Deloitte.

Operational Integrity Enhancement

Securities Industry Analysis

CENTER *for*
REGULATORY
STRATEGY
AMERICAS

Securities

Over the past decade, our nation's securities markets have become deeply reliant on electronic trading systems and other sophisticated technologies, exposing securities firms, customers, and overall markets to higher levels of technology related risk. In an effort to mitigate this risk, regulators are raising the bar by issuing new requirements and guidance about how firms develop, test, implement, and monitor systems to ensure an adequate level of system capacity, integrity, availability, resilience, and security.

In the past, regulators tended to view technology problems as a standard part of business operations. But in the wake of numerous highly publicized technology problems that caused significant market disruptions and threatened the integrity of the financial system, regulators now expect firms that access and operate the markets to prevent problems before they occur—and to have technology governance structures and controls in place that are designed to ensure their systems operate smoothly, reliably, and in accordance with the rules and regulations.Key regulations, guidance, and regulatory trends include:

Regulation SCI (Systems Compliance and Integrity)[1]

This regulation applies to entities that operate the core components of the securities markets, including national securities exchanges, clearing agencies, securities information processors, and alternative trading systems. It requires firms to adopt, among other things, an IT governance framework and system controls that ensure an adequate level of integrity, availability, resilience, capacity, and security for systems that are necessary to maintain a fair and orderly market. Also, it prescribes minimum procedures that firms must establish to ensure functional integrity and system compliance, including development process and system change controls and inclusion of legal and regulatory staff in the design, review, and testing of certain system changes. Firms must monitor systems for disruptions, intrusions, and compliance events, and report these instances to the Securities and Exchange Commission (SEC) and impacted market participants. In addition, it requires firms to periodically test the design and effectiveness of the SCI program, including an annual review by objective personnel.

Adviser business continuity and transition plans

The SEC recently proposed a rule that would require SEC-registered investment advisers to "adopt and implement written business continuity and transition plans reasonably designed to address operational and other risks related to a significant disruption in the investment adviser's operations."[2] The proposed rule is a response to recent business disruptions that have recently impacted the financial services industry. These disruptions include operational issues such as a systems malfunction in August 2015 that, for several days, prevented a financial institution from calculating accurate net asset values (NAVs) for hundreds of mutual funds and exchange-traded funds. Disruptions also include natural disasters such as Hurricane Sandy. The goal of the proposed rule—and the SEC's related guidance[3]—s to address business continuity practices and the ability of market participants to continue operations in times of crisis. Key focus areas include: backup processes and contingency plans; monitoring incidents and communications protocols; understanding the interrelationship of critical service provider business continuity plans; and contemplating a variety of disruption scenarios.

FINRA Regulatory Notice 15-09[4]

This guidance applies to all broker-dealers that engage in algorithmic trading and is focused on ensuring the algorithms are developed with functional integrity and comply with all rules and regulations. It requires firms to perform a risk assessment of new algorithms or material changes to existing algorithms, including how the newly developed algorithm will interact with algorithms already in production. Broker-dealers should follow a software development and change management process that includes adequate levels of testing prior to placing algorithms into production. Pre-production testing should ensure an algorithm performs as intended and operates in accordance with all rules and regulations. To comply with this requirement, firms should review the completeness and effectiveness of test cases used in the regression-testing process with personnel that have knowledge of the rules and regulations. Also, to ensure appropriate supervision over the algorithms, brokerdealers should perform post-production monitoring and compliance checks, including periodic effectiveness testing of IT and compliance monitoring controls.

Digital investment advice (robo advisers)[5]

In March 2016, FINRA published its Report on Digital Investment Advice, which identifies practices that FINRA believes firms should consider and tailor to their business models. According to the report, digital investment advice tools support one or more of the following core activities in managing an investor's portfolio: customer profiling, asset allocation, portfolio selection, trade execution, portfolio rebalancing, tax-loss harvesting, and portfolio analysis. These investment advice tools can be broken down into two groups: tools that financial professionals use (financial

professional facing tools) and tools that clients use (client-facing) tools. Client-facing tools that incorporate the first six activities—customer profiling through tax-loss harvesting—are frequently referred to as "robo advisors" or "robos."

The report includes in-depth insights and recommended practices across a wide range of areas, including:

- Governance and supervision
- Investor profiling
- Rebalancing
- Training
- Lessons for investors

FINRA expects digital investment advice tools to play an increasingly important role in wealth management, and indicates investor protection should be a paramount objective as firms develop their digital investment advice capabilities. According to the report, firms need to establish and maintain an investor protection foundation that accounts for the considerations raised by digital investment advice. One key element of that foundation is understanding customer needs. Another is using tools with sound methodological groundings, and a third is understanding those tools' limitations. FINRA believes the effective practices outlined in its report will help firms advance investor protection objectives in their use of digital investment advice tools.

FINRA 2016 examination priorities

FINRA has indicated that technology issues will be a priority in its 2016 examination process. FINRA highlighted several areas of focus including (i) cybersecurity, (ii) change management and software development, (iii) data quality and governance, and (iv) outsourcing.

SEC Rule 15c3-5 Enforcement[6]

SEC Rule 15c3-5 is intended to address the risks that can arise as a result of the automated, rapid electronic trading strategies that exist today and to bolster the confidence of investors in the integrity of our markets. The rule is applicable to brokerdealers with access to trading securities by virtue of being an exchange member, an Alternative Trading System (ATS) subscriber, or an ATS operator with non-broker-dealer subscribers. Such broker-dealers with market access are required to establish, document, and maintain a system of risk management controls and supervisory procedures that, among other things, are reasonably designed to: (1) systematically limit the financial exposure of the broker or dealer that could arise as a result of market access and (2) ensure compliance with all regulatory requirements that are applicable in connection with market access.

Both the SEC and FINRA are bringing enforcement actions against firms for technology failures under SEC Rule 15c3-5. These cases generally involve technology that is coded incorrectly or a process failure occurs in the development process.

Regulation AT

This proposed regulation includes a series of risk controls, transparency measures, and other safeguards to improve transparency and reduce the potential risks associated with automated trading on designated

contract markets (DCMs). Regulation AT requires the implementation of risk controls—such as maximum order message and maximum order size parameters—as well as the establishment of standards for the development, testing, and monitoring of algorithmic trading systems. It also requires high-volume traders that use algorithmic trading for key futures products to register with the Commodity Futures Trading Commission (CFTC). Other requirements include the use of self-trade prevention tools by market participants on DCMs and the disclosure of rules and attributes of DCM electronic trade matching platforms that materially affect factors such as: the time, price, or quantity of execution of market participant orders; the ability to cancel or modify orders; and the transmission of market data and order or trade confirmations to market participants.[7]

FINRA cybersecurity guidance[8]

This guidance includes a summary of results from FINRA's examination of various broker-dealer information security programs. It provides insights and guidance on a wide range of leading practices that broker-dealers should incorporate into their information security programs, covering everything from governance and risk management to technical controls, information sharing, and vendor management.

National Futures Association (NFA) cybersecurity guidelines

NFA's Interpretive Notice to NFA Compliance Rules 2-9, 2-36, and 2-49 entitled "Information Systems Security Programs (Interpretive Notice)," effective March 1, 2016, requires all member firms to adopt and enforce written policies and procedures to secure customer data and access to their electronic systems.[9] The interpretive notice is designed to establish general requirements relating to members' information systems security programs (ISSPs), but to leave the exact form of an ISSP up to each member, thereby allowing the member flexibility to design and implement security standards, procedures, and practices that are appropriate for its circumstances. Given the rapidly changing nature of technology and threats to information systems, it's NFA's policy not to establish specific technology requirements.[10]

Cybersecurity preparedness and leading practices[11]

In 2015, the Office of Compliance Inspections and Examinations (OCIE) published a risk alert that presented findings from its study of cybersecurity preparedness and practices at 57 registered broker-dealers and 49 registered investment advisers. According to the study, a large majority of the examined broker-dealers (88 percent) and advisers (74 percent) have experienced cyberattacks directly or through one or more of their vendors—with most attacks taking the form of malware or fraudulent emails.

To help mitigate the cybersecurity problem, the vast majority of broker-dealers (93 percent) and advisers (83 percent) have adopted written information security policies, and most broker-dealers (89 percent) and advisers (57 percent) conduct periodic audits to determine compliance with these information security policies and procedures. Also, the vast majority of broker-dealers (93 percent) and advisers (79 percent) conduct periodic risk assessments on a firm-wide basis to identify cybersecurity threats, vulnerabilities, and potential business consequences. However, fewer broker-dealers (79 percent) and advisers (32 percent) require those same types of cybersecurity risk assessments of vendors with access to their firms' networks.

Many firms identify leading practices through information-sharing networks, and the vast majority conduct firm-wide inventorying, cataloging, or mapping of their technology resources. Over half of the broker-dealers (58 percent) and a smaller number of the advisers (21 percent) maintain insurance that covers losses and expenses attributable to cybersecurity incidents. However, among the firms surveyed, only one broker-dealer and one adviser reported filing claims.

SEC cybersecurity guidance for investment management[12]

Investment companies and registered investment advisers are increasingly reliant on digital information and technology, elevating the importance of protecting sensitive and confidential information about their clients and investors. In April 2015, the SEC's investment management division highlighted a number of measures for funds and advisers to consider when addressing cybersecurity risk. Key focus areas include:

- Assessment: conduct a periodic assessment of cybersecurity risks, impacts, and capabilities.
- Incident management: develop a strategy to prevent, detect, and respond to cybersecurity incidents.
- Implementation: Implement the strategy through written policies and procedures—along with formal training—to guide officers and employees when addressing cybersecurity threats.

Given the constantly evolving nature of cybersecurity risks, this will likely remain a critical issue for the SEC well into the future.

Cybersecurity enforcement[13]

The SEC recently filed its first-ever cybersecurity enforcement action. The commission had been signaling for some time that it would bring an enforcement case against a regulated entity for violation of the specific cybersecurity rules in Regulation S-P, and similar actions are expected to follow shortly. In this particular case, the SEC alleged that the firm in question failed to establish cybersecurity policies and procedures reasonably designed to safeguard customer information, as required by Rule 30(a) of Regulation S-P under the Securities Act of 1933. It was ultimately determined that the firm had failed to conduct a periodic risk assessment, implement a firewall, and encrypt sensitive customer information, all of which helped enable a data breach that compromised the personal information of approximately 100,000 people.

In the wake of the filing, SEC Chair Mary Jo White warned, "it is incumbent upon private fund advisors and other regulated entities to employ robust, state-of-the-art plans to prevent, detect, and respond" to cybersecurity risks. Although public companies are not subject to Regulation S-P or any specific SEC rules about their cybersecurity practices, the SEC has signaled that it is closely examining the accuracy and completeness of public company disclosures about their cyber policies and risks to the business from a cyber incident, as well as disclosures following a cyber breach. Firms should expect additional SEC scrutiny of cyber policies and practices of both regulated entities and of public company issuers.

Contacts

Susan Ameel
Managing Director
Deloitte Advisory
Deloitte & Touche LLP
sameel@deloitte.com

Mike Jamroz
Partner
Deloitte Advisory
Deloitte & Touche LLP
mjamroz@deloitte.com

Endnotes

1. "Forward look: Top regulatory trends for 2016 in securities," Deloitte
2. US Securities and Exchange Commission, 17 CFR Part 275, Release No. IA-4439; File No. S7-13-16, RIN 3235-AL62
3. "Business Continuity Planning for Registered Investment Companies," US Securities and Exchange Commission, IM Guidance Update, June 2016, No. 2016-04
4. "Forward look: Top regulatory trends for 2016 in securities," Deloitte
5. "Report on Digital Investment Advice," FINRA, http://www.finra.org/sites/default/files/digital-investment-advice-report.pdf
6. "Rule 15c3-5 — Risk Management Controls for Brokers or Dealers with Market Access: A Small Entity Compliance Guide," SEC, https://www.sec.gov/rules/final/2010/34-63241-secg.htm
7. "CFTC Unanimously Approves Proposed Rule on Automated Trading", www.cftc.gov, November 24, 2015
8. ibid
9. "FAQs: NFA Cybersecurity Interpretive Notice, National Futures Association, http://www.nfa.futures.org/NFA-compliance/NFA-general-compliance-issues/faqs-cybersecurity-interpretive-notice.pdf
10. National Futures Association (NFA), "9070 - NFA COMPLIANCE RULES 2-9, 2-36 AND 2-49: INFORMATION SYSTEMS SECURITY PROGRAMS," Board of Directors, August 20, 2015, http://www.nfa.futures.org/nfamanual/NFAManual.aspx?RuleID=9070&Section=9
11. Office of Compliance Inspections and Examinations ("OCIE"), National Exam Program Risk Alert, Vol. IV, Issue 4, "Cybersecurity Examination Sweep Summary," February 3, 2015, https://www.sec.gov/about/offices/ocie/cybersecurity-examination-sweep-summary.pdf
12. US Securities and Exchange Commission, IM Guidance Update, "Cybersecurity Guidance," April 2015, 2015-02
13. "Return of the cyborg part II: first-ever SEC cybersecurity enforcement action filed against investment advisory firm," November 19, 2015, http://www.lexology.com/library/detail.aspx?g=4bf3ec32-11bb-40c1-a965-68bf3a26764e23

CENTER *for*
REGULATORY STRATEGY
AMERICAS

The Deloitte Center for Regulatory Strategy provides valuable insight to help organizations in the financial services, health care, life sciences, and energy industries keep abreast of emerging regulatory and compliance requirements, regulatory implementation leading practices, and other regulatory trends.

Home to a team of experienced executives, former regulators, and Deloitte professionals with extensive experience solving complex regulatory issues, the Center exists to bring relevant information and specialized perspectives to our clients through a range of media including thought leadership, research forums, webcasts, and events.

Deloitte.