

網絡安全與運營韌性

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

數碼化有其另一面：脆弱性。金融機構是網絡攻擊的首選目標，無論是勒索軟件、網絡釣魚，還是通過入侵供應商實施的攻擊。日內瓦金融中心擁有富裕客戶和大宗商品貿易商，是首要目標之一。瑞士金融市場監管局（FINMA）通過其關於運營風險的通函，要求受監管機構管理 IT 風險，並在二十四小時內報告嚴重的網絡攻擊。2025 年，聯邦針對關鍵基礎設施遭受的網絡攻擊引入了一般性報告義務。¹ 已知案例（其中數起涉及瑞士法語區的機構）表明，成功的攻擊往往針對機構的服務提供商，而這些提供商的安全受到的監控不如機構本身嚴密。²

運營韌性不僅限於網絡安全。它關係到機構在發生故障、攻擊、供應商失靈或災難時維持其關鍵職能的能力，其前提是識別這些職能、設定情景、進行測試並制定恢復計劃。歐盟（EU）已通過一部關於數字運營韌性的法規，自 2025 年 1 月起適用，對機構及其關鍵 IT 服務提供商施加了詳細要求。隸屬於歐洲集團或為歐盟境內客戶提供服務的日內瓦機構感受到了其間接影響。³ 此外，雲服務和銀行系統提供商集中於少數幾家公司，且幾乎全部為美國公司，由此形成的依賴如今已被瑞士和歐洲當局視為一種系統性風險。

注意。將 IT 外包給雲服務提供商轉移的是執行，但責任仍然保留機構仍須就數據的保密性、可用性和完整性對其客戶和 FINMA 負責，包括提供商設立於境外並受可能要求其向本國當局披露數據的法律約束的情形。

1 註釋

1. FINMA 第 2023/1 號通函 “Operational risks and resilience – banks”，取代第 2008/21 號通函，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）；關鍵基礎設施遭受網絡攻擊後須在二十四小時內向國家網絡安全中心（NCSC）報告的義務，以《資訊安全法》為依據，自 2025 年 4 月 1 日起施行，自 2025 年 10 月 1 日起適用處罰（NCSC，“L’obligation de signaler les cyberattaques contre des infrastructures critiques entre en vigueur le 1er avril 2025”，bacs.admin.ch）。
2. FINMA，專題 “Cyber risks (2024)” 以及 2024 年 6 月 7 日關於第 03/2024 號監管通告的新聞稿（finma.ch）：2024 年報告的成功或部分成功的網絡攻擊較上年增加 30%；勒索軟件（PLAY、AKIRA 和 Lockbit 3.0 團伙）、商業電郵入侵、成波的拒絕服務攻擊以及供應鏈攻擊，後者約佔所報告事件的三分之一；2022—2023 年報告的攻擊中，半數以上涉及外包服務；報告義務以《瑞士金融市場監管法》第 29 條第 2 款（FINMASA）為依據；2023 年開展了十餘次專門針對網絡風險的現場檢查。

3. 2022 年 12 月 14 日關於金融業數字運營韌性的第 2022/2554 號（歐盟）條例（《數字運營韌性法》，DORA），自 2025 年 1 月 17 日起適用：IT 風險管理、事件報告、韌性測試、第三方提供 商 風 險 ； Autorité de contrôle prudentiel et de résolution ， “ Digital Operational Resilience Act (DORA)” ， acpr.banque-france.fr（2026 年 9 月訪問）。

僅供一般參考。本文不構成法律或稅務意見，不能取代針對個別情況的專業意見，亦不建立律師與客戶關係。本文反映截至 2026 年 9 月的法律狀況。

網上版本：hk.helveticaregister.com/geneva-cybersecurity-and-operational-resilience