Deloitte.

德勤

澳門金融管理局指引的最新發展

科技及操作風險管理指引的修訂概述

MAKING AN IMPACT THAT MATTERS since 1845

總體概述

隨著現代金融業的發展和新興技術的採用，新的業務模式和挑戰亦隨之而來。在促進發展的同時，澳門金融管理局（簡稱“金管局”）進一步優化了對金融科技方面的監管，以完善法規中的合規和安全要求。

2023年，金管局完善了與技術和操作風險管理相關的指引，當中包括：

- 《電子銀行風險管理指引》 (第005/B/2023-DSB/AMCM號傳閱文件)；
- 《科技及網絡風險管理指引》(第017/B/2023-DSB/AMCM號傳閱文件)；
- 《外判管理指引》(第020/B/2023-DSB/AMCM號傳閱文件)；
- 《雲技術的補充說明》 (第021/B/2023-DSB/AMCM號傳閱文件)。

科技及操作風險管理指引的關鍵里程碑

2008
- 電子銀行風險管理指引 [2023 年重新修訂]

2009
- 外判管理指引 [2023 年重新修訂]
- 業務持續管理指引

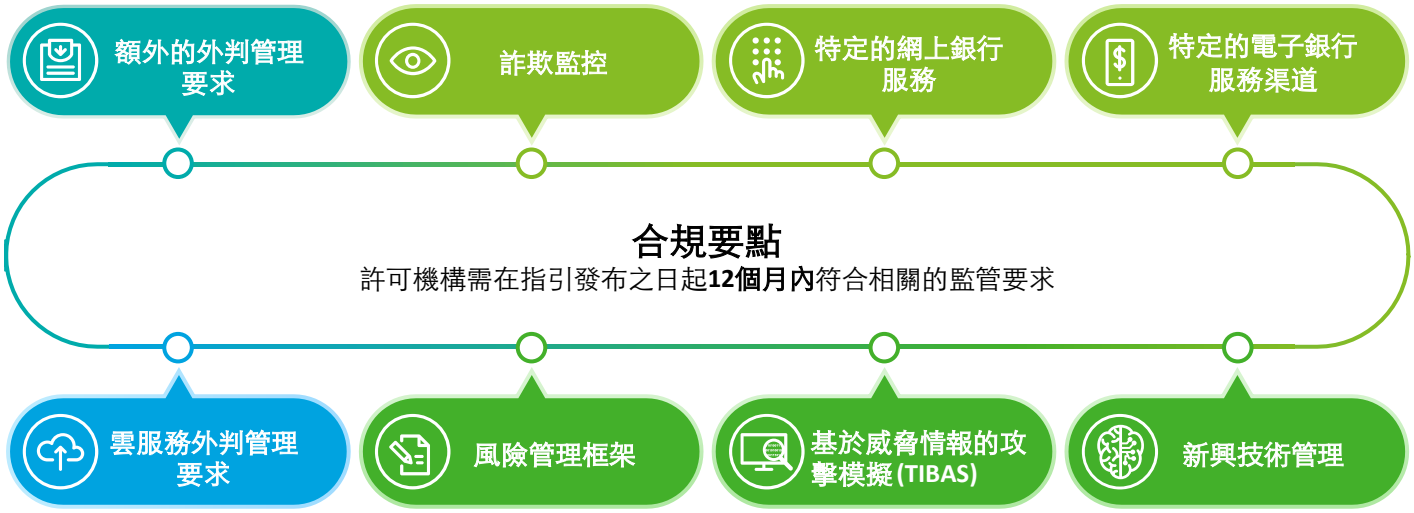
2019
- 網絡防衛指引 [2023 年重新修訂]

2023
- 電子銀行風險管理指引
- 科技及網絡風險管理指引 *[取代網絡防衛指引]*
- 外判管理指引
- 雲技術的補充說明 *[新]*

*備註: 本修訂概述的法規要求中文版本為非官方翻譯，實際條文請參考金管局官方指引。

金管局新修訂指引中的合規要點

以下是新修訂指引中所新增的控制要求主要內容，許可機構應盡快對現有的安全控制點進行差異分析，了解是否存在差異或違規的情況，並在修定指引生效後的 12 個月內完成相關的補救/修復措施。金管局將對許可機構進行實地視察及非實地審核，以確定許可機構是否符合相關法規的監管要求。



電子銀行風險管理指引(第005/B/2023-DSB/AMCM號傳閱文件)	科技及網絡風險管理指引(第017/B/2023-DSB/AMCM號傳閱文件)	外判管理指引(第020/B/2023-DSB/AMCM號傳閱文件)	雲技術的補充說明(第021/B/2023-DSB/AMCM號傳閱文件)

電子銀行風險管理指引
(第005/B/2023-DSB/AMCM號傳閱文件)

背景

金管局於2023年6月26日發佈了新修訂的《電子銀行風險管理指引》 (第005/B/2023-DSB/AMCM號傳閱文件)，該指引闡明了關鍵風險的管理原則，並從技術和營運角度，為許可機構就識別、評估和管理電子銀行相關風險提供指導。這些修訂包括完善通過網上銀行、自助終端和電話銀行渠道向客戶提供金融產品和服務的安全措施，並增加建立欺詐監測機制等要求，以識別、緩解和降低欺詐帶來的風險。

義務

#1 遵守修訂後的指引
許可機構應在2024 年 6 月前遵守此指引的要求

#2 獨立評估
在推出/上線電子銀行系統，或對現有服務進行重大變化之前，應進行獨立評估

#3 風險評估
完成 #2 後，應至少每兩年或在發生重大變化時進行一次風險評估

#4 技術評估
滲透測試和漏洞掃描應至少每年進行一次，評估結果應在金管局要求時提交

#5 向金管局提交報告
#2獨立評估報告應提交給金管局， 該報告將作為現場檢查和非現場審查的參考

適用於

在澳門註冊的許可信用機構或海外銀行在澳門的分行

所有正從事或將會從事電子銀行活動的信用機構

在提供服務時採用/將採用電子通訊渠道的以下機構:
(a) 根據第 15/83/M 號法令獲許可經營的財務公司；及
(b) 根據第 25/99/M 號法令獲許可經營的進行資產管理活動的機構；及
(c) 根據第 83/99/M 號法令獲許可經營的投資基金管理公司；及
(d) 根據《金融體系法律制度》獲許可經營的金融中介機構和其他金融機構。

主要更新詳情

安全領域

董事會和管理層的監督 | 安全控制 | 詐欺監控

業務持續計劃 | 外判管理 | 跨境活動管理

詐欺監控	制定欺詐監測機制	制定欺詐處理程序	建立欺詐監測和應對團隊	為工作人員提供相關培訓
業務持續計劃	定期進行容量規劃工作	制定業務連續性機制、事故應急和管理機制	定期進行系統事故應急計劃演習	實施自動性能監測和警報機制、進行端到端的性能測試
安全控制及其他範疇	補充身份驗證和授權控制方面的要求	補充對敏感資訊的加密算法的要求	新增對手機銀行（包括移動支付）的安全要求	新增技術安全評估要求，並應定期進行技術安全評估（如最少每年進行一次滲透測試和漏洞掃描）
	新增對網上銀行服務的安全要求（如資金轉帳、網上提交資料服務、遙距開戶服務、帳戶匯集服務及開放式應用程式介面）	新增對特定的提供電子銀行服務渠道的安全要求（如社交媒體平臺、自助服務終端機、手機銀行業務）	補充對客戶安全的要求（如客戶認知計劃、適時的通知及風險披露等）	

科技及網絡風險管理指引
(第017/B/2023-DSB/AMCM號傳閱文件)

背景

金融領域的科技和網路風險正在迅速變化，許多金融機構也在推行數字化，以提高營運效率並為客戶提供更好的服務。

金管局為協助許可機構提升對技術和網路風險的抵禦能力，於2023年12月11日發佈了新修訂的《科技及網絡風險管理指引》（第017/B/2023-DSB/AMCM號傳閱文件），取代了《網絡防衛指引》(第016/B/2019-DSB/AMCM號傳閱文件)。新指引包含了有關新興技術管理，和提升資訊科技開發和運營等要求，為許可機構提供技術和網路風險管理原則和最佳實踐的基礎。

義務

#1 遵守修訂後的指引
許可機構應在2024 年 12 月前遵守此指引的要求

#2 獨立評估
應至少每兩年進行一次獨立評估；或根據金管局的通知進行獨立評估

#3 向金管局提交報告
應在金管局要求時提供獨立評估報告，該報告將作為現場檢查和非現場審查的參考

適用於

- 在澳門註冊的信用機構或於海外註冊成立之銀行在澳門開設的分行
- 金融公司
- 現金速遞公司
- 資產管理公司
- 投資基金管理公司
- 其他金融機構

主要更新詳情

安全領域

科技及網絡風險管理框架 | 管治和策略 | 資訊科技項目管理和系統開發

資訊科技服務運營 | 網絡安全 | 應對和恢復 | 新興技術

科技及網絡風險管理框架	建立風險管理框架和風險管理流程
管治和策略	**提高授權機構及員工的情境意識** • 應包括新開發的技術 • 應包括行業威脅情報和資訊共享論壇，並訂閱威脅情報來源
資訊科技項目管理和系統開發	建立資訊科技項目管理架構以管理使用了科技的項目
資訊科技服務運營	完善遠端存取管理
應對和恢復	建立資訊科技問題管理
網絡安全	**密碼學** • 採用國際標準的加密演算法與加密密鑰的長度
	數據處置和銷毀 • 建立安全流程來管理數據處置和銷毀
	基於威脅情報的攻擊模擬 (TIBAS) • 建立客製化的端到端網路攻擊測試場景 • 在生產環境中執行以模擬現實生活中的攻擊場景，或考慮對與生產組件非常相似的模擬組件進行測試 • TIBAS 應由合格的測試人員進行
新興技術	**新興技術管理原則** • 建立治理框架和風險管理措施
	物聯網 (IoT) • 維護可連接到人工智慧網路/互聯網的所有物聯網設備的庫存（例如多功能印表機、安全攝影機和智慧電視） • 實施適當的安全措施（例如存取控制、監控等）
	人工智能（AI） • AI治理 • AI應用日誌記錄 • AI應用的數據安全 • 網路安全措施 • 應急措施
	分布式分類帳技術 (DLT) • 例如：區塊鏈 • 識別和評估潛在風險 • 參考其他治理框架/國際標準/最佳實踐

外判管理指引
(第020/B/2023-DSB/AMCM號傳閱文件)

背景

隨著外判在澳門日益普遍，越來越多的金融機構將其業務運營、維護和業務活動或功能外判給供應商，相關風險亦隨之而來。

為確保所有許可機構簽訂的全部外判安排，尤其是涉及重大業務活動或職能的外判安排，均經過適當的盡職調查、批准和持續監控；金管局於2023年12月28日發佈了新修訂的《外判管理指引 》(第020/B/2023-DSB/AMCM號傳閱文件)，此指引概述了金管局對許可機構的外判安排的監管要求，以及許可機構在簽訂外判安排時應考慮的關鍵問題。

外判定義

“外判”乃是許可機構將其部分業務的日常操作，一般在固定期間內，判給另一方（包括關聯方）辦理的安排。

義務

#1 遵守修訂後的指引
許可機構應在2024 年 12 月前遵守此指引的要求

#2 向金管局提交建議書，如涉及:
- 外判重要業務活動/功能;
- 重大變更/修改現有外判範圍

#3 持續監測
持續監控服務提供商的業績、財務狀況和風險狀況，管理與外判活動/功能相關的風險

適用於

在澳門註冊的許可機構以及海外註冊成立的許可機構澳門分行

其他由金管局監管的金融機構

主要更新詳情

風險評估

在進入/改變現有外判安排範圍之前進行風險評估

離場策略

制定離場策略，管理資料刪除/轉移、智慧財產權和資訊權、終止控制以及轉向其他服務提供者的過渡等

集中度風險

將集中風險納入風險管理框架和外判政策，包括：

a) 評估集中風險
b) 對發現的任何集中風險實施風險補救

保密

更詳細的保密要求，例如評估數據保護相關的安全控制、責任、定期審查和監控

分包

開展盡職調查，管理與分包相關的風險，並考慮采取以下控制措施：

a) 包含分包商責任條款
b) 保留終止合同的權利
c) 通知要求
d) 持續監控

雲服務外判管理
(參考《雲技術的補充說明》)

雲技術的補充說明
(第021/B/2023-DSB/AMCM號傳閱文件)

背景

隨著雲端運算技術的興起，更多澳門的許可機構開始採用第三方服務供應商提供的雲計算服務。 雖然雲計算服務的採用具有業務敏捷性、可擴展性和節省成本等優勢，但同時也會產生相應的風險。

金管局於2023年12月28日發佈了《雲技術的補充說明》 (第021/B/2023-DSB/AMCM號傳閱文件)，概述了金管局對許可機構使用雲計算服務的監管要求，以及許可機構在簽訂雲計算服務時應考慮的關鍵問題。

義務

#1遵守新增的指引
許可機構應在2024 年 12 月前遵守此指引的要求

#2 就應用新的雲服務諮詢金管局
在簽訂任何重要的雲服務協議之前，許可機構應與金管局協商和討論其計劃

適用於

在澳門註冊的許可機構以及海外註冊成立的許可機構澳門分行

其他由金管局監管的金融機構

本指引適用於所有雲服務的外判安排（“雲安排”），無論是外判給雲服務供應商（"CSP"）提供服務，還是依賴 CSP 提供服務。

所有類型的重大雲安排：

服務模型:
- 軟件即服務 (“SaaS”)
- 平臺即服務 (“PaaS”)
- 基礎設施即服務(“IaaS”)

部署模型:
- 公有雲 (Public Cloud)
- 私有雲 (Private Cloud)
- 社區雲 (Community Cloud)
- 混合雲 (Hybrid Cloud)

主要更新詳情

安全領域

治理 | 數據位置和傳輸 | 審計/審查安排 | 外判協議 | 額外的關鍵控制

(A) 架構設計	(B) 虛擬化容器化	(C) 數據安全和加密	(D) 應用安全	(E) 身份和訪問管理	(F) 變更和配置管理
(G) 事件和安全事件管理	(H) 業務連續性管理	(I) 培訓	根據部署的服務模型，許可機構可能與雲服務供應商（CSPs）共同承擔安全控制的管理和運營責任，包括（A）到（I）。		

德勤如何提供協助？

德勤提供的是基於我們對您的業務需求和項目特點的理解，以及我們的經驗而**量身定制的服務和方法**，而不僅僅是提供一套標準化的服務。您可以根據自身需求的特徵、類型和監管要求，選擇最合適的評估和諮詢服務。德勤旨在提供專業、持續和靈活的服務模式，幫助您節省時間和人力成本。

獨立評估

- 全行合規性評估
- 電子銀行服務上線獨立評估
- 第三方評估
- 雲服務評估
- Swift CSP 評估
- 其他獨立評估

技術評估

- 漏洞掃描
- 移動應用和網站滲透測試
- 配置審查
- 紅隊演練
- 基於威脅情報的攻擊模擬 (TIBAS)

諮詢

- 制定及改進政策和程序，以實現安全和合規流程
- 設計適合客戶環境的科技及網絡風險管理框架
- 提供網絡安全意識培訓，以提升員工防禦網絡攻擊的能力

為什麼選擇德勤?

了解業界和您所面臨的挑戰

我們在**銀行業擁有豐富的知識**，在**為澳門、香港和中國客戶**交付類似客戶、規模和範圍的**項目方面積累了豐富的經驗**。這些經驗使我們了解客戶可能面臨的主要風險和問題，有助於我們的工作保持實用性和有效性。

强大的專業團隊

我們的項目合夥人擁有**超過十八年的專業經驗，我們的評估和技術團隊擁有多年的網絡安全諮詢服務經驗**。我們的專家具有 **CISSP、CISA、OSCP 和 CREST** 資格，他們的知識和專業技能能够爲項目帶來價值。

熟悉網絡安全發展和趨勢

我們精通澳門金融業的網絡安全現狀、監管要求和最佳實踐，了解各地的網絡安全及數據私隱的法律法規發展，以及最新的威脅情報。我們致力於幫助客戶解讀監管要求，改善網絡安全環境，並與客戶分享行業的最新趨勢。

開啟對話

如果您有興趣進一步了解我們的服務，請聯繫我們：

鄭偉傑
澳門分所主管合夥人

電話號碼：+853 8898 8898
電子郵件：sidcheng@deloitte.com.mo

鄭若琳
風險諮詢合夥人

電話號碼：+852 2238 7119
電子郵件：eicheng@deloitte.com.hk

李家敏
戰略客戶中心總監

電話號碼：+853 8898 8833
電子郵件：carlei@deloitte.com.mo

梁嘉碧
風險諮詢副總監

電話號碼：+852 2258 6266
電子郵件：beleong@deloitte.com.hk

MAKING AN IMPACT THAT MATTERS since 1845