第 2023/1 号通函：运营风险与韧性

Dr Alexander Ressos, TEP
Attorney-at-Law (Switzerland), Solicitor (Hong Kong),
Solicitor (England & Wales)

瑞士金融市场监管局（FINMA）2022 年 12 月 7 日第 2023/1 号通函《操作风险与韧性——银行》（“Operational risks and resilience – banks”）于 2024 年 1 月 1 日生效，取代了关于银行操作风险的第 2008/21 号通函。其中关于运营韧性的规定须在两年过渡期内实施，即在 2026 年 1 月 1 日之前完成。[1] 该通函载有关于信息和通信技术（ICT）风险管理、网络风险、关键数据、业务连续性管理和运营韧性的要求。机构必须将其 IT 系统的开发、测试和生产环境分离并对变更管理加以规范（边码 47 至 60）。机构必须识别网络威胁、保护其资产、发现攻击、应对事件并从中恢复；对于影响关键资产的成功网络攻击，必须在 24 小时内向 FINMA 报告，并在 72 小时内提交完整报告（边码 61 至 70）。[2]

该通函将关键数据定义为对提供服务或监管目的极为重要、因而需要加强安全措施的数据（边码 71 至 82）。[3] 用于训练或运行人工智能系统的客户数据往往属于此意义上的关键数据。业务连续性管理要求设定恢复时间目标和恢复点目标，制定连续性计划和灾难恢复计划，并定期进行测试（边码 83 至 96）。最后，运营韧性的概念要求机构识别其关键职能，并界定“中断容忍度”，即在严重但合理的情景下机构所能接受的关键职能最大中断程度，并定期加以测试（边码 97 至 114）。[4]

对卢加诺的银行而言，运营韧性要求意味着需要识别哪些职能（例如支付、托管和客户访问）属于关键职能，并梳理这些职能所依赖的人员、流程、技术、信息和提供商。如果某个人工智能系统已成为关键职能的一部分，例如一个缺之则无法放行支付的监控系统，机构就必须为其失效预作规划：退回人工流程、采用替代提供商或提供缩减的服务。FINMA 在第 08/2024 号指引中要求对备用方案进行记录，这正是连接两套规则的纽带。[5]

1 《信息安全法》规定的网络攻击报告义务

自 2025 年 4 月 1 日起，瑞士关键基础设施的运营者须向国家网络安全中心报告网络攻击；该中心已于 2024 年改组为联邦网络安全办公室（BACS）。这项义务通过修订《信息安全法》（ISA）而引入，适用对象包括银行、保险公司和金融市场基础设施等。如果攻击危及基础设施的运行、导致信息被篡改或外泄、长期未被发现，或与勒索、威胁或胁迫相关，则须在发现攻击后 24 小时内报告。自 2025 年 10 月 1 日起，违反报告义务可被处以最高 10 万瑞士法郎的罚款。[6] 因此，受 FINMA 监管的金融机构必须协调两条报告渠道：根据第 2023/1 号通函向 FINMA 报告，以及根据《信息安全法》向 BACS 报告。联邦当局已提供统一的报告表格，使一份报告即可同时满足两方面的要求。[7]

2 注释

1. FINMA 第 2023/1 号通函 “Operational risks and resilience – banks”，2022 年 12 月 7 日，https://www.finma.ch/en/~/media/finma/dokumente/dokumentencenter/myfinma/ rundschreiben/finma-rs-2023-01-20221207.pdf?la=en。
2. FINMA 第 2023/1 号通函（同上），边码 47–70。
3. FINMA 第 2023/1 号通函（同上），边码 71–82。

4. FINMA 第 2023/1 号通函（同上），边码 83–114。
5. FINMA，第 08/2024 号指引（同上），第 2.5 节。
6. 2020 年 12 月 18 日《联邦信息安全法》（Information Security Act，ISA），SR 128，第 74a–74h 条及第 74e 条（处罚），经 2023 年 9 月 29 日联邦法律修订；2025 年 3 月 7 日《网络安全条例》（CSO），SR 128.51。自 2025 年 4 月 1 日起生效，处罚自 2025 年 10 月 1 日起适用。
7. 联邦网络安全办公室（BACS），关于报告义务及报告表格的信息。

仅供一般参考。本文不构成法律或税务意见，不能替代针对个案的专业意见，亦不建立律师与客户关系。本文反映截至 2026 年 9 月的法律状况。

在线版本：cn.helveticaregister.com/lugano-circular-2023-1-operational-risks-and-resilience