Regulation SCI and MiFID II

SCI和Mifid II 规则

In November 2015, the SEC’s Regulation Systems Compliance and

Integrity (Reg SCI) came into effect, as a way to deal with increasing

systemic market risks due to the financial industry’s reliance on

technology, including the widespread risk of cyber attacks. It is

designed to minimize the likelihood and impact of technology failures,

including the kinds of large-scale, public IT failures that we’ve

looked at so far.

2015年11月，SEC的系统合规性和完整性监管(Reg SCI)生效，作为一种应对日益增长的由于金融行业对于技术的依赖所带来的系统性市场风险，包括网络攻击的广泛风险。它是旨在将技术故障的可能性和影响降至最低，包括我们所能遇见到的的大规模公共IT故障。

Initially, Reg SCI only applies to US national stock exchanges and

other self-regulatory organizations (SROs) and large alternative

trading systems. However, the SEC is reviewing whether to extend

this regulation, or something similar, to other financial market participants,

including market makers, broker-dealers, investment advisers, and transfer agents.

最初，Reg Sci仅适用于美国国家证券交易所、其他自律组织（SROs）和大型另类交易系统。然而，SEC正在审查是否拓展这项规定，或类似于其他金融市场参与者，包括做市商、经纪商、投资顾问和过户代理。

Reg SCI covers IT governance and controls for capacity planning,

the design and testing of key systems, change control, cyber security,

disaster recovery, and operational monitoring, to ensure that

systems and controls are “reasonably designed” with sufficient

capacity, integrity, resiliency, availability, and security.

Reg Sci涵盖IT治理和能力，包括容量规划，关键系统的设计和测试、变更控制、网络安全，

灾难恢复和运营监控，以确保系统和控制“合理设计”，具备充分的容量、完整性、弹性、可用性和安全性。

It requires ongoing auditing and risk assessment, immediate notification

of problems and regular reporting to the SEC, industry-wide testing of business continuity planning (BCP) capabilities, and extensive record keeping for IT activities. Failure to implement appropriate controls and to report to the SEC when these controls fail could result in fines and legal action.

它需要持续的审计和风险评估，问题的及时报告和定期向SEC报告，整个行业的业务连续性规划（BCP）能力测试，以及详尽的IT活动记录。如果未实施适当的控制措施，并在这些措施失效时未及时向SEC报告，则可能导致罚款和法律诉讼。

In Europe, MiFID II regulations address many of the same areas,but extend to trading firms as well as execution venues like exchanges.

在欧洲，Mifid II法规涉及许多相同的领域，但扩展到交易机构和交易所等执行场所流。

What do these regulations mean to organizations adopting or looking

to adopt DevOps?

这些规定对实施或整准备实施DevOps的组织意味着什么？

The regulators have decided that relevant procedures and controls will be considered “reasonably designed” if they consistently follow

generally recognized standards—in the SEC’s case, these are published

government standards from the ISO and NIST (such as NIST 800-53). However, the burden is on regulated organizations to prove that their processes and control structures are adequate,whether they follow Waterfall-based development and ITIL, or Agile and DevOps practices.

监管机构认为，如果他们始终遵循公认标准，相关程序和控制措施将被视为“合理设计”。在SEC的案例中，其颁布了源自ISO和NIST（如NIST800～53）的政府标准。然而，负担在于被监管机构，它们要证明其过程和控制结构是充分的，无论他们遵循基于瀑布的开发和ITIL，或者敏捷和DevOps实践。

It is too soon to know how DevOps will be looked at by regulators

in this context. In Chapter 2 we’ll look at a “Compliance as Code”

approach for building compliance controls into DevOps practices,

to help meet different regulatory and governance requirements.

在这种情况下,关于监管机构将如何看待DevOps的论断还为时过早。在第2章中，我们将讨论通过“合规性即代码” 在DevOps实践中建立合规控制的方法，

帮助满足不同的监管和治理要求。