MdME

LEGAL UPDATE 法律資訊

Guideline on Cloud Outsourcing for Insurance Sector
保險業務雲端外判管理指引之實施

To supplement the Guideline on Outsourcing Activities for the Insurance Sector, which will enter into force on 1 May 2025, the Monetary Authority of Macao ("AMCM") has issued the Guideline on Cloud Outsourcing Activities for the Insurance Sector (the "Supplementary Guideline"), which shall also become effective on the same date. The key provisions of the Supplementary Guideline are summarized as follows:

為配合補充將於 2025 年 5 月 1 日生效之《保險業務外判管理指引》，澳門金融管理局（下稱「AMCM」）現發出《保險業務雲端外判管理指引》（下稱「補充指引」），補充指引亦將於同日正式生效，其主要內容摘要如下：

Definition of Cloud Outsourcing under the Supplementary Guideline

（補充指引下之雲端外判）

Cloud computing services encompass a broad spectrum of services that provide on-demand access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services), which can be rapidly provisioned and released. These services can be delivered through various service and deployment models with detailed descriptions outlined in the Guideline.

雲端運算服務包括一系列能夠使用戶按需求存取共享的可配置運算資源（例如：網絡、伺服器、儲存、應用程式和服務）的服務並能快速進行資源配置及釋放。該等服務可透過不同的服務模式及部署模式提供，各模式的描述詳載於補充指引內。

Scope of Application（適用範圍）

The Supplementary Guideline applies to all authorized institutions, including insurers, reinsurers, and pension fund management companies incorporated in Macao, as well as the Macao branches of foreign institutions ("Authorized Institutions ").

It applies to all material cloud arrangements, including but not limited to, the service models and deployment models mentioned in the Supplementary Guideline that involving material business activities / functions, no matter the Authorised Institutions enter into outsourcing arrangements either directly with a Cloud Service Provider ("CSP") offering relevant material outsourcing services or with a service provider that relies significantly upon a CSP for the delivery of such services. Examples of material cloud outsourcing arrangements are provided in Appendix 1 of the Supplementary Guideline.

Whenever cloud services are arranged by the Authorised Institution's head office and extended to the Authorised Institution (even without a direct CSP-institution contract), the arrangement is still considered cloud outsourcing under the Supplementary Guideline. Under such circumstances, Authorised Institutions must:

- Document governance structures and oversight mechanisms set by the head office;
- Obtain assurance or attestations regularly from the head office on compliance with key risk management requirements;

- Implement local monitoring and oversight procedures for cloud services affecting their operations.

Even for non-material cloud outsourcing arrangements, Authorized Institutions should appropriately identify, address, and monitor potential risks by taking into consideration the nature, scale, and complexity involved.

補充指引適用於所有獲許可機構，包括在澳門登記成立的保險公司、再保險公司及退休基金管理公司以及海外獲許可機構的澳門分行（下稱「獲許可機構」）。

補充指引適用於所有涉及重要業務活動/功能的重要雲端安排，包括但不限於補充指引所述的各種服務模式和部署模式，無論獲許可機構係直接與提供相關重要外判服務之雲端服務供應者（下稱「CSP」）訂立外判安排，抑或與高度依賴 CSP 提供有關服務之其他服務供應商訂立外判安排，均屬適用範圍之內。

有關重大雲端外判安排之示例可參閱補充指引附件一。

若 CSP 由獲許可機構的總行聘用並延伸服務至獲許可機構，(即使 CSP 與獲許可機構沒有直接合約關係)，該雲端服務亦被視為補充指引下的雲端外判。在此情況下，獲許可機構應：

- 記錄並保存總行就雲端外判安排所建立的管治架構和監督機制的文件
- 定期從總行獲取並保存證明符合主要風險管理要求的證明或保證
- 對影響其營運的雲端服務實施適當的本地監控和監督程序

即使屬於非重要雲端外判安排，獲許可機構亦應考量相關服務的性質、規模及複雜程度以適當識別、處理及監察潛在的風險。

Due Diligence Requirements（盡職調查）

Authorised Institutions should perform thorough due diligence of a CSP before and throughout cloud arrangements, proportionate to the arrangement's complexity and materiality. Minimum areas of due diligence shall include the CSP's:

- Financial stability and viability
- Reputation and relevant experience
- Technical capability, robustness, and resilience of cloud infrastructure
- Information security and data protection measures
- Business continuity and disaster recovery plans

- Regulatory compliance and adherence to industry standards
- Contractual terms including service level agreements, liability, and termination rights

Additionally, cloud-specific risks such as multi-tenancy risks, concentration risks, and supply chain risks must also be assessed during due diligence. For cloud operations spanning multiple geographic regions, Authorised Institutions should also perform due diligence to address cross-border jurisdictional risks.

獲許可機構應建立適當之盡職調查程序，以於訂立雲端服務安排前及服務期間評估 CSP 之能力及適切性。盡職調查之範圍應與有關雲端安排之重要性及複雜程度相稱，並至少須涵蓋 CSP 之以下範疇：

- 財務穩定性和可行性
- 雲端服務提供方面的經驗和聲譽
- 技術能力，包括其雲端基礎設施的穩健性和恢復力
- 資訊安全和資料保護措施
- 業務持續性和災難恢復安排
- 監管合規性和對行業標準的遵守
- 合約條款和條件，包括服務水平協議、責任和終止權利

再者，多租戶風險、集中風險和供應鏈風險等因素亦應納入盡職調查之考量，在雲端營運跨越多個地理位置的情況下，獲許可機構應進行額外的盡職調查以評估境外司法管轄區的風險。

Regulatory Consultation（監管諮詢）

Authorised Institutions are required to consult and discuss their cloud outsourcing plans with AMCM before entering any material cloud arrangements.

在簽訂任何重要雲端安排的協議前，獲許可機構應與 AMCM 協商和討論其計劃。

Governance Framework（管治框架）

Authorised Institutions must establish a governance framework ("Framework") for cloud outsourcing aligned with their overall business and IT strategies, policies, and internal processes, or adapt existing outsourcing policies to address specific cloud risks. Moreover, responsibilities and authorities for managing cloud arrangements must be clearly defined, documented, and communicated to the board, senior management, and relevant stakeholders. The board and senior management are responsible for reviewing and approving this Framework, which must minimally address the follows:

- Planning Stage including Business requirements, risk assessments, due diligence, and approval processes
- Roles and Responsibilities of responsible personnel for documentation, management and monitoring
- Ongoing Monitoring and assessment procedures to outsourcing arrangements and CSPs
- Data Location and Transfer requirements
- Cloud Subscription and Billing Management
- Security Controls
- Audit / Review Arrangements
- Business Continuity Management
- Exit Strategy

獲許可機構應針對雲端外判安排建立管治框架（下稱「框架」），該框架應與獲許可之整體業務及資訊科技策略、內部政策及程序保持一致，或透過調整現有外判政策，以處理雲端服務特有之風險。此外，獲許可機構須清晰界定及記錄管理雲端安排之相關責任及授權，並向董事會、高級管理層及相關持份者清楚傳達。董事會及高級管理層須負責審查並批准框架，框架亦最少須涵蓋以下內容：

- 規劃階段包括業務需求、風險評估、盡職調查和新雲端安排的批准
- 負責記錄、管理和監控雲端安排的人員的角色和責任
- 針對雲端安排和 CSP 的持續監控和評估程序，以及時發現和獲悉的變更
- 數據位置和傳輸要求

- 雲端訂閱和計費管理
- 安全控制
- 審計/審查安排
- 業務持續性管理
- 退出策略

Regular Risk Assessment and Ongoing Monitor Mechanism

（定期風險評估及持續監控機制）

Authorised Institutions should conduct regular and comprehensive risk assessments and monitoring mechanism covering CSP's regulatory compliance, security controls, and data centre operations.

獲許可機構應定期進行全面的風險評估，並建立相關監控機制，以涵蓋雲端服務供應商（CSP）之法規遵循情況、安全控制措施及數據中心營運狀況。

Assessments must address potential operational, security, resilience, concentration, and supply-chain risks and the following elements should be reviewed regularly:

- Adequacy of Contingency Plan (data portability, interoperability)
- Feasibility of multi-cloud strategies
- Existence of Exit strategies to ensure smooth transitions when needed

相關評估須涵蓋營運、資訊安全、系統抵禦、集中風險及供應鏈等潛在風險，並應定期審查以下各項要素：

- 應變措施的充足性(數據和服務的互操作性和可攜性)
- 採用多雲策略的可行性
- 在必要時可及時退出的退出策略

Legal, Regulatory, and Data Handling:（法律、監管與資料處理）

Authorized Institutions should clearly understand relevant legal and regulatory frameworks, contractual obligations, and data location requirements before cloud migration. Data processing and storage jurisdictions should be agreed with CSPs, and Authorized Institutions should retain contractual rights to reject or terminate arrangements if unsuitable changes to data locations occur. Additionally, transfers of personal data outside Macao must notify/ request approval from the competent authority in accordance with the Personal Data Protection Law.

獲許可機構在將系統和數據遷移至雲端之前，應了解適用於數據處理的相關法律和監管框架、合約要求和限制。獲許可機構和 CSP 應確定並同意可接受的數據處理和儲存的司法管轄區。獲許可機構應保留在 CSP 變更不理想時拒絕擬變更或終止外判協議的合約權利。對於涉及個人數據跨境轉移的雲端安排，應根據《個人資料保護法》向具權限當局作出通知或提交批准申請。

Requirements for Cloud Outsourcing Arrangement Negotiation and Agreements

（雲端外判安排之磋商及協議）

Authorized Institutions should clearly agree with CSPs on billing models, usage monitoring, reporting requirements, and establish safeguards to prevent unexpected service cessation due to exceeded quotas.

獲許可機構應與 CSP 就計費模式、使用監控要求和主要服務的通知要求達成協議，並採取措施防止因超出配額酬做成服務中斷。

In addition to the requirements set forth in the Outsourcing Guideline for outsourcing agreement, cloud outsourcing agreements with CSPs should explicitly define:

- Data centre locations in supporting the Authorised Institution's data processing and storage
- Notification timelines and approval procedures for changes to data centre locations
- CSP obligations for incident response, investigation, recovery assistance, and support for exit processes

除《外判指引》所訂明的外判協議要求外，獲許可機構與雲端服務供應商（CSP）簽訂之雲端外判協議亦應明確界定以下事項：

- 支援獲許可機構數據處理和儲存的可接受數據中心位置
- 數據中心位置變更的通知要求包括通知時限和批准程序
- CSP 在發生事故時協助提供應對、調查、恢復和協助退出流程的責任

Post Notification to AMCM（向 AMCM 通報）

Material cloud outsourcing agreements and supporting documentation must be submitted to AMCM within 30 days, together with the form designated for the filing purpose.

重要雲端外判協議及相關文件須於協議訂立後 30 日內連同指定的申報表格一併提交至 AMCM 備案。

Audits or Certifications requirements（審計或認證要求）

Regular external or internal audits of cloud arrangements are required. Third-party certifications or reports from independent, reputable organizations may be accepted provided that the certifications or reports are:

- conducted by skilled, qualified, independent parties as listed in appendix 3 of the Supplementary Guideline.
- Cover relevant CSP systems and operations.
- up-to-date, applicable, and address key risk areas.

獲許可機構須定期對雲端安排進行外部或內部審計。倘獲許可機構採納由獨立及具信譽的第三方機構所發出的認證或報告，則有關認證或報告須符合以下條件：

- 進行審計的一方須具備必要的知識和技能，並為補充指引附件 3 所載之信譽良好和獨立的組織
- 涵蓋 CSP 用於儲存或處理獲許可機構數據的系統和營運
- 認證為最新並涵蓋主要風險領域

Cloud Security Control（雲端安全控制）

Authorised Institutions must implement robust security controls to mitigate risks associated with cloud arrangements. Responsibility for managing these controls may vary depending on the cloud service model adopted, in any case, Authorised Institutions remain ultimately accountable for safeguarding their information and must therefore proactively identify and apply the appropriate security controls relevant to their cloud arrangements.

Areas of security control are included but not limited as follows:

- Cloud´s Architectural Design
- Virtualisation and Containerisation
- Data Security and Encryption
- Application Security
- Identity and Access Management
- Change and Configuration Management
- Event and Security Incident Management
- Business Continuity Management

獲許可機構須採取穩健的安全控制措施，以降低與雲端安排相關之風險。儘管安全控制措施的管理責任或會因所部署的雲端服務模式而有所不同，惟獲許可機構在任何情況下，仍需對保護其資訊承擔責任。因此，獲許可機構應主動識別並適當實施相關之安全控制措施，以確保資訊安全獲得妥善保障。

雲端安全控制範疇包括但不限於：

- 架構設計
- 虛擬化和容器化
- 數據安全和加密
- 應用程序安全
- 身份和訪問管理
- 變更和配置管理
- 事件和安全事故管理
- 業務持續性管理

Date of Application（實施日期）

Authorised Institutions must fully comply with the Supplementary Guideline within 12 months of its issuance, i.e., by 1 May 2026. Existing Cloud Outsourcing Arrangements entered into before the effective date will be grandfathered, provided they are reviewed for compliance with the key principles of the Supplementary Guideline. If the review of material operational outsourcing arrangements is not completed within the stipulated period, Authorized Institutions must notify AMCM, outlining the planned measures or exit strategy, and may request an extension to complete the revision.

獲許可機構須在補充指引生效後的 12 個月內，即 2026 年 5 月 1 日前完全遵守相關規定，補充指引生效前訂立的現有外判安排和協議將獲得豁免，惟獲許可機構須就該等外判安排進行審查，確保其符合補充指引所訂明的主要原則及要求。如獲許可機構未能於上述期限內完成審查，須主動通知 AMCM 並說明其計劃採取的措施或退出策略，亦可向 AMCM 申請延期完成審查。

Our Contributor:

撰稿人：

Carlos Eduardo Coelho | 高革義
Partner | 合夥人

carlos.coelho@mdme.com
Visit Profile
個人簡介