NSCP NATIONAL SOCIETY OF COMPLIANCE PROFESSIONALS Currents March 2020

New Year, New Beginnings for Firm Risk Assessment Programs

By Patricia M. Harrison, Ernest E. Badway and Joshua Horn

With the start of a new year and decade, firms need to redouble their efforts in evaluating and upgrading their risk assessment programs. Over the past year, the SEC and FINRA have made their intentions known, and it does not appear any quarter will be provided to firms in the upcoming year.[1]

We attempt with this article to assist firms in further developing and improving their risk assessment programs. Firms should, initially, determine the methods to be used to develop risk-based testing programs; understand how to execute compliance testing programs; and gather techniques for raising, remediating, tracking and closing issues. Further as part of this process, firms must have the ability to write effective WSPs, conduct risk assessments, execute the testing program, report writing, and, finally, remediating and closing issues.

There are 6 "W's" for effective WSPs: (1) **W**ho is the owner and/or accountable person or group? (2) **W**hat is the applicable rule, principal or standard; supervisory reviews must be performed, and internal controls are needed (preventative, detective, corrective)? What happens if these controls fail (escalation, reporting)? Are exceptions allowed? (3) **W**hen do supervisory reviews need to be performed? (4) **W**here is the supervision being conducted (main office v. branch)? (5) **W**hy is this applicable to our firm? (6) **W**hen and how does our firm ensure actions are being performed and documented? WSPs must be user-friendly in plain language, and updated regularly. In short, these questions must be answered to ensure effective WSPs. In particular, firms must be certain as to defined responsibilities for supervision and oversight as well the types of reviews to be performed and the documentation necessary to demonstrate said reviews.

We next lay out the appropriate steps that a firm should consider in reviewing its risk assessment program.

Risk Assessment

Late in December 2019, FINRA announced a new structure for its risk monitoring program.[2] Nonetheless, FINRA reiterated its commitment to analyzing firm's risk assessment programs, and that its examinations will continue in 2020 with a concerted effort to be more efficient and tailored to a firm's specific risk parameters.

Broadly speaking, a risk assessment program is a systematic process of identifying and analyzing potential (negative) events that may be involved in a projected activity or undertaking. To accomplish this one should create a risk matrix that is used during the risk assessment to define the level of risk by considering the category of probability or likelihood against the severity of the risk. A risk matrix is a simple mechanism to increase visibility of risks, and assist in focusing the firms attention on the areas of greatest risk to the firm.

The first step in the process is to conduct a risk inventory. It is primarily based on rules and regulations applicable to the firm, considers the firm's business model, and should be broad and comprehensive. One particular starting point for any such inventory is FINRA's WSP checklist.[3] FINRA has created this exhaustive checklist, but assumes a much broader inquiry and pre-supposes that the firm is engaging in re-working of its WSPs.

We suggest that the firm consider several areas for testing purposes. In particular, testing should be inclusive of: advertising; advisory agreements; allocations; anti-money laundering; best execution; breakpoints; books and records; code of ethics/personal trading; communication; custody; and cybersecurity. We have included the chart below as a guide to the firm so that it may review the appropriate procedure and test it to determine if it is adequate for detecting conduct the firm is attempting to deter.

About the Authors

Patricia M. Harrison is the Managing Member of PMH Compliance Solutions, LLC. She can be reached at patriciamharrison77@gmail.com.
Ernest E. Badway is a Partner in Fox Rothschild LLP's Securities Industry Group. He can be reached at ebadway@foxrothschild.com.
Joshua Horn is a Partner in Fox Rothschild LLP's Securities Industry Group. He can be reached at jhorn@foxrothschild.com.

1. Tom Zanki, "SEC And CFTC Regulatory Priorities To Watch In 2020," https://www.law360.com/articles/1228214/sec-and-cftc-regulatory-priorities-to-watch-in-2020; https://www.sec.gov/about/offices/ocie/national-examination-program-priorities-2020.pdf; and https://www.finra.org/sites/default/files/2020-01/2020-risk-monitoring-and-examination-priorities-letter.pdf.
2. *See* https://www.finra.org/media-center/newsreleases/2019/finra-announces-senior-leadership-team-under-new-examination-and.
3. *See* https://www.finra.org/sites/default/files/WSP-Checklist.pdf

Risk Assessment

The chart is meant to illustrate for a firm a possible review template. It is by no means a complete and comprehensive policy review. However, we suggest that the example below may be adapted to the particular risks associated with the firm's business operations. We hope that, at the very least, it provides appropriate guidance to begin the firm's risk assessment.

Question	Comment	Conclusion This is intentionally blank as a place for you to fill in for your firm.
WHY do we need this policy?	*Insert reference for source of policy e.g. regulatory, internal, client requirement, best practice, etc.*	
WHY is it applicable to our firm?	*Consider what activities are undertaken that make this requirement relevant to our firm*	
WHAT is the rule, principal or standard that the firm has or will adopt in relation to the need for this P&P?	*This can be quoted from legal/ regulatory source(s), internal mandate as approved by the Board or a committee, quote from a client investment management agreement, etc.*	
WHAT definitions are relevant to this policy?	*Provide clarity as to terms that may be subject to confusion*	
WHAT activities does the policy cover? AND/OR to WHOM does the policy apply?	*Consider the functions that are relevant to the policy and/or identify the individual groups, functions that are covered by the policy, e.g. all staff, all trading staff, etc.*	
WHO are the stakeholders	*That is who needs to be involved with policy drafting and procedure development?*	
WHO owns and approves the policy?	*This can be a department/function, committee or individual*	
WHO has accountabilities under this policy?	*Specify which people/groups have to undertake actions to effect the procedures to implement the policy, e.g., who reports, who reconciles, who supervise, who oversees, who escalates, who approves, who authorizes, etc.*	
Are exceptions permitted?	*If so, specify what activities or circumstances may result in an exception, who has the authority to approve them, and what particular reporting or documentation is required*	
WHAT are the consequences of breaches?	*Consider relevant internal and external consequences. Internal consequences could be censure, termination, suspension of privileges, demotion, etc. External consequences could be reporting to legal/regulatory authorities, etc.*	

Question	Comment	Conclusion
WHAT reporting is required?	*That is, who does the reporting, what is reported, how frequently is it reported?*	
WHAT documentation is required?	*That is, what needs to be retained either in soft or hard copy form, to evidence that the policy is operating, e.g. a report, a reconciliation, a sign off, etc.*	

Procedures

Similarly, we provide a template for firms to consider changes and/or relevant revisions to their WSPs. This is a critical step for any firm to ensure that its revised WSPs will comply with the type of business it is engaged in and the associated risks it encounters. These procedures, however, must be practical and, specifically, should be tailored to fit the firm's risk profile.

Question	Comment	Conclusion This is intentionally blank as a place for you to fill in for your firm.
WHAT internal controls would be effective in implementing the policy?	*For example, consider which of the following apply (non-exhaustive list):* • *Segregation of duties* • *Approval* • *Authority* • *Limits* • *Security* • *Reconciliations* • *Review Supervision* • *Oversight*	
WHAT are the action steps required to engage the internal controls?	*Consider the correct order of steps, ensure clarity but avoid "too much" detail*	
WHEN do the activities take place?	*Consider the trigger for activity, e.g. when trading, when initiating cash movement. Consider the frequency for activities daily, week, monthly, quarterly, etc.*	
WHAT resources are necessary to perform the action steps?	*This could be receipt of information, a request, disclosure, form or system access, etc.*	
WHO is going to perform the action steps?	*Also consider who the back-up will be in case of absence, as well as business continuity issues*	
WHO is going to review/approve/ supervise/oversee the actions? HOW are they going to do this?	*Also consider who the back-up will be in case of absence, as well as business continuity issues*	
WHAT are the outputs of the actions? HOW are the outputs to be recorded, retained, reviewed, approved, etc.?	*Consider the results from these changes and how it is reported*	
WHAT regulatory filings or client disclosures result from the activities?	*Consider how filing or disclosure is achieved and recorded, who is responsible, penalties for missed filings, etc.*	
HOW are you going to ensure that the actions are done?	*Consider system alerts, certifications, exception reports, testing procedures, etc.*	

Test Processing Components:

Initially, the best test processing begins by identifying a rule and/or WSP testing item. Firms should select and notify interviewees for this project while establishing a review timeframe. As part of any test processing, the firm must determine an appropriate sample size so as to collect relevant data and documentation.

As discussed below, once this is accomplished, the firm must assess and/or analyze the data and documentation. It is critical that the firm document its findings as well as distribute a suitable report to the required executives at the firm for approval and implementation. However, the drafting of said report does not end the processes, remediating/training and maintaining work papers are also required.

As we discuss above, firms should consider testing on areas that include: SEC and FINRA Annual Exam Priorities Letters; new business lines, products or activities; area(s) tested last year that had significant findings; prior regulatory exam findings; client complaints; regulatory notices and alerts; new/amended rules and regulations; and notable disciplinary/enforcement actions. The firm must also consider including low or lower risk items, but testing these items with less rigor and frequency.

Categories of Sampling Methods

When considering sample methods, a firm should consider two types of sampling. The first sampling type is probability sampling, a type of sampling where a subset selection—called a statistical sample-- of individuals from within a statistical population to estimate characteristics of the whole population. Probability sampling must contain a sample with a known probability of being selected, and may consider certain types of sampling methods such as:

- simple random sampling (SRS), a subset of individuals (a sample) chosen from a larger set (a population), chosen randomly and entirely by chance;
- stratified sampling, a sampling from a population partitioned into subpopulations;
- cluster sampling, a mutually homogeneous but internally heterogeneous grouping from a statistical population;
- systematic sampling, statistical method involving the selection of elements from an ordered sampling frame; and
- multistage sampling, taking in stages using smaller and smaller sampling units at each stage.

Further, some of these methods above may be combined in stages where the firm would choose several methods to arrive at a conclusion based upon objective criteria.

The second type of sampling is non-probability sampling, a technique where the firm would select a sample based upon its own subjective judgment and not some random selection. Such sampling does not have a known probability of being selected as inconvenience or voluntary response surveys. Moreover, the probability samples are selected in such a way so that they are population representative. Essentially, the firm would direct the type of testing based upon subjective criteria.

Regardless of choice, these sample forms provide the most valid or credible results for a firm since they reflect the characterizations of the selected population. The representative sample group or set chosen from a larger statistical population or group of factors or instances would adequately replicate the larger group according to chosen characteristic or quality the firm is studying. Thus, determining the sample size may be difficult, so a firm may wish to consider the use of on line sample size calculators; margin of error; and confidence levels. Nonetheless, firms should look at the whole picture, and not one component, or one piece. In fact, the old adage is true "follow the money," therefore, focusing on the following: investment banking project; IB project team communications (clients, research); pitch books, research reports; restricted lists/watch lists/wall crossings; personal trading/client trading; project file (books and records, due diligence); and other client projects.

When completed, assess the results of your sampling.

Writing the Report

There are different forms the report may take depending on the regulations that apply. However, all have certain characteristics to include that are: positive and negative occurrences, conclusions based on facts, recommendations and summary of remediation efforts, and pending matters to be addressed. Further, the reports should not include: opinions not supported by facts; subjective comments and unproductive criticism.

The types of reports include the FINRA Rule 3120 Report that should have as a best practice, all sampling rationales, testing processes, and findings, as well as corrective actions taken for findings quickly remedied.[4] The FINRA 3130 Certification summarizes testing processes; notes significant exceptions and material violations; and details remediation plan(s).[5] Another type of report is the Investment Advisers Act of 1940 Rule 206(4)-7 report that describes each review conducted; a summary of material changes since the last report and a summary of review findings; as well as a description of remediation made to policies and or procedures, training/education plans. [6]

Remediation Considerations

Remediation is often a critically overlooked aspect of this testing process. Firms have to correct problems. It is simply not enough to identify the problem and create new procedures.

Nonetheless, when providing guidance to a business unit for remediating an issue, compliance must consider the nature of the findings in deciding the appropriate remediation steps. For example, firms should consider the magnitude, time sensitivity, and/or client harm, among other things, when working out these remediation issues. Similarly, firms should consider certain aspects of the conduct before engaging remediation, on such things, including, but not limited to, recidivist/repeat findings, pervasiveness of the issue, and relevant regulatory requirements or rules.

Similarly, when remediating deficiencies, firms have to specifically say what it will do, and do what the firm says it will do. Firms should not limit themselves in this process, and may consider a change to one or more of the 6 W's discussed above, a change to the WSP, initiate personnel training and/or education. Training as a remediation step may be essential, but you first must ask if training is applicable to deal with issues noted in testing. Training may not always be appropriate given any past trainings and the results or lack thereof. When something has not worked, firms may have to do something different if certain prior acts of remediation have not worked. Essentially, firms have to demonstrate they are taking reasonable steps to correct the issue to protect themselves from potential regulatory action.

Conclusion

In short, developing an effective risk assessment program that is multi-layered and faceted requires many different skills and patience. The good news is it can and should be employed regularly.

4. *See* https://www.finra.org/rules-guidance/rulebooks/finra-rules/3120?element_id=11346&rbid=2403.
5. *See* https://www.finra.org/rules-guidance/rulebooks/finra-rules/3130.
6. *See* https://www.law.cornell.edu/cfr/text/17/275.206(4)-7.