Deloitte.

德勤

澳门金融管理局指引的最新发展

科技及操作风险管理指引的修订概述

MAKING AN IMPACT THAT MATTERS since 1845

总体概述

随着现代金融业的发展和新兴技术的采用，新的业务模式和挑战亦随之而来。在促进发展的同时，澳门金融管理局（简称“金管局”）进一步优化了对金融科技方面的监管，以完善法规中的合规和安全要求。

2023年，金管局完善了与技术和操作风险管理相关的指引，当中包括：

- 《电子银行风险管理指引》 (第005/B/2023-DSB/AMCM号传阅文件)；
- 《科技及网络风险管理指引》(第017/B/2023-DSB/AMCM号传阅文件)；
- 《外判管理指引》(第020/B/2023-DSB/AMCM号传阅文件)；
- 《云技术的补充说明》 (第021/B/2023-DSB/AMCM号传阅文件)。

科技及操作风险管理指引的关键里程碑

2008
- 电子银行风险管理指引 [2023 年重新修订]

2009
- 外判管理指引 [2023 年重新修订]
- 业务持续管理指引

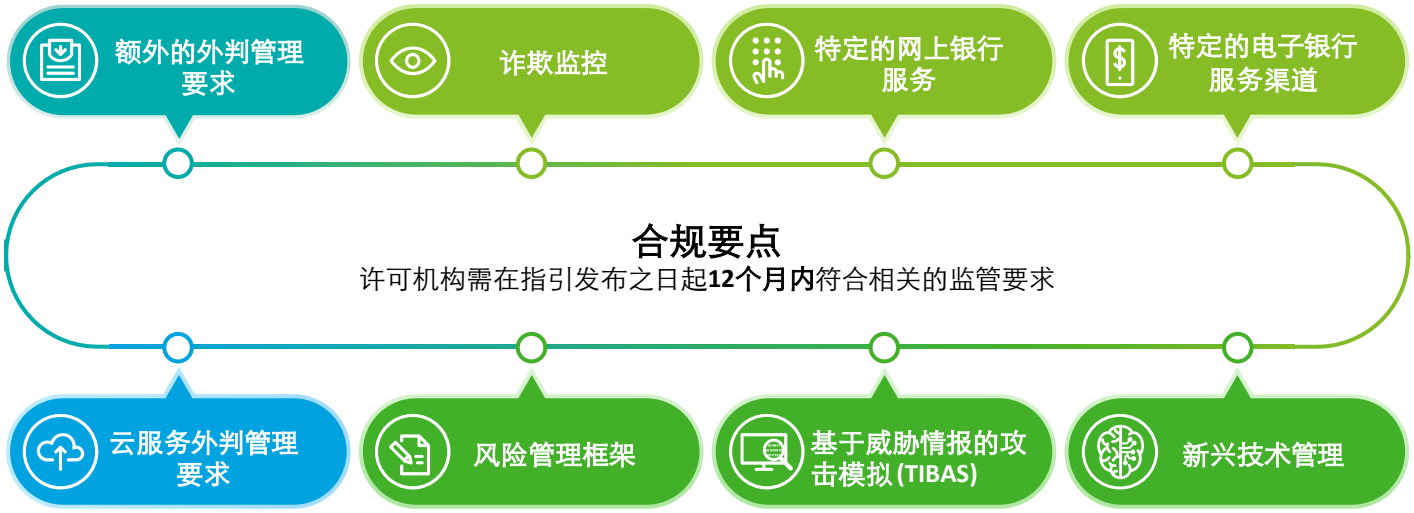
2019
- 网络防卫指引 [2023 年重新修订]

2023
- 电子银行风险管理指引
- 科技及网络风险管理指引 *[取代网络防卫指引]*
- 外判管理指引
- 云技术的补充说明 *[新]*

*备注: 本修订概述的法规要求中文版本为非官方翻译，实际条文请参考金管局官方指引。

金管局新修订指引中的合规要点

以下是新修订指引中所新增的控制要求主要内容，许可机构应尽快对现有的安全控制点进行差异分析，了解是否存在差异或违规的情况，并在修定指引生效后的 12 个月内完成相关的补救/修复措施。金管局将对许可机构进行实地视察及非实地审核，以确定许可机构是否符合相关法规的监管要求。



电子银行风险管理指引 (第005/B/2023-DSB/AMCM号传阅文件)	科技及网络风险管理指引 (第017/B/2023-DSB/AMCM号传阅文件)	外判管理指引 (第020/B/2023-DSB/AMCM号传阅文件)	云技术的补充说明 (第021/B/2023-DSB/AMCM号传阅文件)

电子银行风险管理指引
(第005/B/2023-DSB/AMCM号传阅文件)

背景

金管局于2023年6月26日发布了新修订的《电子银行风险管理指引》 (第005/B/2023-DSB/AMCM号传阅文件)，该指引阐明了关键风险的管理原则，并从技术和营运角度，为许可机构就识别、评估和管理电子银行相关风险提供指导。这些修订包括完善通过网上银行、自助终端和电话银行渠道向客户提供金融产品和服务的安全措施，并增加建立欺诈监测机制等要求，以识别、缓解和降低欺诈带来的风险。

义务

#1 遵守修订后的指引
许可机构应在2024 年 6 月前遵守此指引的要求

#2 独立评估
在推出/上线电子银行系统，或对现有服务进行重大变化之前，应进行独立评估

#3 风险评估
完成 #2 后，应至少每两年或在发生重大变化时进行一次风险评估

#4 技术评估
渗透测试和漏洞扫描应至少每年进行一次，评估结果应在金管局要求时提交

#5 向金管局提交报告
#2独立评估报告应提交给金管局， 该报告将作为现场检查和非现场审查的参考

适用于

在澳门注册的许可信用机构或海外银行在澳门的分行

所有正从事或将会从事电子银行活动的信用机构

在提供服务时采用/将采用电子通讯渠道的以下机构:
(a) 根据第 15/83/M 号法令获许可经营的财务公司；及
(b) 根据第 25/99/M 号法令获许可经营的进行资产管理活动的机构 ； 及
(c) 根据第 83/99/M 号法令获许可经营的投资基金管理公司；及
(d) 根据《金融体系法律制度》获许可经营的金融中介机构和其他金融机构。

主要更新详情

安全领域

董事会和管理层的监督 | 安全控制 | 诈欺监控

业务持续计划 | 外判管理 | 跨境活动管理

诈欺监控	制定欺诈监测机制	制定欺诈处理程序	建立欺诈监测和应对团队	为工作人员提供相关培训
业务持续计划	定期进行容量规划工作	制定业务连续性机制、事故应急和管理机制	定期进行系统事故应急计划演习	实施自动性能监测和警报机制、进行端到端的性能测试
安全控制及其他范畴	补充身份验证和授权控制方面的要求	补充对敏感资讯的加密算法的要求	新增对手机银行（包括移动支付）的安全要求	新增技术安全评估要求，并应定期进行技术安全评估（如最少每年进行一次渗透测试和漏洞扫描）
	新增对网上银行服务的安全要求（如资金转账、网上提交资料服务、遥距开户服务、帐户汇集服务及开放式应用程式介面）	新增对特定的提供电子银行服务渠道的安全要求（如社交媒体平台、自助服务终端机、手机银行业务 ）	补充对客户安全的要求（如客户认知计划、适时的通知及风险披露等）	

科技及网络风险管理指引
(第017/B/2023-DSB/AMCM号传阅文件)

背景

金融领域的科技和网路风险正在迅速变化，许多金融机构也在推行数字化，以提高营运效率并为客户提供更好的服务。

金管局为协助许可机构提升对技术和网路风险的抵御能力，于2023年12月11日发布了新修订的《科技及网络风险管理指引》（第017/B/2023-DSB/AMCM号传阅文件），取代了《网络防卫指引》(第016/B/2019-DSB/AMCM号传阅文件)。新指引包含了有关新兴技术管理，和提升资讯科技开发和运营等要求，为许可机构提供技术和网路风险管理原则和最佳实践的基础。

义务

#1 遵守修订后的指引
许可机构应在2024 年 12 月前遵守此指引的要求

#2 独立评估
应至少每两年进行一次独立评估；或根据金管局的通知进行独立评估

#3 向金管局提交报告
应在金管局要求时提供独立评估报告，该报告将作为现场检查和非现场审查的参考

适用于

- 在澳门注册的信用机构或于海外注册成立之银行在澳门开设的分行
- 金融公司
- 现金速递公司
- 资产管理公司
- 投资基金管理公司
- 其他金融机构

主要更新详情

安全领域

科技及网络风险管理框架 | 管治和策略 | 资讯科技项目管理和系统开发

资讯科技服务运营 | 网络安全 | 应对和恢复 | 新兴技术

科技及网络风险管理框架	建立风险管理框架和风险管理流程	管治和策略	**提高授权机构及员工的情境意识** • 应包括新开发的技术 • 应包括行业威胁情报和资讯共享论坛，并订阅威胁情报来源		
资讯科技项目管理和系统开发	建立资讯科技项目管理架构以管理使用了科技的项目	资讯科技服务运营	完善远端存取管理	应对和恢复	建立资讯科技问题管理
网络安全	**密码学** • 采用国际标准的加密演算法与加密密钥的长度	**数据处置和销毁** • 建立安全流程来管理数据处置和销毁	**基于威胁情报的攻击模拟 (TIBAS)** • 建立客制化的端到端网路攻击测试场景 • 在生产环境中执行以模拟现实生活中的攻击场景，或考虑对与生产组件非常相似的模拟组件进行测试 • TIBAS 应由合格的测试人员进行		
新兴技术	**新兴技术管理原则** • 建立治理框架和风险管理措施	**物联网 (IoT)** • 维护可连接到人工智慧网路/互联网的所有物联网设备的库存（例如多功能印表机、安全摄影机和智慧电视） • 实施适当的安全措施（例如存取控制、监控等）	**人工智能（AI）** • AI治理 • AI应用日志记录 • AI应用的数据安全 • 网路安全措施 • 应急措施	**分布式分类账技术 (DLT)** • 例如：区块链 • 识别和评估潜在风险 • 参考其他治理框架/国际标准/最佳实践	

外判管理指引
(第020/B/2023-DSB/AMCM号传阅文件)

背景

随着外判在澳门日益普遍，越来越多的金融机构将其业务运营、维护和业务活动/功能外判给供应商，相关风险亦随之而来。

为确保所有许可机构签订的全部外判安排，尤其是涉及重大业务活动/职能的外判安排，均经过适宜的尽职调查、批准和持续监控；金管局于2023年12月28日发布了新修订的《外判管理指引》(第020/B/2023-DSB/AMCM号传阅文件)，此指引概述了金管局对许可机构的外判安排的监管要求，以及许可机构在签订外判安排时应考虑的关键问题。

外判定义

“外判”乃是许可机构将其部分业务的日常操作，一般在固定期间内，判给另一方（包括关联方）办理的安排。

义务

#1 遵守修订后的指引
许可机构应在2024 年 12 月前遵守此指引的要求

#2 向金管局提交建议书，如涉及:
- 外判重要业务活动/功能;
- 重大变更/修改现有外判范围

#3 持续监测
持续监控服务提供商的业绩、财务状况和风险状况，管理与外判活动/功能相关的风险

适用于

在澳门注册的许可机构以及海外注册成立的许可机构澳门分行

其他由金管局监管的金融机构

主要更新详情

风险评估

在进入/改变现有外判安排范围之前进行风险评估

离场策略

制定离场策略，管理资料删除/转移、智慧财产权和资讯权、终止控制以及转向其他服务提供者的过渡等

集中度风险

将集中风险纳入风险管理框架和外判政策，包括：

a) 评估集中风险
b) 对发现的任何集中风险实施风险补救

保密

更详细的保密要求，例如评估数据保护相关的安全控制、责任、定期审查和监控

分包

开展尽职调查，管理与分包相关的风险，并考虑采取以下控制措施：

a) 包含分包商责任条款
b) 保留终止合同的权利
c) 通知要求
d) 持续监控

云服务外判管理
（参考《云技术的补充说明》）

云技术的补充说明
(第021/B/2023-DSB/AMCM号传阅文件)

背景

随着云端运算技术的兴起，更多澳门的许可机构开始采用第三方服务供应商提供的云计算服务。 虽然云计算服务的采用具有业务敏捷性、可扩展性和节省成本等优势，但同时也会产生相应的风险。

金管局于2023年12月28日发布了《云技术的补充说明》 (第021/B/2023-DSB/AMCM号传阅文件)，概述了金管局对许可机构使用云计算服务的监管要求，以及许可机构在签订云计算服务时应考虑的关键问题。

义务

#1遵守新增的指引
许可机构应在2024 年 12 月前遵守此指引的要求

#2 就应用新的云服务咨询金管局
在签订任何重要的云服务协议之前，许可机构应与金管局协商和讨论其计划

适用于

在澳门注册的许可机构以及海外注册成立的许可机构澳门分行

其他由金管局监管的金融机构

本指引适用于所有云服务的外判安排（“云安排”），无论是外判给云服务供应商（"CSP"）提供服务，还是依赖 CSP 提供服务。

所有类型的重大云安排：

服务模型:
- 软件即服务 (“SaaS”)
- 平台即服务 (“PaaS”)
- 基础设施即服务(“IaaS”)

部署模型:
- 公有云 (Public Cloud)
- 私有云 (Private Cloud)
- 社区云 (Community Cloud)
- 混合云 (Hybrid Cloud)

主要更新详情

安全领域

治理 | 数据位置和传输 | 审计/审查安排 | 外判协议 | 额外的关键控制

(A) 架构设计	(B) 虚拟化容器化	(C) 数据安全和加密	(D) 应用安全	(E) 身份和访问管理	(F) 变更和配置管理
(G) 事件和安全事件管理	(H) 业务连续性管理	(I) 培训	根据部署的服务模型，许可机构可能与云服务供应商（CSPs）共同承担安全控制的管理和运营责任，包括（A）到（I）。		

德勤如何提供协助？

德勤提供的是基于我们对您的业务需求和项目特点的理解，以及我们的经验而**量身定制的服务和方法**，而不仅仅是提供一套标准化的服务。您可以根据自身需求的特征、类型和监管要求，选择最合适的评估和咨询服务。德勤旨在提供专业、持续和灵活的服务模式，帮助您节省时间和人力成本。

独立评估

- 全行合规性评估
- 电子银行服务上线独立评估
- 第三方评估
- 云服务评估
- Swift CSP 评估
- 其他独立评估

技术评估

- 漏洞扫描
- 移动应用和网站渗透测试
- 配置审查
- 红队演练
- 基于威胁情报的攻击模拟 (TIBAS)

咨询

- 制定及改进政策和程序，以实现安全和合规流程
- 设计适合客户环境的科技及网络风险管理框架
- 提供网络安全意识培训，以提升员工防御网络攻击的能力

为什么选择德勤?

了解业界和您所面临的挑战

我们在**银行业拥有丰富的知识**，在**为澳门、香港和中国客户**交付类似客户、规模和范围的**项目方面积累了丰富的经验**。这些经验使我们了解客户可能面临的主要风险和问题，有助于我们的工作保持实用性和有效性。

强大的专业团队

我们的项目合伙人拥有**超过十八年的专业经验，我们的评估和技术团队拥有多年的网络安全咨询服务经验**。我们的专家具有 **CISSP、CISA、OSCP 和 CREST** 资格，他们的知识和专业技能能够为项目带来价值。

熟悉网络安全发展和趋势

我们精通澳门金融业的网络安全现状、监管要求和最佳实践，了解各地的网络安全及数据私隐的法律法规发展，以及最新的威胁情报。我们致力于帮助客户解读监管要求，改善网络安全环境，并与客户分享行业的最新趋势。

开启对话

如果您有兴趣进一步了解我们的服务，请联系我们：

郑伟杰
澳门分所主管合伙人

电话号码：+853 8898 8898
电子邮件：sidcheng@deloitte.com.mo

郑若琳
风险咨询合伙人

电话号码：+852 2238 7119
电子邮件：eicheng@deloitte.com.hk

李家敏
战略客户中心总监

电话号码：+853 8898 8833
电子邮件：carlei@deloitte.com.mo

梁嘉碧
风险咨询副总监

电话号码：+852 2258 6266
电子邮件：beleong@deloitte.com.hk

MAKING AN IMPACT THAT MATTERS since 1845