-bill-to-stamp-out-unfair-practices-and-promote-competition-in-digital-markets (last accessed Dec 7, 2023).

註 28：成員包括美國聯邦準備銀行、通貨監理局、證券交易委員會、保險監理官協會等 18 個聯邦及州金融主管機關。

註 29：參酌「金融機構運用新興科技作業規範」（2020.4.17）第 2 條規定，IaaS、PaaS、SaaS 之定義如下：IaaS（Infrastructure As A Service）：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；PaaS（Platform As A Service；平台即服務）：雲端服務業者提供作業系統使用，承租人能於此作業系統操作其軟體，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；SaaS（Software As A Service；軟體即服務）：承租人能使用軟體，但並不掌控軟體、作業系統、硬體。

註 30：*See* U.S. Department of the Treasury, *The Financial Services Sector’s Adoption of Cloud*

Services, at 23-24 (2023).

註 31：*See id*. at 23-24.

註 32：*See id*. at 49-61.

註 33：U.S. Department of the Treasury, U.S. Department of the Treasury Kicks Off Public-Private Executive Steering Group to Address Cloud Report Recommendations, *available at* https://home.treasury.gov/news/press-releases/jy1503 (last accessed Dec 7, 2023).

註 34：iThome，銀行局揭雲端服務治理架構六大重點，未來將由銀行公會訂定相關自律規範（2023.11.7）載於 https://www.ithome.com.tw/news/159672，最後瀏覽日 2024 年 2 月 25 日。

註 35：數位發展部中華民國 112 年 9 月 22 日數授資法字第 1125000186 號公告，預告修正「資通安全管理法」。

註 36：*See* European Union, supra note 18.

註 37：*See* Bank of England, supra note 21, at 22.