Optimizing Compliance Risk Management
Risk Assessments, Monitoring and Testing

Monday, March 16, 2020

Moderator:

- Susan M. Boudrot, Managing Director and Global Chief Compliance Officer, TD Ameritrade Holding Corp.

Panelists:

- James Cornwell, Director, Compliance Risk Assessments, Societe Generale
- Lori Ryan-Thurton, Americas Head of AFC and Compliance Testing and QA, Deutsche Bank
- Matt Schurter, Vice President, Global Compliance Testing, the Charles Schwab Corporation
- Josh Stahl, Director, Enterprise Testing, Wells Fargo
- John Walsh, Partner, Eversheds Sutherland LLP

Topics:

- Rules, Regulations and Regulatory Expectations
- The Virtuous Circle of Risk Assessments, Monitoring & Testing
- The Three Lines of Defense
- Technological Developments
- Recent Enforcement Activity

Rules, Regulations and Regulatory Expectations

Generally, the starting point in any discussion of compliance is the regulatory requirement that animates the program. This is true for risk assessments, monitoring and testing. But, we should recognize at the outset, this is an area where specific, bright line standards are rare. Instead, one should approach this area as an example of principles based regulation. The regulators have set out general principles, and expect the regulated community to determine how they should be implemented. A quick survey of regulatory standards illustrates this point.

In 2003, the Securities and Exchange Commission ("SEC") adopted compliance rules for funds[1] and investment advisers.[2] The rules simply state that funds and advisers must adopt policies and procedures reasonably designed to prevent violations. In the SEC release adopting these rules,[3] the Commission added a little more detail, by observing that when funds and advisers prepare these policies and procedures, they should identify conflicts and other compliance factors creating "risk exposure" for the firm and its clients in light of the firm's particular operations.[4] Upon this passing reference to risk exposure has been founded a large and expansive world of fund and adviser risk assessments, monitoring, and testing.

In 2008, the Board of Governors of the Federal Reserve issued a supervisory letter, SR 08-8, entitled ***Compliance Risk Management Programs and Oversight at Large Banking Organizations with Complex Compliance Profiles***.[5] The letter summarized the Federal Reserve's expectations for banks' compliance programs. A section of the letter was entitled "Risk Assessments and Monitoring and Testing Programs." Among other things, the Federal Reserve said, risk assessments are the foundation of an effective compliance monitoring and testing program. Further, the "scope and frequency of compliance monitoring and testing activities should be a function of a comprehensive assessment of the overall compliance risk associated with a particular business activity." Finally, periodic testing of compliance controls by compliance staff was "strongly encouraged." In short, while somewhat more detailed than the SEC's statement about fund and adviser risk exposures, the Federal Reserve's guidance remained at a high level, and contingent on the firm's own assessment.

In 2005 the NASD adopted Rule 3012.[6] Importantly, the NASD said, members should conduct an inventory of all of their businesses, the rules and regulations applicable to those businesses, and identify any gaps or deficiencies in the coverage of the firm's internal control processes. Thus was born the "gap analysis" which ever since has been a key part of every broker-dealer's risk assessment. Then, in 2014, FINRA adopted Rule 3120,[7] which was based upon and updated

---

[1] *See* Rule 38a-1, 17 C.F.R. 270.38a-1.
[2] *See* Rule 206(4)-7, 17 C.F.R. 275.206(4)-7.
[3] Compliance Programs of Investment Companies and Investment Advisers, Release No. IA-2204, IC-26299, (December 2003), https://www.sec.gov/rules/final/ia-2204.htm.
[4] This statement was directed to advisers, and then, in the Commission's discussion of funds it adopted the issues it had discussed for advisers.
[5] *See* https://www.federalreserve.gov/boarddocs/srletters/2008/SR0808.htm.
[6] *See* Notice to Members 05-29, https://www.finra.org/rules-guidance/notices/05-29.
[7] *See* Regulatory Notice 14-10, https://www.finra.org/rules-guidance/notices/14-10.

Rule 3012. Rule 3120 requires member firms to establish "control policies and procedures that test and verify" that the firm's supervisory procedures are reasonably designed. Finally, in 2004 FINRA adopted Rule 3013, which established a procedure for certifying the compliance and supervisory procedures.[8] A few years later, this rule was rolled over into FINRA Rule 3130.[9] These rules rely upon assessments and testing, but they are largely silent about how that should be done, other than through a gap analysis, and testing and verification.

In 2012, the Commodity Futures Trading Commission ("CFTC"), adopted Rule 3.3 which requires entities under its jurisdiction to have a chief compliance officer. At the same time, the CFTC required entities under its jurisdiction to have risk management programs, which must address, among other things, legal risk.[10] While a detailed discussion of the required risk management program is beyond the scope of this outline, when it was adopted, commentators urged the CFTC to adopt a more flexible approach.[11] The CFTC rejected these comments, and indicated that it believed its requirements reflected "prudent risk management practices." In 2018 the CFTC amended Rule 3.3, but in doing so indicated that its changes should not impact entities' risk assessment processes.[12]

In sum, from a passing reference in an SEC release, to a slightly more robust discussion in a Federal Reserve supervisory letter, through the NASD's gap analysis and FINRA's testing and verification, to the CFTC's legal risk assessment, it is clear that the regulators require and expect risk assessments, monitoring and testing. However, it is equally clear that it is up to each firm to determine how this principle should be implemented.

The Virtuous Circle of Risk Assessments, Monitoring & Testing

The virtuous circle of risk assessments, monitoring, and testing, is a rubric that is used to visualize, understand and assess an optimal risk process. It is only a rubric, not a regulatory requirement. Nonetheless, the Three Lines of Defense (discussed below), began as a rubric, morphed into a best practice, and today, particularly for firms subject to the bank regulators, has taken on many of the airs of a mandatory practice. A rubric as simple and powerful as the virtuous circle could well follow the same path.

---

[8] *See* Notice to members 04-79, https://www.finra.org/rules-guidance/notices/04-79.
[9] *See* Regulatory Notice 08-57, https://www.finra.org/rules-guidance/notices/08-57.
[10] *See* Rule 23.600, 17 C.F.R. 23.600.
[11] *See* Swap Dealer and Major Swap Participant Record Keeping, Reporting, and Duties Rules; Futures Commission Merchant and Introducing broker Conflicts of Interest Rules, and Chief Compliance Officer Rules for Swap dealers, major Swap Participants, and Futures Commission Merchants, RIN 3038-AC96, (April 3, 2012), https://www.cftc.gov/sites/default/files/idc/groups/public/@lrfederalregister/documents/file/2012-5317a.pdf.
[12] *See* Chief Compliance Officer Duties and Annual Report Requirements for Futures Commission Merchants, Swap Dealers, and Major Swap Participants, Amendments, RIN 3038-AE56 (August 20, 2018), https://www.cftc.gov/sites/default/files/2018-08/federalregister082118.pdf.

In essence, the virtuous circle means that risk assessments inform the monitoring program, the monitoring program feeds into the testing program, and the testing program is used to correct, enhance, and reconfigure risk assessments. Ideally, each of the three processes should support and enhance the next following step, and ultimately, the entire system. While simple in structure, it can be challenging in implementation.

The panel will present and discuss an example of this rubric.

Three Lines of Defense

The Institute of Internal Auditors ("IIA") is an international professional association for internal auditors. In January 2013 it published a position paper entitled ***The Three Lines of Defense in Effective Risk Management and Control***.[13] In the years since, this position paper has exercised tremendous influence. In shorthand, it has come to be known as "3LOD."

In summary, the IIA's model stated that effective risk management required the interaction of three groups (which translated to the three lines of defense):

1. Functions that own and manage risks;
2. Functions that oversee risks; and
3. Functions that provide independent assurance.

Further, the IIA stated, while not among the three lines, governing bodies and senior management have essential roles. They have responsibility and accountability, the IIA said, for setting the organization's objectives and establishing the means by which it will achieve those objectives. The Three Lines of Defense Model is intended to help them achieve those goals.

The first line (functions that own and manage risks) consists of operational managers. The IIA described this function as a "cascading responsibility structure," in which the upper levels provide guidance and the lower levels draft and execute detailed policies and procedures. The ultimate goal is to provide adequate managerial and supervisory controls.

The second line (functions that oversee risks) consists of managerial activities designed to help and monitor the first line. These activities include compliance, risk management, and controllership. While these specialized functions focus on different subject matters, all work to ensure that the first line is, in the IIA's words, "properly designed, in place, and operating as intended."

The third line (functions that provide independent assurance) consists of internal auditors. This activity is characterized by its high level of independence and objectivity. Further, its work is reported to the highest levels of the organization, including the governing body and senior management. The IIA noted that this level is distinguished from the second, because it is free of

[13] *See* https://global.theiia.org/standards-guidance/Public%20Documents/PP%20The%20Three%20Lines%20of%20Defense%20in%20Effective%20Risk%20Management%20and%20Control.pdf.

the managerial responsibilities that can undermine independence. Importantly, the IIA stated, this third line is important in smaller entities, as well as those which are larger. Smaller entities may face equally complex environments with less formal and robust structures.

The IIA noted in its position paper that every organization is unique, and therefore, there is no one right way to coordinate the three lines. This is familiar to many financial services firms that have allocated specialized third line responsibility to groups other than internal audit. Many broker-dealers, for example, assign third line investigative responsibility to compliance, usually to specialized teams with some level of enhanced autonomy.

In June 2019, the IIA issued an ***Exposure Document***, proposing to update its guidance.[14] This was the first time that the guidance had been revisited since 2013. The Exposure Document highlighted the benefits of the current model. It was, the IIA said, "simple, easy to communicate, and easy to understand." However, it continued, the freedom to assign roles (as noted above for broker-dealers), and collaboration among roles, can lead to a "blurring of the lines." The new document was intended to help address that concern.

One of the most important issues discussed by the Exposure Document, was how to achieve a coordinated approach among the different lines. The governing body, it said, must ensure that "roles and responsibilities are clearly understood by all functions, supported by regular interaction and communication." Further, the IIA identified additional means of assuring effective coordination. The IIA's list can serve as a check list in assessing the effectiveness of coordination within an organization:

- Have you ensured that individual, team, and departmental goals are aligned with the strategic priorities and operational needs of the organization?
- Have you ensured a common understanding of the purpose and roles of each part of the organization?
- Have you established a common vocabulary for describing aspects of governance, risk management, and control?
- Do you use common rating or measurement systems across all functions?
- Do you share resources, including subject matter experts, among functions?

Finally, after releasing the Exposure Document, the IIA conducted a survey, in which it obtained more than 2,000 responses, and in October 2019 it issued a report of its results, entitled, ***Three Lines of Defense: Report on the Public Exposure Findings June-September 2019***.[15] The IIA has indicated that it expects to finalize and release its new position paper during 2020.

The work of the IIA is always of interest, given the leadership role it has played on this topic. However, for certain firms, the Three Lines of Defense are more than a best practice. For example, in 2014, the Office of the Comptroller of the Currency (OCC) published "heightened standards" guidelines on risk governance that directly engaged with the Three Lines of

[14] *See* https://na.theiia.org/about-ia/PublicDocuments/3LOD-IIA-Exposure-Document.pdf.
[15] *See* https://na.theiia.org/about-us/about-ia/Documents/Public-Exposure-Report-General-Release.pdf.

Defense.[16] Also in 2014, the Basel Committee on Banking Supervision (BCBS) urged the banking industry to "strengthen the implementation of the three-lines of defense."[17] Finally, the Bank of International Settlements, Financial Stability Institute, has published a paper which seeks to add a fourth line of defense, involving external auditors and regulators.[18] The IIA's Exposure Document took account of this concept (though it did not add them as a new line).

As a result of this regulatory guidance in the banking space, brokerage firms that are owned by or affiliated with banking entities generally view the Three Lines of Defense as more mandatory than hortatory. This gives them added reason to await the IIA's issuance of its final revised position, which as noted above, is expected in 2020.

Technological Developments

Technology is playing an increasing role in every aspect of the economy, including in risk assessments, monitoring and testing. Many firms have embarked on technology programs in these areas, and multiple vendors have stepped forward to support these efforts. While it is often difficult to look into programs in the private sector, the SEC provides an interesting model, which is at least partially visible to the public.

A few years ago, the SEC made a public commitment to using technology and data to enhance its regulatory programs. Then Chair Mary Jo White described this program in a speech to the SEC Speaks in 2014.[19] She said the agency was "using powerful new data analytics and technology tools in our National Exam Program to conduct more effective and efficient risk-based examinations of our registrants." More specifically, she continued, "OCIE's Office of Risk Assessment and Surveillance aggregates and analyzes a broad band of data to identify potentially problematic behavior. In addition to scouring the data that we collect directly from registrants, we look at data from outside the Commission, including information from public records, data collected by other regulators, SROs and exchanges, and information that our registrants provide to data vendors. This expanded data collection and analysis not only enhances OCIE's ability to identify risks more efficiently, but it also helps our examiners better understand the contours of a firm's business activities prior to conducting an examination."

Chair White continued by asking, "What is next?" She responded by stating, "The Office of Risk Assessment and Surveillance is developing exciting new technologies – text analytics, visualization, search, and predictive analytics – to cull additional red flags from internal and external data and information sources. These tools will help our examiners be even more efficient and effective in analyzing massive amounts of data to more quickly and accurately hone in on areas that pose the greatest risks and warrant further investigation."

The scale of this effort was highlighted in another speech made by then Chair White, in this case to the National Society of Compliance Professionals.[20] She said: "The Risk Analysis

[16] *See* https://www.occ.gov/news-issuances/news-releases/2014/nr-occ-2014-4a.pdf.
[17] *See* https://www.bis.org/publ/bcbs292.pdf.
[18] *See* https://www.bis.org/fsi/fsipapers11.pdf.
[19] *See* https://www.sec.gov/news/speech/2014-spch022114mjw
[20] *See* https://www.sec.gov/news/speech/2013-spch102213mjw

Examination … team uses quantitative analytics to examine clearing firms and large broker dealers by downloading all transactions cleared by the firm over the prior year or two and then subjecting that data to a broad range of queries designed to identify problematic behavior. In one exam that was recently completed, the RAE team collected and analyzed over 400 million transactions. And the next exam is expected to analyze more than twice that many."

In short, the SEC is using "powerful new data analytics and technology tools" to scour sample sizes measured in the hundreds of millions of transactions. This gives them a powerful new way to conduct the agency's risk assessments, monitoring and testing.

We can expect the SEC's capabilities to grow even more powerful once the consolidated audit trail, or CAT, is in place. Chairman Clayton testified to the Senate in December 2019 that the CAT will enhance regulatory oversight of the securities markets.[21] Although, at the same time, he noted that progress on the CAT had been much slower than initially anticipated due to a number of factors.

Many private businesses wish to emulate the SEC, but they face challenges. The most important is cost. While the SEC has been very open about its data and technology program, determining its cost is difficult, at least for those outside of the government. Nonetheless, from time to time information is released which provides some insight to the general public. In 2019, the SEC's Inspector General audited the agency's investments in information technology. The results were published in a public report.[22] While the report was redacted in certain areas, it provides enough information to understand the agency's commitment to information technology.

For example, in 2018, the SEC spent approximately 18% of its budget, or $300 million on technology. Of that, approximately two thirds was spent on the steady state environment, while the remainder was spent on enhancements. More specifically, turning to the programs of most interested to financial service firms, spending on an enhancement contract for the examination program increased from $4.7 million to $5.7 million. Further, the investment for an unidentified office (which was likely enforcement, since the specific recipient was redacted pursuant to the enforcement exemption from the Freedom of Information Act) increased from $1.3 to $6.8 million. Hence, while the details are unclear, and these amounts represent only information technology investments, not the people who use these resources, one can see that the upward trend is measured in millions of dollars.

How can firms keep up? On interesting trend is the institutionalization of the risk assessment, monitoring and testing function within firms. In 2017, a study published in the American Sociological Review reported that in 1994, less than 1% of banks had a Chief Risk Officer.[23] By 2008, the percentage had risen to 35%. Further, most were implementing some form of Enterprise Risk Management ("ERM"). As the risk process is further institutionalized across the

---

[21] *See* https://www.sec.gov/news/testimony/testimony-clayton-2019-12-10

[22] *See* https://www.sec.gov/files/SEC-has-Processes-to-Manage-IT-Investments-but-Improvements-are-needed.pdf

[23] *See* K. Pernall, J Jung, & F Dobbin, The Hazards of Expert Control, American Sociological Review, https://journals.sagepub.com/doi/full/10.1177/0003122417701115.

industry, and risk managers demand a more prominent place in firms' budget processes, perhaps they will acquire more technological capability to keep up with the regulators.

Recent Enforcement Activity

Compliance professionals recognize that risk can emerge from any point within the organization. Nonetheless, it is particularly unsettling when risk emerges from within compliance, and in a manner that threatens the integrity of the firm's risk assessment, monitoring and testing process. Unfortunately, in 2019, a FINRA enforcement case highlighted this issue.[24]

Vincent Joseph Storms was a compliance associate with a broker-dealer. His primary responsibility was to audit branch offices and perform any necessary follow-up work. As a standard audit procedure, branch office registered representatives were asked to complete a questionnaire regarding various compliance issues.

The questionnaires asked about undisclosed outside business activities, undisclosed securities accounts at other broker-dealers, the use of LinkedIn profiles, and whether the branch used third party vendors to store data. The firm used a software program to store the registered representatives' answers. The software also generated a numerical score for each response, ranging from 1 to 3. A score of 1 or 3 required no follow-up. However, a score of 2 required the responsible branch auditor to engage in additional steps before the audit would be considered complete.

While the numeric scores were generated by the firm's software, compliance associates exported the data to a master spreadsheet. They would then use the spreadsheet to process the answers. The data within the software program could not be altered, but it could be changed in the spreadsheet.

Apparently, Storms changed valuations entered on the master spreadsheet. According to the FINRA default decision, over a nine-month period, Storms altered 524 questions from 145 registered representatives, affecting 60 branch audits. When his supervisor confronted him about the alterations, he tried unsuccessfully to correct the data he had altered.

In the Hearing Officer's words, the altered information "was critical to the Firm's operations." The Hearing Officer went on the say, "The Firm relied on Storms to honestly fulfill his function as a compliance associate. Instead, Storm's misconduct created significant risks for the Firm."

The idea that identified risks were not being reviewed, and that tainted information was flowing through the firm's risk assessment and monitoring system, is certainly troubling. Perhaps even more troubling, however, was Storm's motive. The Hearing Officer said, "By doing this, Storms avoided performing required follow-up work."

[24] *See* Department of Enforcement v. Vincent Joseph Storms, Disciplinary Proceeding No. 2017053982801 (July 3, 2019).

In the event, Storms was barred for this conduct. In the interest of fairness, we should note that Storms did not respond to FINRA, so this was a default decision, and we have not heard Storms' side of the story. Nonetheless, this case shows us, yet again, if any reminder were needed, that risk can emerge from any point within an organization, and for any reason, including from within the risk assessment, monitoring and testing process.

Conclusion

Risk assessment, monitoring and testing is in flux, with many new challenges and opportunities. It is an exciting time to be in the field.