Post-Trade Compliance and Surveillance Systems for Buy-Side Firms

By Brian DeDonato, CAIA

When it comes to ensuring the integrity of capital markets, a new trend is emerging among global regulators: focus on buy-side market participants with an intensity that was once reserved only for our sell-side counterparts. This movement has several implications, but as it pertains to monitoring the trading desk, regulators now expect that buy-side firms adopt and implement a consistent, holistic approach to post-trade compliance and surveillance.

The term "post-trade compliance and surveillance" is broad, but it generally refers to a set of operational procedures designed to identify non-compliant trading and investment activity. If the buy-side is expected to emulate the sell-side's approach, technology must play a critical role. This article will break down the beginning stages of surveillance-system design into four simple steps. This is not intended as a framework for the development of proprietary systems (although it may serve as a starting point), but rather an opportunity for compliance to gather the necessary information prior to making a buy or build decision.

Step 1: Define the Trading Activities and How to Detect Them

First, make a list of compliance risks derived from investment activities, and document how to detect them in plain English. Examples of risk factors to consider include failures to obtain the best available price; side-by-side management conflicts such as front-running, account favoritism or unfair allocation methodologies; market abuse and insider trading; and prohibited transactions. For simplicity, let's use insider trading detection as an example. A query designed to detect suspicious outperformance of a trade might be expressed in the following manner:

> *Identify all trades where the security type is an equity instrument, the total traded value exceeds $3M OR more than 10,000 shares were traded, the transaction type is buy-to-open, and the unrealized return over T+2 is greater than 5%.*

Note that insider trading tests should screen for three different scenarios: realized gains, unrealized gains, and loss aversion. To identify instances where a position may have been reduced or liquidated ahead of an adverse material news event, we would alter the query as such:

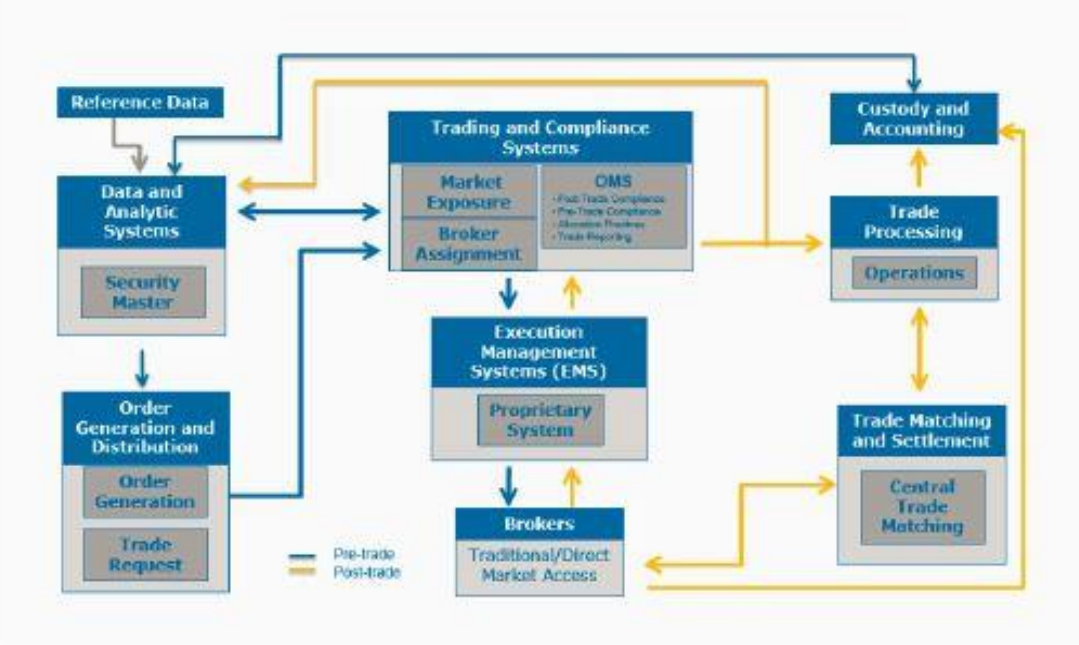
> *Identify all trades where the security type is an equity instrument, the total traded value exceeds $3M OR more than 10,000 shares were traded, the transaction type is sell-to-close, and the unrealized return over T+2 is less than negative 5%.*

As you can see, simple conditional statements can adequately describe the types of trades we are seeking to identify. It is critical in the beginning stages of system design to avoid over-complicating the problem, which tends to result in over-engineering the solution.

Step 2: Define the Data Requirements and the Source Systems

Next, we must document the data requirements and map each data set to the source system. The primary data sets include trades and portfolio positions, while the secondary or reference data sets include benchmark and individual security historical price and volume information. Primary data sets will reside either at the custodian, prime broker, order management system or accounting system, while reference data sets are generally stored in the security master or data warehouse(s).

About the Author
Brian DeDonato, CAIA is Product Manager with Ascendant Compliance Management. He can be reached at bdedonato@ascendantcompliance.com.



Step 3: Identify the Proper Benchmarks and Thresholds

A benchmark might exist in the form of a return profile (as in the case of the insider trading example), but there are numerous other benchmarks we can leverage to identify trade exceptions for other risk factors. For example, to design a test for best execution, we want to reference a volume weighted average price (VWAP) or an arrival price to assess the quality of execution. For side-by-side management conflicts, we compare execution prices and allocations between client accounts when trading in the same securities over a given interval of time. Each test requires careful consideration of what benchmark is best suited to identify the potential misconduct.

Thresholds, on the other hand, allow us to differentiate between a result that is expected (e.g., a return that is in line with a broad market index) versus a result that is aberrational (e.g., a return that vastly exceeds the broad market return over the same interval of time).

Step 4: Test and Adjust Thresholds to Minimize False Positives

In the example for insider trading detection, we are screening transactions for those that generate performance above an arbitrary benchmark that is fixed at 5%. This tends to generate a significant number of false positives when the general market or market sector is rising (or declining in the event of loss aversion screens). For these reasons, we might incorporate the concept of incremental returns above an index such as the S&P 500. Our new trade query now looks something like this:

> *Identify all trades where the security type is an equity instrument, the total traded value exceeds $3M OR more than 10,000 shares were traded, the transaction type is buy-to-open, and the unrealized return over T+2 is greater than 5% above the return for the S&P 500 Index.*

In Conclusion

The process of reducing false positives is iterative. You will often find that adding new data fields to a primary data set or adding an additional reference data set can dramatically improve the output from a surveillance system. There is no one-size-fits-all solution, but in order to find the solution that adequately addresses the compliance risks at your firm, you must start somewhere. These four steps are a great place to begin.