

Broker-Dealer  
Investment Adviser  
Insurance  
Research

300 Day Hill Road • Windsor, CT 06095 • [www.limra.com/compliance](http://www.limra.com/compliance) • Issue 2009-2 • Bimonthly

May 2009

## Leveraging Online Technology for Supervisory Requirements

By Greg Clukey, Pinpoint Global VP Business Development and Larry Niland, LIMRA Senior Regulatory Advisor

FINRA and SEC rules regarding supervision, supervisory controls, testing and certification (such as FINRA Rule 3012 and SEC Rule 38a-1) provide an opportunity for Chief Compliance Officers and their broker-dealers to leverage the use of online, Web-based technology to help deliver, test, control, and document their firm's supervisory control processes.

The use of an online, integrated solution not only simplifies the work effort, it can greatly increase a firm's operational efficiency in three areas:

1. Communicating the processes and procedures that define the supervisory controls;
2. Delivering the tools to help supervisors implement them; and
3. Ongoing testing and verification of the supervisory procedures by providing instant, *real-time* access to the testing data, thereby enabling a more robust risk-based review of critical procedures.

In addition, integrating all the components into a single delivery and monitoring "system" provides a powerful environment for proactively managing supervisory controls. The following are some examples of how companies can leverage online technology to achieve these goals:

### Written Supervisory Procedures (WSPs)

WSPs — as defined in FINRA Rule 3010 — must be communicated and made readily available to all who supervise personnel in the conduct of a firm's securities and/or investment banking business. When WSPs are delivered in paper form it creates challenges and costs in both distribution and updating, as well as risks in not being able to ensure the latest procedures are read, understood, or followed. By leveraging online technology, WSPs become available to all locations from a single source, and companies can add new procedures or make changes to existing procedures easily, making them instantly available to all. Online WSPs also enable searching and indexing to simplify finding specific procedures, as well as the targeting of specific WSPs based on the role and responsibilities of a specific user. Full tracking of a WSP access log can also measure how actively the organization is focusing on the supervisory process.

### Outside Business Activities (OBAs) Reporting

As defined by FINRA Rule 3030, representatives engaged in OBAs must provide notification to the firm whenever any changes occur. Submitting

## NOTABLE

- ▶ LIMRA's annual [Compliance and Market Conduct Exchange](#) June 24–26, Las Vegas, NV
- ▶ LIMRA's [2009 AML Ongoing Training Course](#) is available now
- ▶ Free LIMRA Podcast: [Think Like a Criminal to Enhance Your Company's AML Compliance](#)
- ▶ *Supervisory Controls System*: online preview available by request

## COMING SOON

- ▶ Webinar: *New Reality of Product Review*, June 15, 2009

## SERVICES AND PRODUCTS

- ▶ 3012/3130 consulting
- ▶ AML education
- ▶ AML auditing and consulting
- ▶ BD branch auditing
- ▶ Expert witness testimony
- ▶ *Supervisory Controls System (SCS)*
- ▶ Post-purchase surveys to monitor compliance and suitability issues
- ▶ RIA auditing and consulting
- ▶ Seminar auditing
- ▶ WSP and compliance manuals

## CONTACT US

For information, assistance, or proposals:

LIMRA Compliance and Regulatory Services  
300 Day Hill Road, Windsor, CT 06095  
Phone: 877-843-2641  
Email: [Compliance-RegSvs@limra.com](mailto:Compliance-RegSvs@limra.com)

[www.limra.com/compliance](http://www.limra.com/compliance)

© 2009, LIMRA®



this data online provides the ability to tailor the questions on the form to reflect the nature of the activity. This not only streamlines the forms, it simplifies the process for the registered representatives and registered principals. It also enables the OBA form to be instantly available and automatically routed and reviewed by all entitled personnel both at the local and home office levels. This includes a real-time view of all OBA forms that have been submitted, where they are in the process, what types of activities have been reported, and who has not submitted as required. OBAs allow assessment of specific risks that might be associated with certain activities and permit automated testing of the associated procedures.

### **Annual Compliance Meeting (ACM) Requirement**

The ability to satisfy the ACM requirements using online technology is defined in FINRA Rule 3010(a)(7). Delivering the ACM online not only eliminates the travel costs associated with face-to-face meetings, but also allows the registered representatives and registered principals to complete those requirements unique to their roles, at their convenience, to ask clarifying questions, and to do so without taking too much time away from their selling

activities. Real-time tracking of those individuals that complete the ACM, and more importantly those who have not, provides a critical measurement point and opportunity for corrective action.

### **Summary**

Leveraging online technologies, including real-time data collection and reporting, enables firms to gain operational efficiencies and address key compliance requirements, including:

1. Collecting audit information and other supervisory requirements;
2. Reporting findings;
3. Assigning remediation tasks and responsibilities; and
4. Tracking and documenting compliance.

*The technology exists today for implementing an integrated online solution, and its benefits should make this a top priority for any broker-dealer's supervisory management. "Supervisory Controls System" (SCS) — an integrated online solution by LIMRA which is powered by Pinpoint Global technology — automates all of the above and more. For more information please email Larry Niland at: [lniland@limra.com](mailto:lniland@limra.com).*

## **Chief Privacy Officers' Perspective on Data Privacy and Security**

*By Larry Niland, LIMRA Senior Regulatory Advisor and David Somers II, Esq., LIMRA Regulatory Consulting Director*

### **Best Practices and Regulation Roundtable Meeting**

Over 261 million data records of U.S. residents have been exposed due to security breaches since January 2005, according to the [Privacy Rights Clearinghouse](#). If you've talked to your firm's Chief Privacy Officer (CPO) lately chances are he or she was not in a good mood. States are passing new regulations at a record pace on how client personal information and other critical data must be protected, controlled, transmitted, encrypted, transported, shredded; and when it is not, how to report the breach to everyone affected, including the regulators.

At a recent LIMRA roundtable meeting in Connecticut of broker-dealer and insurance company CPOs, participants discussed data privacy and security best practices and regulation. The following issues and topics are highlights from the meeting:

#### **1. New State Regulations**

The CPOs focused on new state regulations and the specific challenges related to meeting those new requirements. As of January 1, 2009, forty-four states have enacted legislation requiring notification of securities breaches involving personal information. Most notably, Massachusetts' new regulation ([201 CMR 17.00](#)) requires companies to implement a comprehensive data security plan, including encryption.

#### **2. Identity Theft "Red Flags" Rule Implications**

CPOs from firms that are involved in credit extension or hold creditor check writing accounts discussed the impact of the Identity Theft "Red Flags Rule" (16 CFR 681.11) promulgated under the FACT Act, and the implications for broker-dealers pursuant to FINRA Regulatory Notice 08-69. The primary goal of the Identity Theft "Red Flags Rule" is to help identify, detect, and respond to specific activities, patterns, or practices that could be the result of identity theft. Some CPOs expressed confusion and uncertainty concerning their obligations under the rule, with much of the discussion focusing on reporting obligations when possible discrepancies are found.

A few weeks after the roundtable meeting, the Federal Trade Commission (FTC) delayed the compliance and enforcement deadline of the "Red Flags Rule" from May 1, 2009 to August 1, 2009 in order to give creditors and financial institutions with "covered accounts" more time to develop and implement written identity theft prevention programs. In addition, the FTC has released a ["Red Flags Rule" compliance guide for businesses](#).

### 3. Defining and Remediating a “Breach”

Each CPO’s firm has a plan to respond to and report data breaches, but the CPOs differed on how firms should decide what qualifies as a breach, and how to remedy the breach. Breach costs can vary widely depending on the extent and nature of the data breached as well as the appropriate remedy. In assessing risk, most CPOs try to balance the risk of identity theft and the potential for misuse when deciding how to reassure clients and what remedies to offer clients (e.g., credit monitoring services). All the CPOs agree that once a breach occurs it is critical to respond quickly, use a predetermined team to assess the breach from the top down, and promptly report the breach to the required regulators.

### 4. Data Encryption

CPOs also discussed data encryption and standards, when encryption must be used, and what steps firms are taking to minimize or eliminate the use of certain customer data like social security numbers. Some CPOs use techniques for data masking, namely making personal client data work for the firm but rendering it useless to persons who come to possess it by breach or accident. All the CPOs’ firms are in the process of or have already completed encrypting all company mobile devices, including employee laptop computers and Blackberry devices. In addition, some CPOs also require hard-drive encryption on all employee desktop computers.

### 5. Vendor and Contract Management

The CPOs perform varying degrees of data inventories since the requirement to do so varies by regulator. All the CPOs’ firms have privacy policies and train employees across the enterprise. However, many CPOs are still debating how to deal with vendors in possession of private information; this includes affiliates and third-party vendors servicing clients (e.g., IT vendors managing databases). Many express concerns that the regulators setting policy on certification of vendors possessing such data may not understand how varied and complex those relationships really are. The CPOs have all met with their legal or contract procurement department to ensure that new legal agreements contain the appropriate language to meet all the emerging requirements and to assure that affiliated and third-party vendors are obligated to take the required steps to protect client information, including controls and testing. A few CPOs whose firms have overseas operations that access U.S. client data indicate that they have extremely robust controls on the data accessed at those facilities.

### 6. Virtual Employees and Independent Contractors

The emerging employment trend of remote employees or “virtual employees” is causing some privacy concerns for CPOs. Although these employees may have access to client data to do their work, the equipment they use can vary at some firms. A few firms maintain strict

requirements that only company-provided hardware with encryption technology can be used for such activities. CPOs with independent producers or registered representatives talked about checking their firms’ data systems, including encryption compliance and breach reporting at branch offices. Other CPOs noted how data used to comply with their firms’ Business Continuity Plans (BCPs) was protected. Such BCP data can also be helpful in identifying the scope of breaches when data equipment is stolen.

### 7. Email Policies and Practices

The email policies and practices at the CPOs’ firms led to a discussion that included how to roll out encryption, different approaches to secure/encrypted email, and the use of email review technology to either quarantine or block emails containing private information (e.g., social security numbers and credit card numbers). All the CPOs agree that such policies and practices are beneficial, but none say that their current system works perfectly.

*If you would like to learn how **LIMRA’s Virtual Worker** assessment test can help your company identify, train, and manage virtual employees, please contact Wendy Weston at: [wweston@limra.com](mailto:wweston@limra.com).*

*To learn more about how to improve you firm’s privacy controls or how to join **LIMRA’s Privacy Officer Roundtable**, please contact Larry Niland at: [lniland@limra.com](mailto:lniland@limra.com).*

## Risk-Based Reviews of Branch Offices

*By Larry Niland, LIMRA Senior Regulatory Advisor and Fred McDonald, LIMRA Senior Regulatory Advisor (former FINRA District Director, District 11)*

### **Suggestions for Assessing Branch Office Risks and FINRA’s BORAM**

As we enter the fourth year of the new definitions for branch offices (as defined in NASD NTM 05-67) many broker-dealers still struggle with how often to visit branch office locations. More firms are transitioning to a risk-based review of their branch operations. The purpose of this article is to help broker-dealers identify those factors and collect those data points in order to assess risk and improve supervisory controls.

The basic factors to be considered are similar to those in FINRA’s Branch Office Risk Assessment Matrix (BORAM) in the Web IR questionnaire. Many broker-dealers have limited resources, making it impossible for all but the smallest firms to visit every branch every year. FINRA has limited resources as well, but branch office visits are part of every routine exam. FINRA will inevitably visit some of your branch offices; and, although your registered representatives may be independent contractors for employment purposes, as your representative all their activities in the securities business are your broker-dealer’s responsibility.

Listed below are seven proactive steps that your broker-dealer firm should take to conduct its own risk-based review and be better prepared:

### 1. Search for Problematic Branch Offices and Representatives

Research your representatives by using firm-wide results for the most recent period. Identify those branches with the highest income and highest revenue. Search for the smaller branches with highest per representative income; this might yield a branch with either a large number of representatives, or a branch with one or two representatives with very high per representative income. The next step is to search for branches with the most complaints or frequent or large arbitrations.

Identify any problem representatives by using the [Web CRD Report Center](#) or firm records. These representatives may be on heightened supervision or have Form U4 disclosures involving prior complaints or regulatory actions. Add to this list any representative or branch identifiable from the firm's exception reports. These might be internal reports on transactions such as variable annuity replacements or exception reports from your clearing firm.

### 2. Assess Local Supervision

Using the information from step one, assess the current state of local or OSJ supervision. Examine the geographic dispersion, the number of supervisors, and the number of representatives at the branch. Is the branch office or OSJ well supervised given the supervisor's span of control? How far is the branch office from the OSJ? How often does that supervisor go there? What are the registration categories of the representatives? Are there dedicated supervisors at the branch offices with necessary registrations and experience in those activities carried out at the branch? Have they been clearly delegated to carry out specific supervisory tasks?

### 3. Evaluate Business Activities at the Branch Office

Evaluate the range and complexity of business activities. Consider the activities of the branch by revenue and market, asset management with discretion inside an investment adviser firm, market making activities, website activity, and outside business activities. All of this information is available to firms and regulators from [Web CRD](#) and Form BR. Identify those branches with disclosed OBAs that may be conducted in connection with, or as an accommodation to, the solicitation of the firm's clients. This should include financial planning and investment advice, mortgage origination, and fixed product sales including EIAs, TPA services, and pension consulting services.

### 4. Review Sales Material Review Records

Sales material review records can reveal those branch offices holding free lunch/dinner seminars. These may need added oversight in the form of "mystery shoppers" attending those seminars to assure approved materials are delivered properly. Generally, any sales to seniors will draw additional scrutiny from FINRA and state regulators.

### 5. Examine Complaint Reports and CRD Disclosures

Examine the number of complaints reported, the nature of the complaints, and the amount or number of settled complaints. Also, search for any representatives at or near the threshold for heightened supervision under FINRA Rule 3010. Consider what may be appropriate for representatives who either made disclosures on Form U4 or who joined their current broker-dealer with a history of prior disclosures at a previous firm.

### 6. Review Branch Office Deficiencies

Most firms have a process for logging and following up on any deficiencies or exceptions noted during their branch office inspection program. Use these reports to identify any branches with above-average deficiencies or exceptions, or repeat findings in certain areas.

### 7. Review Internal Exception Reports

Review exception reports from various areas of the broker-dealer, clearing firm, trade desk, suitability review units, variable annuity replacement review units (e.g., any reports showing "above expected" replacements of annuity products under FINRA Rule 2821), customer service, and new account unit not in good order (NIGO) reports.

### Summary

By performing the seven steps above, it is possible for broker-dealers to develop a risk-based branch office review program. Such a program would mitigate increased risk to the firm by conducting either more frequent or targeted reviews of those branch offices or non-branch locations deemed to have higher risks, thus making more effective use of the firm's compliance resources.

Firms can also automate the collection and aggregation of the above data points to assist them in conducting more targeted reviews as part of their normal exam cycle, or to distribute self-assessment tools or questionnaires to branch office supervisory staff to identify the current status of any specific risk or activity. Branch offices deemed low risk might only receive the minimum required visits or be asked to complete self-assessment reviews periodically between audits or inspections. If trends or increased concerns are detected, unannounced visits can also be scheduled. It is difficult to replicate the value of an unannounced, on-site inspection by an experienced and trained examiner with true independence from the branch being reviewed.