The Costs of Compliance

合规成本

Regulatory compliance is a basic fact of life in the financial industry,

affecting almost every system and every part of the organization; it

impacts system requirements, system design, testing, and operations,

as well as the personal conduct of industry employees.

监管合规是金融业的一个基本事实，几乎影响到组织的每个系统和每个部分；它影响系统需求、系统设计、测试和运营，以及行业员工的个人行为。

 Global firms are subject to multiple regulators and different compliance

regimes with overlapping and often conflicting requirements

for different business activities and financial products. In the US

alone, a bank could be subject to regulation by the OCC, the Federal

Reserve, the SEC, FINRA, the regulatory arms of the different

exchanges, the CFTC, and the FDIC.

全球公司受到多个监管机构和不同的合规制度的约束，针对不同的业务活动和金融产品，他们的要求重叠且经常相互冲突。仅在美国，银行就可能受到的监管来自货币监理署(OCC)、联邦储备委员会，SEC，FINRA，不同的交易所的监管机构、CFTC和FDIC。

Regulations like Dodd-Frank, GLBA, Regulation NMS, Regulation

SCI, and MiFID II (and of course, for public financial institutions,

SOX) impose mandatory reporting requirements; restrictions

around customer data privacy and integrity; mandatory operational

risk management and credit management requirements; mandatory

market rules for market data handling, order routing, trade execution, and trade reporting; rules for fraud protection and to protect

against money laundering, insider trading, and corruption; “know

your customer” rules; rules for handling data breaches and other

security incidents; business continuity requirements; restrictions on

and monitoring of personal conduct for employees; and auditing

and records retention requirements to prove all of this. Regulations

also impose uptime requirements for key services, as well as requirements

for reporting outages, data breaches, and other incidents and

for preannouncing and scheduling major system changes. This

means that regulatory compliance is woven deeply into the fabric of

business processes and IT systems and practices.

Dodd Frank、GLBA、全美市场系统规则、系统合规性和完整性规则、和Mifid II（当然，对于公共金融机构，还有SOX法案）都有强制报告要求；对于客户数据隐私和完整性的限制；强制运营风险管理和信贷管理要求；市场数据处理、订单路由、交易执行和交易报告的强制性市场规则；欺诈保护、防止洗钱、内幕交易和腐败的保护规则；“了解您的客户”的规则；处理数据泄露和其他安全事件的规则；业务连续性要求；对员工个人行为的限制和监控；以及审计并记录保存要求，以证明所有这些。法规同时对关键服务的正常运行时间有要求，以及要求报告停机、数据泄露和其他事件，以及对主要系统变更体现发布预告和时间表。这个这意味着监管合规性被深深地编织在业务流程、IT系统和实践中。

The costs and complexities of regulatory compliance can be overwhelming:

constant changes to compliance reporting requirements,

responding to internal and external audits, policies and procedures

that need to be continuously reviewed and updated and approved,

testing to make sure that all of the controls and procedures are being

followed. Paperwork is required to track testing and reviews and

approvals for system changes, and to respond to independent audits

on systems and controls.

法规遵从性的成本和复杂性可能是压倒性的：对合规报告要求的不断变化，响应内部和外部审计、政策和程序需要不断审查、更新和批准，实施测试以确保所有的控制和程序被遵守。测试、评审以及批准系统变更需要通过书面跟踪，并响应对系统和控制上的独立审计。