澳 門 金 融 管 理 局
AUTORIDADE MONETÁRIA DE MACAU

傳閱文件 021/B/2023-DSB/AMCM
(日期: 二零二三年十二月二十八日)

雲技術外判的補充說明

隨著雲計算技術的興起，更多澳門獲許可機構開始探索使用外部雲服務供應商（Cloud Service Provider, "CSP"）提供的雲計算服務，以提高其營運效能。雖然採納雲計算服務帶來包括業務敏捷性、擴展性及成本節約等優勢，惟機構須妥善識別、處理及監控因採用雲外判安排（"雲安排"）而產生的風險和挑戰。

《雲技術外判的補充說明》（"補充說明"）是 AMCM《外判管理指引》的補充。

引言

1. 本補充說明的目的為概述 AMCM 對雲安排的要求，以及獲許可機構在採用雲安排時需考慮的重要審慎要求。

2. 雲計算服務包括一系列可快速配置及釋放、並可依需求而使用的可調整且共享的（如網絡、伺服器、存儲設備、應用程序和服務等）計算資源。

3. 雲計算服務能以多種模式進行部署，每種部署模式有著不同的固有風險和需考量的審慎事項。這些服務和部署模式包括：
   (a) 服務模式：
      - 軟件即服務 ("SaaS") – 提供完全基於雲計算技術的應用程序，並由 CSP 管理及託管。
      - 平台即服務 ("PaaS") – 提供開發及／或應用程序的平台服務，如數據庫、應用程序平台、文件存儲及協作工具，以促進開發、測試和部署工作。
      - 基礎設施即服務 ("IaaS") – 提供可依需求配置的基礎計算設施服務，如計算、儲存和網絡服務。
   (b) 部署模式：
      - 公共雲 – 通過互聯網向公眾提供的雲基礎設施，有關設施的所有組件由 CSP 擁有和管理。

- 私有雲 – 供單一組織專用的雲基礎設施。有關設施可由該組織或第三方所管理和運營，並可部署於組織場所內或外。
- 社區雲 – 供特定組織群體專用的雲基礎設施，這些組織有共同的關注點（如使命、安全要求、政策和合規考慮）。有關設施可由一個或多個的組織群體、第三方、或前述兩者的組合所管理和運營，並可部署於組織場所內或外。
- 混合雲 – 由上述兩種或以上雲部署模式（即公共、私有或社區雲）所組成的雲基礎設施，這種部署保留每種模式獨有性質，並透過標準化或專有技術結合連接，以實現數據和應用程序的可轉移性。這種組成的雲基礎設施讓使用者利用每種模式所提供的優點（如在私有雲上存儲機密數據，並在公共雲上運行其他較不敏感的功能）。

適用範圍

4. 本補充說明適用於住所在澳門的獲許可機構，以及海外獲許可機構的澳門分行。在適用的情況下，此補充說明也適用於受 AMCM 監管的其他金融機構（但不包括從事保險業務及／或管理私人退休基金的機構）。

5. 本補充說明適用於符合《外判管理指引》中主要業務活動／功能定義的所有類型主要雲安排[1]，有關安排包括但不限於第 3(a)和 3(b)段所描述的各種雲服務和部署模式。具體而言，補充說明適用於獲許可機構將主要外判安排委託予一家 CSP，或機構所委託的服務供應商在提供服務過程中顯著依賴一家 CSP。

[1] 一些主要雲安排的例子如下：
(a) 儲存或處理客戶資料或員工數據，包括個人身份識別資料（“PII”）、敏感財務資料（如信用卡、薪資、銀行帳戶）以及在數據洩漏時可能會對客戶造成重大影響的其他數據；
(b) 業務運作系統，包括核心銀行應用程序、金融交易和交易系統；
(c) 涉及監管報表、會計資料或其他可能影響金融市場的非公開商業敏感資料的存儲或處理；
(d) 內部控制功能的系統，如審計、風險管理及合規等；及
(e) 獲許可機構定義為關鍵的外判業務活動。

6. 由於雲計算服務具有多租戶性、數據混合，且傾向於在多個地點進行數據儲存和處理的特性，獲許可機構須建立額外的控制措施，以管理主要雲安排及有關與數據存取、保密性、完整性、數據主權、安全性、可恢復性、合規性和審計等方面的風險。

7. 獲許可機構須在簽訂任何主要雲安排協議前，向 AMCM 諮詢並討論其計劃。

治理

8. 獲許可機構須建立有關雲外判的治理框架（“雲外判框架”），有關框架須與機構的整體業務、資訊科技策略及相關內部政策和程序保持一致。雲外判框架須清晰訂明管理雲安排的角色、責任、權力和所有權，而董事會、高級管理層及其他參與機構管理的相關方須對此有充分了解。董事會與高級管理層須定期檢視和審批雲外判框架，以管理雲安排中各個組成部份的相關風險。

9. 雲外判框架須至少包括以下部分：
   (a) 由業務需求、風險評估、盡職調查和新雲安排審批等所組成的規劃階段；
   (b) 獲許可機構內負責記錄、管理和監控雲安排的人員的角色和責任；
   (c) 持續監控和風險評估的程序；
   (d) 數據存儲地點和轉移的要求；
   (e) 雲訂閱和收費管理；
   (f) 安全控制；
   (g) 審計／審查的安排；
   (h) 業務持續性管理；
   (i) 退出策略。

10. 獲許可機構須建立適當的盡職調查流程，在開展雲外判前和雲外判期間評估 CSP 的服務水平和合適性。除了 AMCM 《外判管理指引》的要求外，評估還須包括雲服務特有的考慮因素，如多租戶風險、集中風險和供應鏈風險等。當雲服務的運營跨越多個地理位置時，機構須進行更深入的盡職調查，以評估有關海外司法管轄區所帶來的特定風險。

11. 獲許可機構須建立持續的監控和風險評估程序，以識別、監控及緩釋雲安排所涉及的風險。除了操作、網絡安全及系統恢復能力相關的風險外，機構還須注意，尤其在核心業務運作中的潛在集中度風險。為此，機構須定期審視：(i) 緊急應變計劃的完善度，包括數據和服務的互通性和可轉移性；(ii) 採用多個雲策略的可行性；(iii) 退出策略，以確保在必要時能及時退出。若 CSP 依賴第三方或供應商來履行其職能，機構須採取適當措施以管理潛在的供應鏈風險。此外，機構須建立機制，以持續確保 CSP 將按適用的行業標準妥善管理風險。

數據儲存位置及轉移

12. 獲許可機構將系統和數據遷移到雲端之前，須充分了解與數據處理相關的法律法規要求、合約條款和限制。機構須明確可接受處理和儲存數據的國家或司法管轄區並與 CSP 達成共識。機構須確保其可在 CSP 提出對數據存儲位置的不利變更時，有權按合約拒絕有關變更或終止外判協議。對於涉及將個人資料轉移至澳門以外的雲安排，機構須參考《個人資料保護法》中具體的通知、批准和控制要求。

外判協議

13. 除按 AMCM 《外判管理指引》的要求外，雲安排的協議亦須涵蓋以下事項：
    (a) 可接受的數據中心位置以支援獲許可機構的數據處理和儲存；
    (b) 對於數據中心位置變更的通知要求，包括通知時點和審批流程；
    (c) 在事故發生時，CSP 協助提供響應、調查和恢復的義務；及
    (d) 在退出過程中 CSP 的義務，包括但不限於協助進行充分的測試，以確保獲許可機構可順利將系統過渡至內部的環境，或其他 CSP 的雲環境。

14. 基於雲產品的特性，CSP 提供用量計費模式（即用多少付多少）的選項，可根據獲許可機構的雲服務使用情況來收費。在合約商議過程中，機構須與 CSP 就計費模式、關鍵服務使用量的監控及通知需要，如有關的監控平台和報告週期，達成共識。此外，機構須制定相應措施，以防止因超出預設配額而導致服務中斷。

審計／審查安排

15. 獲許可機構須定期對雲安排進行外部或內部審計，並在考慮有關的風險性質和程度，以及外判安排對機構的影響後，明確界定審計範圍和頻率。在滿足以下條件的前提下，機構可選擇採納第三方認證或具有等同效力的報告：
    (a) 進行審計的單位必須具備所需的專業知識與技能，且獨立於提供或支援雲安排所涉及的單位或功能；
    (b) 審計報告的範圍須涵蓋用於儲存或處理機構數據的 CSP 系統和其運作。

16. 獲許可機構有責任與 CSP 保持溝通，以確保有關審計發現得到適當且及時的補救。

額外的關鍵控制

17. 為進一步應對與雲安排相關的安全風險，獲許可機構須實施完善的安全控制措施，包括但不限於第 18 至 35 段內所列出的措施。取決於所部署的服務模式，機構有可能與 CSP 共同承擔管理和運營安全控制措施的責任。例如，在 SaaS 服務模式中，網絡安全風險通常由 CSP 管理；而在 IaaS 服務模式中，這可能是機構和 CSP 共同的責任。無論如何，機構仍有責任保護其資訊。因此，機構須按其雲安排的具體情況，識別並實施適當的控制措施。

(A) 架構設計

18. 獲許可機構須確保雲架構設計及底層基礎設施組件能提供高安全性、可用性、恢復能力和性能。機構須借助雲架構所提供的功能來提升系統彈性，例如自動擴展（auto-scaling）能力。此外，機構還須進行系統資源的健康檢查和實時監控，以檢測雲環境中的服務故障或中斷情況。

19. 為確保存取控制的安全性，在設計網絡架構時，須考慮常見的網絡安全威脅（如分散式阻斷服務攻擊），以及連接雲環境、邏輯隔離和公眾訪問的相關風險。在適用的情況下，須採用適當的技術來加強網絡隔離程度，如透過軟件定義網絡技術，分開多個虛擬網絡和雲用戶的帳戶／網絡分段。

(B) 虛擬化及容器化

20. 虛擬化和容器化是雲計算中使用的基礎技術，它們使資源池能夠更容易地被部署和按需求擴展或縮減。獲許可機構須明確在雲環境中實施和利用虛擬化及容器化技術時的安全標準，並須就機構與 CSP 之間的角色與責任達成共識，並以書面記錄作為操作參考。

21. 獲許可機構須對任何虛擬機（VM）或容器映像，設計並管理一套基準配置，以確保在雲環境中新創建的系統達到既定安全標準，並須對存取或更改虛擬機和容器映像的配置，實施存取和身份認證控制。

(C) 數據安全及加密

22. 獲許可機構須審查並確保現有數據分類政策已涵蓋了雲環境的考量。對在雲環境中儲存或處理的任何敏感信息，須考慮額外的安全控制，如先進的加密技術、標記化和邏輯隔離等措施。

23. 為加強對敏感信息的保護，獲許可機構須對傳輸中和靜止的敏感信息及其備份副本實施先進的加密算法。同時，須制定詳細的政策和程序，以規範加密材料的整個生命週期，包括生成、使用、更新至廢棄加密密鑰。此外，機構須實施強而有效的保護措施，如存取控制和加密控制等，以保護儲存在雲環境中的私密和其他加密密鑰的完整性。

24. 為識別和警示任何對如個人身份（“PII”）或支付相關等敏感信息的未經授權存取或變更，須部署監控或偵測的控制措施。如雲服務可通過互聯網訪問，須實施額外的預防資料外洩控制措施，如雲訪問安全代理（“CASB”）。

25. 獲許可機構須從 CSP 獲取並核實有關涵蓋支撐機構業務運營的數據中心的獨立評估報告，以確保已實施適當保護措施。同時，機構須確保 CSP 及時對獨立評估報告所識別的任何安全威脅、風險或安全問題採取補救措施。

(D) 應用程序安全

26. 如同獲許可機構於內部部署應用程序及相關的託管安排，機構須審視現有的系統開發生命週期（SDLC）流程，以確保雲環境特有的安全風險及相應的緩解策略已涵蓋到 SDLC 的各個階段。機構須按適用的監管要求、行業最佳實踐或內部指引進行如滲透測試和源代碼審查等安全測試。

27. 對於由 CSP 託管的應用程序（如在 SaaS 服務模式下的雲應用程序），獲許可機構須審查 CSP 所實施的安全控制措施，以確保雲應用程序的安全性。

(E) 身份識別及存取管理

28. 獲許可機構須更新有關身份和存取管理政策，以納入有關雲環境的用戶帳戶管理、存取權限及遠程訪問等控制措施。機構須密切關注雲環境的發展趨勢和威脅，並定期審核雲環境的身份和存取管理政策及控制措施，以確保這些政策和措施保持健全，且符合行業最佳實踐和標準。

29. 獲許可機須對雲服務和功能實施一致的用戶存取控制（如最小權限分配和職責分離）。用戶存取權限的變更，須由指定的負責人或獨立的部門進行評估和審核。若 CSP 的雲環境（如雲管理控制平台）可透過互聯網訪問，機構須尤其對特權帳戶的訪問，以及所有具權限訪問重要業務功能和涉及敏感或機密數據的活動的帳戶，實施高強度的身份驗證控制（如多因素身份驗證），以降低冒充和未經授權訪問數據的風險。

(F) 變更與配置管理

30. 獲許可機構須建立正式的變更管理流程並與 CSP 取得共識，以規範應用程序或配置變更的處理，包括提出變更請求、測試、撤回、審批、報告及責任等。為避免任何意外的服務中斷，須明確規定安裝修補程式和進行軟件更新的時間段。所有變更記錄須作保存以便日後的審計用途。

31. 獲許可機構須為雲環境設定基準配置，並定期進行審核以確保配置的合適性。倘發現偏離基準配置的情況，須發出警示。在個別須嚴格執行基準配置的情況，機構須部署自動化解決方案，將雲環境設定恢復到基準配置狀態。

(G) 事件及安全事故管理

32. 為確保雲環境的機密性、可用性和完整性，獲許可機構和 CSP 須有效地監控與網絡、基礎設施和應用程序有關的事件記錄。機構須採用合適的流程和工具，例如安全事故和事件監控（SIEM）工具，以自動執行記錄的整合，以及結合情報來源以進行關聯性分析。

33. 獲許可機構須制定清晰且有效的安全事故應對計劃，以確保能偵測並及時應對在雲環境中的安全事故。機構須就事故應對的角色、責任及通報流程與 CSP 達成共識，並將之記錄在事故應對計劃，以作為運營的參考。

(H) 業務持續性管理

34. 獲許可機構須為雲環境中的信息資產制定災難恢復計劃和程序，並定期進行測試（如對重要業務活動和功能至少每年進行一次），以驗證計劃和程序的有效性和完整性。對於重要的業務活動和功能，機構須盡可能與 CSP 一同進行測試，以確保有關服務能在短時間內恢復及滿足機構的業務恢復要求。在測試過程中若發現重大的控制缺陷，高級管理層須考慮、審核適當的跟進措施及進行密切監督，並向董事會報告。

(I) 培訓

35. 獲許可機構須確保負責管理雲安排的員工具備執行其職責所需的知識和技能。有關員工並須定期接受培訓，使他們的知識和技能得到更新，以確保雲技術的安全使用及相關風險得到妥善管理。

36. 獲許可機構須儘快及在本補充說明公佈後的 12 個月內，符合有關的要求。