出國報告（出國類別：出席國際會議）

國際證券管理機構組織（IOSCO）

信用評等機構委員會

（Committee on Credit Rating Agencies）

2017 年第 3 次會議

服務機關：金融監督管理委員會證券期貨局
姓名職稱：曾稽核煌鈞、李科員志偉
派赴國家：巴西
出國期間：106 年 12 月 2 日至 106 年 12 月 9 日
報告日期：107 年 2 月 22 日

目　錄

壹、 前言

國際證券管理機構組織（International Organization of Securities Commissions，IOSCO）於第 37 屆年會通過修改 IOSCO 章程，將原執行委員會、技術委員會以及新興市場委員會中之諮詢委員會（Advisory Board）合併為 IOSCO Board，保留新興市場委員會，並將原執行委員會下之常任委員會（Standing Committees）和工作小組（Working Groups）整併為 8 個委員會，包括會計審計暨資訊揭露委員會、次級市場委員會、市場中介機構委員會、執法及資訊交換暨多邊資訊交換合作備忘錄審查小組委員會、投資管理委員會、信用評等機構委員會、商品期貨市場委員會及個人（散戶）投資者委員會，經本會之爭取及努力下，本會獲准加入「會計審計暨資訊揭露」、「信用評等機構」、「個人（散戶）投資者」等三個委員會。

信用評等機構委員會（下稱 C6 委員會）於 2017 年 12 月 5 日至 6 日假巴西里約舉行 2017 年第 3 次會議，本次會議計有澳洲、巴西、德國、香港、以色列、韓國、加拿大、俄羅斯、西班牙、土耳其、英國、美國、歐盟（歐洲證券暨市場監理總署[1]）及我國等 14 國（地區）代表與會，我國係由金融監督管理委員會證券期貨局曾稽核煌鈞及李科員志偉代表出席。

本次會議議程包括 IOSCO 秘書處及各會員國代表就國際監理動態進行報告及分享、討論信用評等機構「委外作業及雲端計算」（Outsourcing and Cloud Computing）專案之問卷回復結果，邀請巴西央行及業者就委外作業及雲端計算之實務作業進行簡報分享，以及就 C6 委員會後續發展進行討論。

[1]歐洲證券暨市場監理總署 European Securities and Markets Authority，ESMA

貳、 IOSCO 秘書處報告及國際監理動態

一、IOSCO 秘書處（下稱秘書處）報告

IOSCO 理事會（下稱理事會）2017 年 9 月於西班牙舉行理事會議，其中因應網路資安議題成立了專案小組（task force）；另鑒於歐盟一般資料保護規章（General Data Protection Regulation，GDPR）將於 2018 年 5 月施行，理事會亦針對資料保密及隱私問題加以討論；理事會並針對首次代幣發行（ICO）議題予以討論，其中多國代表均發表意見，認為 ICO 行為是否屬有價證券仍應回歸基礎面判斷。

二、C6 會員就其監理動態進行報告，重點摘要如下：

（一）韓國：正在研擬建置一個用以揭露發行人評等、債務評等及基金評等的公共平台。

（二）英國：英國國會正在討論將歐盟立法置入英國法規中，以確保其延續性，並降低對公司及投資人之衝擊。信用評等機構相關法規亦為其中一環，英國金融市場行為監管局（Financial Conduct Authority, FCA）刻正提供相關資料，目前仍尚待國會確認。

（三）我國：甫於 2017 年 11 月進行 2 年 1 度的信用評等事業訪查，訪查內容包括 2016 年「信用評等事業管理規則」修訂條文之辦理情形，對於資訊安全之內部控制制度，其他業務之發展情形等事項。

（四）歐盟：持續進行對於其他國家的評等相當性評估作業，此外，ESMA 修正評等認可的指引[2]，已於 2017 年 11 月 17 日發布，自 2019 年 1 月 1 日生效。

[2]Guidelines on the application of the endorsement regime under the CRA (Credit Rating Agencies) Regulation

參、「委外作業及雲端計算」專案背景

C6 委員會於 2017 年啟動「委外作業及雲端計算」(Outsourcing and Cloud Computing）專案（下稱本專案），以探討委外作業如何與雲端計算整合，以及信用評等機構如何於全球關聯企業集團中運用委外作業及雲端計算，以及如何透過信用評等機構關聯企業網絡以發布信用評等及提供「其他業務」。

此外，本專案將評估委外作業與雲端計算是否適用 IOSCO 的相關規章，包括市場中介機構委外作業原則（IOSCO's Principles on Outsourcing of Financial Services for Market Intermediaries)、信用評等機構業務原則（The Principles Regarding the Activities of CRAs)、信用評等機構行為準則（IOSCO's Code of Conduct Fundamentals for CRAs）等，或是否需要建立規範信用評等機構委外作業之準則。

一、 專案背景

委外作業在金融服務業扮演重要的角色，近年來，信用評等機構業已增加委外作業之使用範圍，以期達到降低業務成本、增加獲利及提升生產力等策略性目的。而隨著員工成本逐漸上升，以及服務提供者所能進行的委外作業日益多樣化及專精，委外作業之模式已有多樣化之發展。

C6 委員會表示，本專案與投資人保護及市場健全發展相關，並符合理事會 2017 年關注領域之工作重點，預期本專案將使會員深入瞭解信用評等機構之委外作業及雲端計算對其業務及組織之影響，以及信用評等機構如何因應及管理新科技應用所帶來的風險。

二、 專案範圍及目標

由於委外作業將信用評等流程切分為片段，並分散於集團

內不同國家之各分支機構進行，另雲端計算可能產生之風險包括各信用評等機構可能集中使用部分服務提供者，以及信用評等機構可掌握於雲端存取其數據資料之能力程度。經 C6 委員會廣泛的討論以及信用評等機構監理官聯席會(Supervisory Colleges for CRAs)之建議，認為委外作業及雲端計算係信用評等事業重要的發展趨勢，而有進行專案研討作業細節及相關風險之必要性。

經由本專案，C6 委員會將檢視信用評等機構如何進行及管理委外作業及雲端計算，並與信用評等機構組織及策略進行整合；另一方面，C6 委員會將評估信用評等機構對於委外作業及雲端計算相關法規以及 IOSCO 規範遵循情形，並考量是否需訂定規範以進行監管。

三、 專案進行概況：

IOSCO 理事會於 2017 年第 1 季核可 C6 委員會對於本專案之提案後，C6 委員會即著手草擬本專案問卷，並於 2017 年 8 月 17 日發送問卷予各會員國之信用評等機構，本會亦邀請中華信評股份有限公司（下稱中華信評）參與問卷調查。C6 委員會於此次會議邀請信用評等機構進行簡報，並組成工作小組草擬諮詢報告，預計於 2018 年第 1 季及第 2 季發布公眾諮詢報告及徵詢公眾意見後，於 2018 年第 3 季將專案報告陳送理事會核可後正式發布。

四、 本次會議

C6 委員會除邀請信用評等機構簡報，另邀請巴西央行、伊塔烏銀行及雲端服務廠商（微軟）就「委外作業及雲端計算」專案進行簡報，並分別從監管面、法遵面及實務運作等角度切入探討，詳細內容請見下節。

肆、 簡報

一、 此次 C6 會議由以色列、歐盟及加拿大與會代表先總結並簡報「委外作業及雲端計算」專案之問卷回復結果，其中特別檢視大型信評機構（穆迪、標準普爾、惠譽、DBRS）之回復內容，另邀集穆迪、標準普爾、惠譽進行簡報及進行問答，內容整理如下：

（一）問卷回復總覽：共計有 22 家信評機構回復問卷，其中有 7 家信評機構表示並未委外任何涉及評等流程之業務，6 家信評機構表示無委外任何業務，而大型信評機構中，穆迪及標準普爾有委外部分評等流程業務。

（二）委外作業流程：

1. 某些信評機構進行委外決策時，係視欲委外的功能或業務之性質，採取個案（case by case）基礎，決定哪些人員需要參與決策。
2. 某些信評機構係先確認欲委外的業務，而後進行評估和挑選第三方供應商的流程。
3. 通常涉及委外決策的人員或功能包括：CEO、管理高層、委外業務直接相關部門、財務、IT、法遵、內部稽核、風險管理...等。
4. 標準普爾：其母公司 S&P Global Inc.已訂定供應商委外政策，標準普爾依該政策訂定供應商管理計畫，並設立供應商管理辦公室，作為委外作業流程管理的主要單位。
5. 穆迪：亦訂定內部政策及程序作為委外作業流程的指導，視委外業務是否屬「重要作業事項」(Important

Operational Functions, IOFs[3]）而有所不同，若 IOFs 委外可能對穆迪的內部控制產生妨礙，則該等 IOFs 不應委外，而對於委外的 IOFs，穆迪則依據內部政策及程序以選擇服務供應商。

（三）對供應商的盡職調查（Due Diligence）：

1. 某些信評機構未進行盡職調查，主係：
   （1）僅零星使用委外服務。
   （2）委外對象為知名的大型供應商。
   （3）委外對象為集團內關聯企業。
2. 盡職調查的項目通常包括：
   （1）供應商的業務穩定性。
   （2）聲譽（技術面及財務面）。
   （3）財務狀況（銀行往來或稅務資料）。
   （4）資安維護標準。
   （5）過去的績效。
   （6）國家風險。
   （7）ISO 27001 Information Security Policy on Outsourcing。
3. 標準普爾：依據其供應商管理政策（Vendor Governance Policy），分為締約前及締約後之盡職調查。
   （1）締約前對供應商進行三階段風險評估程序：
      a. 重大性評估。
      b. 聘用風險評估。
      c. 供應商風險評估。

[3] 包括向媒體發送評等公告、對網站的內容備份、維護私有評等資訊的管理及發送平台、對某些全球性金融機構的財務資料服務、對於分析師之教育訓練及證照考試、法令規定申報書件支援服務、評等平臺、資料中心、伺服器、服務中心、電子郵件管理、網路服務、資料庫管理、災難復原服務、支援商業活動之軟體支援、資訊系統支援、外部雲端系統及內部系統之及時整合等項目。

（2）締約後依據供應商之風險等級進行下列監測活動：

a. 服務水準協議（Service Level Agreement，SLA）遵循情形之監控。

b. 檢視供應商之聲譽變化（是否有違反法規、客戶抱怨情形、業界地位）。

c. 供應商員工及重要人員流動情形。

d. 定期檢視營運持續計畫／災難復原計畫。

e. 持續監控資訊安全。

f. 實地訪查供應商，與供應商管理階層面談，並檢視供應商之內部控管環境。

g. 每季進行供應商關係討論會議。

h. 定期就供應商之風險評分進行摘要陳報，包括供應商風險評估、控制管理文件、及供應商監控等執行情形。

4. 穆迪：若委外業務屬重要作業事項，將會執行相對應的風險評估流程，另於聘用後會持續進行監控以及年度檢視。風險評估所考量的風險包括資料損失、網路安全、聲譽風險、作業風險、經營退出風險、交易對手風險、國家風險、合約風險、存取風險及集中度風險等。

5. 惠譽：盡職調查的程度與性質取決於委外作業項目的性質，而且必須依據所訂流程經高階主管的審核。

（四）挑選第三方供應商的考量因素：

1. 多數信評機構共同考量的因素包括供應商的品質、效率、及時性、成本、能否達到法規要求的標準及是否能符合信評機構的最佳利益。另委外業務的項目多屬標準化流程下的重複性工作，或是需求頻繁且要求之

技術性低的非核心業務，且該項業務之委外不會妨害信用評等的品質，並應遵循相關內部控制、行為準則，以及監理機關之法令規定。

2. 標準普爾：除上述因素外，亦衡量供應商可提供的資源以及可提供服務的地區、供應商的核心業務能力、創新能力及技術能力、溝通及回復能力及專業推薦等非價格因素。
3. 穆迪：除上述因素外，亦衡量供應商交付情形、服務目標、整合、技術專長、財務穩定性、組織和管理、聲譽、資訊系統和基礎設施、可擴展性、通訊設施、保險、資訊安全措施、符合穆迪內部規範之能力及供應商的所在地。
4. 惠譽：除上述因素外，亦衡量供應商資料/智慧財產（IP）所有權、能否強化信用分析與研究能力、與資訊系統的相容性與網路安全、是否符合市場常規及業務項目的依賴性等。
5. DBRS：其考量因素因委外業務項目而有所差異，主係依據盡職調查的結果進行評估，包括供應商的聲譽、專業及經驗、管理品質、資安維護能力等。

（五）針對轉包商（subcontractor）的管理：

1. 標準普爾：其與供應商的標準格式協議中已訂有要求轉包商遵守標準普爾政策之規定，且其針對供應商的監管活動亦包括轉包商。
2. 穆迪：其針對供應商風險評估的流程包括瞭解是否有業務再次委外予轉包商；另合約內容給予穆迪保留對委外廠商（包括轉包商）合適的管理權利。
3. 惠譽：原則不允許轉包的行為；例外僅有資料管理

（data management）業務，且轉包商必須遵守相關的服務合約規範並受到管理。

4. DBRS：其委外對象多屬知名且聲譽佳的服務供應商，通常不會要求渠等廠商揭露委外轉包商的情形，惟供應商需對提供予 DBRS 的服務負起全責。

（六）信評機構之內部控制、政策及流程是否適用於第三方服務提供者：

1. 對第三方供應商員工實施教育訓練：若委外業務項目涉及資料謄寫或複製、保密性、法遵議題、軟體開發方法...等，才會對供應商員工執行教育訓練；另可能視委外供應商類型決定是否需要對其員工實施教育訓練。
2. 標準普爾：與供應商間所簽訂之「主要專業服務協議」（Master Professional Services Agreement ）中包括要求供應商遵守標準普爾之相關政策及程序，此外，標準普爾的供應商行為準則（Vendor Code of Conduct）中亦列示供應商對於處理資料以及對於安全及保密之要求。
3. 穆迪：藉由合約要求第三方服務提供者遵循必要的政策及程序。
4. 惠譽：重要的服務供應商必須遵守惠譽所有相關的政策及程序，必須（1）採行嚴謹程度等於或高於 ISO27001 的程序，以維護惠譽資料的安全；（2）確保可辨視身分資訊的保護措施，以符合所有相關的資料保護法規；以及（3）為惠譽資料保密，並確保該等資料僅用於特定服務。
5. DBRS：目前委外業務項目均未涉及該公司機密資料

或內部系統，爰未要求服務供應商遵循該公司之政策或程序規定。

（七）與第三方服務提供者之利益衝突議題：

1. 標準普爾：於供應商管理政策、供應商行為準則及員工業務道德規範（Employee Code of Business Ethics）中規範對於利益衝突之辨視、預防、報告及處理之要點。其中員工業務道德規範中說明可能存有利益衝突的情形包括違反標準普爾及其客戶之最大利益、行為不當以及對於標準普爾之忠誠有疑慮等。
2. 穆迪：與所有第三方服務供應商皆有簽訂合約，其中包括機密資料的保護協議，藉由限制發送及使用機密資料，穆迪得以對委外作業維持適當控制，並將發生利益衝突的可能性降到最低。
3. 惠譽：依據其經驗，因第三方服務供應商產生的利益衝突情形範圍實屬有限。
4. DBRS：潛在的利益衝突情形應於委外作業過程中發現，當下制定並實施減緩計畫。

（八）風險管理議題：

1. 小型信評機構視委外業務之重要性決定風險評估作業的執行程度，如屬非核心業務，甚至未事先進行風險評估。
2. 風險減緩措施：
   （1）盡可能選擇市占率高、市場聲譽佳或是曾有合作經驗的供應商。
   （2）訂定緊急應變計畫及內部備援方案。
   （3）對供應商進行持續監督。
   （4）擬具帶有罰款的嚴格服務水準協議（SLAs）。

（5）具備到供應商現地檢查或稽核的權利。

（6）於供應商合約中載明相關的義務及保護條款。

3. 無法承受之風險：若干信評機構表示未曾面臨過此類風險，標準普爾表示如發現此類風險，將會選擇不與該供應商簽約。

4. 針對第三方服務提供者發生停業（如破產）或產生財務或法律上困難的情形，是否具有緊急應變計畫：

（1）標準普爾：針對內部評估後而辨視為高風險等級之供應商，進行更嚴謹的監控，另對於某些委外作業（如資訊系統），標準普爾會聘用數個供應商；此外，標準普爾針對關鍵的流程、系統及工具均持續更新及維護相關文件以確保具備迅速且不費力更換新供應商的能力。

（2）穆迪：重視使用供應商知識及其他相關工具的權利，以於第三方服務供應商面臨破產或其他影響其提供服務的事件時，將相關工作轉移到新的供應商或將其移轉至內部執行；另目前有使用雲端服務作為災難復原計畫之一環（例如官方網站的備用伺服器是在雲端系統）。

（3）惠譽：已作好失去（並迅速更換）第三方供應商的準備。

（4）DBRS：藉由委外予多家供應商以降低單一供應商中斷服務的風險。

（九）雲端計算使用現況：

1. 三大信評機構均有使用雲端服務，惟未將涉及評等分析核心業務委外予雲端服務供應商。

2. 標準普爾：使用雲端計算的情形包括私有雲、公有雲、

混合雲及多層雲等模式。其官方網站 S&P.com 是集團內第 1 個使用雲端的基礎設施服務（IaaS）的案例，現正評估將 S&P.com 更多功能及某些非核心業務移至雲端運作，曾接洽過 Microsoft 及 Amazon。

3. 穆迪：於 2013 年開始使用雲端服務，惟使用情形僅限於某些特定的客戶關係管理流程及災害復原計畫。目前不考慮將內部作業轉移到外部雲端服務，但仍將定期檢視其可行性。此外，穆迪擁有數個內部資料中心，預期未來可能會採用雲端服務，以減少資料中心的數目。

4. 惠譽：採用結合主機共置資料中心與公共雲端運作的模式，有關主機共置資料中心的部分，惠譽已與 SunGuard 簽訂協議，另惠譽自 2015 年第 4 季開始研究將業務移至亞馬遜網路服務（AWS）雲端平台之可行性，2016 年第 1 季起開始運用雲端服務，相關進度整理如下表。

時間	主要進度
2015 年第 4 季~2016 年第 1 季	開始研究及評估將系統移轉至 AWS 雲端平台之可行性、經濟效益及風險，並訂定風險管理計畫。
2016 年第 2 季~2016 年第 3 季	成立雲端工程團隊（Cloud Engineering Team）、發展詳細計畫及設立相關標準，並開始安裝可應用系統的基礎元件。
2016 年第 4 季	若干關鍵系統順利移至 AWS 雲端平台。
2017 年第 1 季~2017 年第 2 季	共計超過 100 項系統移至 AWS 雲端平台，執行大規模系統測試並將結果文件化。
2017 年第 4 季	主機共置業務規模將縮小近 60%。

（十）C6 與會成員發言摘要：

1. 目前多數信評機構未將評等業務相關系統移至雲端運作，即便有如惠譽使用雲端運算者，仍保留整個系統的管理權和所有權，目前僅使用雲端業者的資源，但未將評等業務直接委外與雲端業者，然隨著人工智慧的發展，未來信用評等事業有無可能將量化分析的工作直接委外予雲端運算或人工智慧，此是值得持續注意的議題。
2. 雲端服務業者聲稱已符合法令所要求的規範標準，客戶端（金融機構）不必再進行稽核工作，但主管機關多仍會要求金融機構應完成相關的內部稽核以確保作業流程均依規定進行，但部分雲端廠商擔心讓客戶稽核會影響到資料的獨立性及隱私而不願意讓客戶進行稽核工作（特別是涉及實體資料庫的現地查核），此點會是主管機關、金融機構及雲端業者需要共同解決的問題。

二、 巴西央行（Banco Central do Brasil）－A Brazilian financial regulatory approach to information technology outsourcing services / cloud based services

（一）巴西央行的主要任務係維持該國貨幣購買力及金融系統的穩定性，針對金融機構採取多項規管（regulation）及監督（supervision）活動，此節簡報由該行分享針對資訊科技委外服務或雲端服務的金融監管方法。

（二）巴西央行於 2017 年通過針對資訊科技金融監理之草案（下稱該草案），其主要內容包括：

1、 要求金融機構建立資訊安全政策：金融機構應負責確

保其委外的服務項目具備可靠、完善、安全及機密性，並確認遵循相關法律規範，即便採取委外策略，金融機構仍需採取相關的監督或風險管理措施。

2、 對於資料處理或儲存採委外服務或雲端服務者，有下列各項規定：

（1）資料儲存、處理及管理的地點及資料進行儲存或傳輸時所採取的安全措施均有特定規範，其中針對某些特定資料的儲存及處理，禁止委外予國外服務廠商（包括雲端服務商）。

（2）與委外廠商簽訂的合約條款必須確保金融機構的盡職調查，並給予巴西央行進入第三方服務供應商的相關設施之權利。

（3）金融機構須在巴西境內保留一份資料副本以供巴西央行隨時可取得。

（4）為降低關鍵 IT 委外服務商或雲端供應商無法提供服務之影響，金融機構須建立相關的預防程序，並進行替換第三方供應商的情境測試。

（5）金融機構須向主管機關申報委外廠商發生之資安事件。

（三）該草案之公眾諮詢期間於 2017 年 11 月 21 日結束，巴西央行收到來自金融機構、IT 服務提供商、法律專家及學者共計超過 76 個意見，巴西央行理事會將提出修正版本草案，提交國家貨幣委員會（National Monetary Council[4]）進行最終審視。

[4] 成員包括：財政部部長、發展規劃部部長（The Minister of planning, development and management）及央行總裁

三、 伊塔烏銀行（Banco Itaú）－Cloud Computing

（一）伊塔烏銀行總部位於巴西聖保羅，係一跨國企業，其在北美洲、南美洲、歐洲及亞洲均設有分支機構，2017 年 9 月底市值約 890 億美元。此節簡報該行分享為何選擇雲端服務，其主要策略及效益何在，另說明相關的法律議題及在巴西如何遵守針對雲端服務的規範。

（二）為何選用公用雲（public cloud）：

1. 及時性（Time to market）：採用雲端服務可因應市場需求推出新服務或產能，藉由運用最新科技，提高企業經營之靈活性，另搭配自動化的應用程式生命週期管理（automated application lifecycle management），能適時推出新服務，減少空窗期。
2. 管理便利性（Management and control）：透由雲端服務商，企業更容易完成系統安全的維護、使用者權限之管理及達到相關法令遵循或認證。
3. 提升資料庫效率（Datacenter efficiency）：企業營運所需的 IT 資源、計算力（computing power）或資料庫可依需求隨時擴充，透過自動化資源配置管理達到最適規模，企業也不必負擔閒置的硬體成本，省下的費用可回饋予消費者。
4. 監控（Governance）：採用雲端服務，企業確有使用的資源（計算力、軟體）才須付費（pay by use），透由計費標準細緻化，企業能更精準安排哪些功能適合採雲端運作，以改善公司之營運模式及競爭力。
5. 其他因素：某些服務或產品僅限透由雲端服務取得（IBM Watson、Microsoft Cortana、Google DeepMind）。

（三）伊塔烏銀行採用雲端服務之過程及現況：

1. 實地參訪雲端服務商，直接與供應商對談，除評估其服務架構之安全性，也可參考其他公司是如何選用雲端服務，伊塔烏銀行並強調透由實地參訪，可更清楚瞭解供應商的文化，這點是選擇供應商重要因素之一。
2. 建立屬於自身的雲端專門知識中心（Cloud Center of Expertise）：該中心負責決定採用雲端服務的策略，後續如何進行監控，並訂定相關的政策及風險評估架構以支援雲端活動。
3. 目前伊塔烏銀行針對雲端服務採取的風險監控管理大致可分為技術、安全性、法遵、委外管理及稽核等面向。

（四）面臨的法律或巴西法規遵循議題：

1. 金融機構選擇雲端服務，考量的法律議題包括：
   （1）安全及保密性：雲端服務者是否具備足夠的能力抵擋網路駭客攻擊，避免資料外洩，及確保資料未遭未授權的使用者讀取或濫用。
   （2）可取得性：金融機構必須擁有資料最終的掌控權，即便將部分功能委外予雲端服務商，金融機構仍須對主管機關及客戶負起全部責任，無論資料是儲存在何地（可能在巴西境外，或非儲存在金融機構本身的資料庫），金融機構都應該有隨時讀取資料的能力，並因應主管機關需要隨時提供相關資料。
   （3）企業永續性：企業選擇雲端服務時，會優先考量容易備份或迅速移轉資料的特性，以備有更換雲端服務商的不時之需。

2. 巴西法規要求：

（1）有關銀行營運及交易資料的數位化文件及其副本必須儲存在巴西境內；自然人透過網路或 App 開戶或結清之電子文件也須儲存在巴西境內。

（2）巴西央行得具備取得有關 IT 或數位外業務委外契約及相關資料的權利。

3. 針對巴西央行 2017 年通過之草案，伊塔烏銀行提出之看法及建議：

草案內容：禁止將特定資料（relevant data）的儲存及處理委外予國外服務廠商（包括雲端服務商），且備份資料亦應儲存在巴西境內，如現有在巴西境外儲存或處理的資料，應於 2021 年前移回巴西。

業界看法：此舉將導致巴西的金融機構難以使用雲端服務，限制其使用最新科技完成龐大的資料處理，進一步將影響其創新和競爭力；另資料集中儲存在巴西，未必能提高安全性，反增加其易攻擊性。

業界建議：不應採直接禁止的管理，縱使資料之實體儲存地點不在巴西境內，透過金融機構採取必要的風險管理政策，要求金融機構具備邏輯上（logically）100%獲取資料的能力，並有向主管機關申報的義務，也能達到主管機關原始監理目的。

草案內容：要求將特定條款納入與委外供應商的合約。

業界看法：太多或太特定的條款將導致金融機構難以委外其業務。

業界建議：應採取原則性規範，重點應在於要求金融機構具備風險管理措施，並與委外業者簽訂適當的書面合約，而非要求特定的條款文字。

四、 Microsoft – Leveraging Opportunity without compromising security

（一）此次會議邀請微軟分享雲端產業的未來發展與金融產業的應用，並加強說明如何運用數位科技完成法令遵循或內部稽核工作。

（二）Microsoft Azure：係微軟的公用雲端服務平台，屬微軟線上服務（Microsoft Online Services）的一部份，自 2008 年開始發展，2010 年 2 月正式推出，目前全球有 42 座資料中心[5]。透過此平台，微軟可提供資料倉儲、巨量資料分析、備份與封存、災害復原、高效能運算、各種服務應用程式...等雲端服務。以下針對資安維護、法令遵循、稽核等功能服務加以說明。

（三）資安維護功能：

1. 使用者可將部分資安維護責任轉移予雲端平台：對傳統企業而言，資安維護需投入大量資源，且要面面俱到才能抵擋駭客攻擊。透由將某些領域（實體網路或資料庫的建置、作業系統、應用程式）的資安維護工作轉交給雲端業者，企業可以將資源分配到較為高端及關鍵的功能（資料的監視、使用者權限管理），進而達到更高安全等級的資安防護。
2. Microsoft Azure Security Center：
   （1）主動偵測資安漏洞：找出並迅速回應駭客攻擊或滲透，並建立復原方案，使資料外洩或竄改的損害降到最低。
   （2）建立持續的系統掃描及資安維護計畫，提升偵測

[5] 在大陸亦設有北京與上海 2 座資料中心，非由微軟直接經營，而係由大陸代理商世紀互聯公司（21vianet）所經營，因此可用的服務較全球服務要少。

與復原的同步性。

（3）減少暴露於內部攻擊的風險：駭客或病毒一旦侵入公司系統內部，便有更多攻擊的管道。

（4）阻擋惡意或其他非必要的應用程式。

（5）專注最關鍵的威脅。

（四）法令遵循及稽核功能：主要協助企業的法遵部門及 IT 部門了解雲端產業的特性，並驗證有關資訊安全及資料保護控管作業是否確實符合最低法令要求。使用者可取得微軟雲端服務的稽核報告，了解如何透過微軟的雲端服務以完成對應不同國家的法規遵循架構，並取得相關文件以了解微軟的雲端服務是如何保護使用者資料：

1. 進階的資料控管：透過自動分類（automatic classification），依據使用者的年紀及類型、資料敏感性程度、使用者軌跡等因素，自動分析後將資料分類。並利用智能政策（intelligent policies）保留具有價值的資料，刪除多餘或太過瑣碎的資料。
2. 線上稽核經理（compliance manager）：透由線上稽核經理，企業可降低有關資料保存及風險評估的成本，投注較多精神在如何達到法規標準，並可做到即時風險評估，簡化稽核報告的作業流程。
3. 該平台目前可出具的相關法遵報告類型有：Archived Compliance Reports、FedRAMP Reports[6]、GRC Assessment Reports、ISO Reports 及 SOC Reports[7]。

[6] 聯邦風險與授權管理計劃（FedRAMP）是一項美國政府整體計劃，提供了標準方法來進行雲端產品和服務的安全評估、授權和持續監控。FedRAMP 要求雲端服務供應商接受第三方評估機構進行的獨立安全評估，以確保授權符合聯邦資訊安全管理法案規定。要向美國政府提供產品和服務的雲端供應商必須證明符合 FedRAMP 規定。FedRAMP 要求的詳細資訊，請參閱 www.FedRAMP.gov。（資料來源：Amazon Web Services）

[7] SOC（Service Organization Controls）：為因應客戶及合作夥伴多次稽核要求，並獲得更高信任，透過獨立第三方（如會計師事務所）對委外服務機構的流程及控制進行查核，包含對財報及資訊安全性、可用性、完整性 、機密或隱私的相關控制出具報告。

（五）C6 與會成員發言摘要：

1. 業務委外不代表相關責任亦隨之外移：現行金融機構普遍使用雲端服務，但主管機關仍要求金融機構本身對於雲端要有所管理，不能因為雲端供應商是知名企業而輕忽相關責任。
2. 資料儲存地之法規的影響：如報告前述，巴西近期提出關於資料儲存規定的草案，俄羅斯、阿根廷...等國亦有類似的規定，歐盟 GDPR 將於 2018 年 5 月正式實施，此類關於資料儲存或跨境傳輸的規定有無可能造成只有某些特定廠商得符合規範，致雲端服務業有大者恆大的現象。
3. 利益衝突考量：金融機構如將資料交給第三方供應商時，該廠商與金融機構自身客戶間的利益衝突問題該如何處理，尚待研究。
4. 如果主管機關跳過金融機構直接向雲端業者索取所需資料，雲端業者是否會配合提供，尚待持續觀察。

伍、 心得與建議

一、網路的普遍與企業全球經營的需求，雲端運算及相關服務的運用成為未來的必行趨勢，對信用評等事業在內的所有金融服務業而言，除考量如何運用雲端服務可使自身更具競爭力以提供市場所需的服務，也意識到運用最新科技時，「資安維護」及「法令遵循」是不可或缺的，同時也是各國主管機關最在意的議題。

二、各國政府鑒於大型雲端服務業者（Amazon、Google、Microsoft）、社群平台（Facebook、LINE）及知名跨國企業（Apple、Uber）均取得大量個人資料，近年來針對個人資料保護規範有更多著墨。以歐盟 2018 年 5 月即將正式實施的 GDPR 為例，跨境傳輸規定從現行「原則許可、例外禁止」改為「原則禁止、例外許可」，且不論在歐盟有無據點，只要蒐集、處理或利用到歐盟民眾個資均須受 GDPR 規範；另大陸也實施新的網路安全法，法案規定所有外國企業須將用戶資料與數據須實質存放在大陸境內且配合大陸審查，由於上述法令限制，「華碩雲端服務」評估後決定退出大陸市場[8]。此類資料儲存在地化及跨境傳輸限制的法令均會影響雲端產業的運作，進一步影響金融服務業使用雲端服務的可行性，若未來亞洲各國普遍對於個人資料保護有更嚴格的規範，屆時可能影響我國信用評等事業之雲端服務使用情形。

三、藉由參與本會議，本會得瞭解雲端服務產業的發展與實務運作，及國際間信用評等事業之運用現況，另於此次會議前本會甫完成對我國信用評等業者（中華信評及惠譽台灣分公司）之例行性訪查，此次會議亦有助於本會協助我國信用評等業

[8] 自由時報電子報，「不對中妥協，華碩關上海資料中心」，2018 年 2 月 13 日

者發展業務之同時予以適當監理。我國信用評等業者屬國際知名信用評等機構之子公司及分公司，其運用委外服務或雲端運算多係遵循母公司之政策並為一致性之管理，中華信評及惠譽台灣分公司自身雖較無主動管理權，惟透過配合母公司之相關作業程序及管理架構，得以完成相關法令遵循及資安維護作業，本會已提醒信用評等業者應注意遵循與母公司當地國不一致之法令規範。

四、本次會議期間，本會亦與其他主管機關保持積極互動，如與香港代表交流關於信用評等事業業務人員（如分析師）是否有專任限制，其資格條件或需取得之證照為何，俾為本會監理之參考；另本會將持續瞭解我國信用評等事業對於「委外作業及雲端計算」之運用情形，並參考該專案相關報告內容，予以適當之監理。

附件資料

附件 1：議程資料

附件 2：簡報資料