

网络安全与运营韧性

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

数字化有其另一面：脆弱性。金融机构是网络攻击的首选目标，无论是勒索软件、网络钓鱼，还是通过入侵供应商实施的攻击。日内瓦金融中心拥有富裕客户和大宗商品贸易商，是首要目标之一。瑞士金融市场监管局（FINMA）通过其关于运营风险的通函，要求受监管机构管理 IT 风险，并在二十四小时内报告严重的网络攻击。2025 年，联邦针对关键基础设施遭受的网络攻击引入了一般性报告义务。¹ 已知案例（其中数起涉及瑞士法语区的机构）表明，成功的攻击往往针对机构的服务提供商，而这些提供商的安全受到的监控不如机构本身严密。²

运营韧性不仅限于网络安全。它关系到机构在发生故障、攻击、供应商失灵或灾难时维持其关键职能的能力，其前提是识别这些职能、设定情景、进行测试并制定恢复计划。欧盟（EU）已通过一部关于数字运营韧性的法规，自 2025 年 1 月起适用，对机构及其关键 IT 服务提供商施加了详细要求。隶属于欧洲集团或为欧盟境内客户提供服务的日内瓦机构感受到了其间接影响。³ 此外，云服务和银行系统提供商集中于少数几家公司，且几乎全部为美国公司，由此形成的依赖如今已被瑞士和欧洲当局视为一种系统性风险。

注意。将 IT 外包给云服务提供商转移的是执行，但责任仍然保留机构仍须就数据的保密性、可用性和完整性对其客户和 FINMA 负责，包括提供商设立于境外并受可能要求其向本国当局披露数据的法律约束的情形。

1 注释

1. FINMA 第 2023/1 号通函 “Operational risks and resilience – banks”，取代第 2008/21 号通函，自 2024 年 1 月 1 日起施行（The Governance Law Firm, “Révision de la FINMA : circulaire Risques et résilience opérationnels – banques”，thegovernancelawfirm.com）；关键基础设施遭受网络攻击后须在二十四小时内向国家网络安全中心（NCSC）报告的义务，以《信息安全法》为依据，自 2025 年 4 月 1 日起施行，自 2025 年 10 月 1 日起适用处罚（NCSC, “L’obligation de signaler les cyberattaques contre des infrastructures critiques entre en vigueur le 1er avril 2025”, bacs.admin.ch）。
2. FINMA, 专题 “Cyber risks (2024)”以及 2024 年 6 月 7 日关于第 03/2024 号监管通告的新闻稿（finma.ch）：2024 年报告的成功或部分成功的网络攻击较上年增加 30%；勒索软件（PLAY、AKIRA 和 Lockbit 3.0 团伙）、商业电子邮件入侵、成波的拒绝服务攻击以及供应链攻击，后者约占所报告事件的三分之一；2022—2023 年报告的攻击中，半数以上涉及外包服务；报告义务以《瑞士金融市场监管法》第 29 条第 2 款（FINMASA）为依据；2023 年开展了十余次专门针对网络风险的现场检查。

3. 2022 年 12 月 14 日关于金融业数字运营韧性的第 2022/2554 号（欧盟）条例（《数字运营韧性法》，DORA），自 2025 年 1 月 17 日起适用：IT 风险管理、事件报告、韧性测试、第三方提供商风险；Autorité de contrôle prudentiel et de résolution，“Digital Operational Resilience Act (DORA)”，acpr.banque-france.fr（2026 年 9 月访问）。

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/geneva-cybersecurity-and-operational-resilience