

Energy trade surveillance roadmap

Maximizing compliance investments
through optimization

January 2016



pwc

A head start for energy regulators

Government regulators have stepped up enforcement of energy-trading regulations in the past few years, with the trend set to continue—if not intensify. Since 2010, the US Commodity Futures Trading Commission (CFTC) and the Federal Energy Regulatory Commission (FERC) have issued more than \$1.3 billion in penalties to energy-trading organizations.¹ From fiscal year (FY) 2013 to FY2014, the FERC opened 41 new investigations compared with 27 in the two years prior.²

Such heightened scrutiny has been fueled by increasingly varied types of illegal market manipulation, such as spoofing, which involves placing large trade orders with the intention of subsequently canceling them in order to drive prices up or down³. Although the concept of spoofing and certain other kinds of illicit activities are well known, the speed at which a guilty verdict can be reached and the now real threat of prison for wrongdoers represent new developments.⁴ In the face of such

changes, many energy-trading organizations are being forced to play catch-up in improving the quality and responsiveness of their own trade surveillance programs.

That pressure is not likely to abate soon, especially when both agencies have gained broad new powers that strengthen their ability to detect and penalize infractions. The CFTC has seen its authority grow with the passage of the 2010 Dodd-Frank Act, which substantially expanded the agency's oversight. The CFTC has wasted little time marshaling resources in response, spending tens of millions of dollars to bolster its technological and analytic resources, its data gathering capabilities, and its staffing.⁵ The CFTC's 2014 annual enforcement report made it clear that the organization intends to remain committed to "aggressive enforcement and policing."⁶

The Energy Policy Act of 2005 similarly gave the FERC greater latitude in pursuing suspect

market positions and questionable trading behaviors. To give enforcement some sting, penalty limits were also raised, from \$10,000 per violation per day to \$1 million—a hundredfold increase.⁷

Energy-trading organizations need the ability to identify possible noncompliance before regulators do—not just for effective compliance purposes but also because regulators have explicitly commented that when it comes to fines and penalties, they will look more favorably on entities that come forward with compliance issues proactively rather than waiting for regulators to discover them.⁸

The challenge is that many energy-trading organizations do not yet have sufficiently integrated compliance risk management functions to detect issues promptly. Without leadership commitment or resources to provide necessary top-level, business-wide attention, internal

¹<http://www.cftc.gov/LawRegulation/Enforcement/EnforcementActions/index.htm>, <http://www.ferc.gov/enforcement/civil-penalties/civil-penalty-action.asp>.

² FERC Annual Reports on Enforcement, FY2011–FY2014.

³ http://dealbook.nytimes.com/2014/10/06/a-new-crime-with-a-catchy-name-spoofing/?_r=0

⁴ <https://www.fbi.gov/chicago/press-releases/2015/high-frequency-trader-convicted-of-disrupting-commodity-futures-market-in-first-federal-prosecution-of-spoofing>.

⁵ <http://www.cftc.gov/PressRoom/SpeechesTestimony/opamassad-19>.

⁶ <http://www.cftc.gov/PressRoom/SpeechesTestimony/opamassad-6>.

⁷ <https://www.ferc.gov/EventCalendar/Files/20071114084824-Staff-report-11-14-07%20.pdf>.

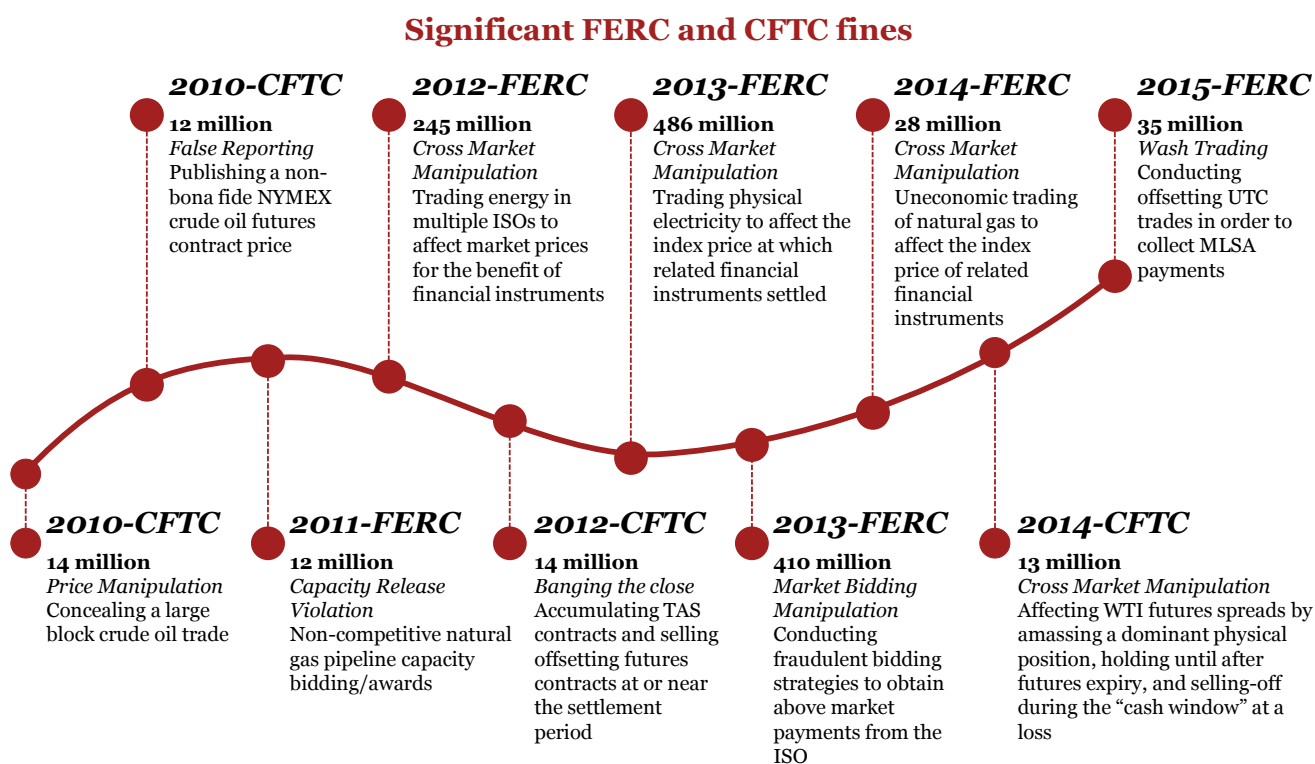
⁸ <http://www.ferc.gov/enforcement/self-reports.asp>.

analyses can drag and hinder compliance officers when it comes to surfacing potential problems. By contrast, both the FERC and the CFTC make use of sophisticated software, extensive data sets, and advanced algorithms that have enabled them to become more and more effective at detecting suspicious trading behaviors. As a result, the agencies are fast—and getting faster—at identifying possible manipulation and abuse.

Some energy-trading organizations have responded by implementing new trade surveillance systems. But these systems are often installed as is, without the customization needed to properly reflect the specific operating characteristics of the energy-trading market or the nuances of an individual company's risk and product profile.

Those surveillance gaps can leave compliance teams shorthanded, unable to meaningfully detect policy infractions, and therefore vulnerable to increased sanctions. Regulators have made it clear that reckless conduct is enough to constitute intent,⁹ and that includes failing to maintain adequate systems, oversight, and controls. During the past five years, the CFTC has issued many fines specifically for supervisory failure, ranging from \$125,000 to \$14 million (Figure 1).¹⁰

Figure 1: The continuing trend of financial penalties for energy-trading infractions



⁹ <https://www.ferc.gov/whats-new/comm-meet/011906/M-1.pdf>, footnote 109.

¹⁰ [http://www.cftc.gov/LawRegulation/Enforcement/Enforcement Actions/index.htm](http://www.cftc.gov/LawRegulation/Enforcement/Enforcement%20Actions/index.htm).

Energy-trading firms with the strongest compliance programs not only potentially reduce the risk of costly penalties but also see a range of other benefits that include reduction of trade risks, increased trade, and improved business efficiencies because their compliance activities give them more insights into their own operations (sidebar). Achieving those benefits requires leaders to address deficiencies in their trade surveillance programs by developing an approach that better reflects, tracks, and optimizes core trading risks and opportunities.

Benefits beyond compliance

With the right support and the right tools, compliance teams can provide valuable insights to the business and to senior management that go beyond their immediate remit. Robust trade surveillance programs and systems that have been customized to an energy-trading firm’s industry and specific business needs both help maintain compliance and increase transparency into the business—and they can result in operational efficiencies.

<i>Impact</i>	<i>Sample benefits</i>
Operational efficiency	- Processes customized and tuned to an energy-trading firm’s specific needs reduce time spent on manual processes, reduce the number of false alerts, and increase teams’ productivity. - Consolidation of internal and external data sources into the trade surveillance system creates efficiencies that reduce cost, increase productivity, and enable real-time monitoring.
Investigative effectiveness	Increased effectiveness in identification and investigation of suspicious activity results in reduced trade risks and lower costs.
Regulatory risk reduction	Effectively enabling groups responsible for organizational compliance and for mitigation of risk reduces the risk of fines and reputational damage.
Business insights	- A robust and optimized trade surveillance program leads to greater transparency and generates insights into the performance of the business, which can help leadership make informed decisions. - Integrated data systems facilitate real-time reporting, which increases the adaptability and flexibility of decision making.

Where energy trade surveillance programs can veer off course

Many energy-trading firms are struggling to keep pace with the intensification in regulatory scrutiny. Part of the challenge lies in the diversity and complexity of energy markets. Whereas trading assets used to consist primarily of basic physical products such as natural gas and electricity, now those assets include arrays of sophisticated financial derivatives. That complexity makes it hard to write precise algorithms for catching precluded behavior. Trading volumes have also spiked in the past 20 years, which can

make identification of aberrant or noncompliant behavior more difficult. Those issues notwithstanding, internal governance and organizational factors pose even bigger issues—ones that are significantly adding to the compliance challenge.

In our experience, the most-critical trade surveillance program breakdowns are occurring in the following areas (Figure 2):

Lack of leadership and accountability: In many energy-trading organizations, compliance is still viewed primarily as a cost center. That viewpoint can make it hard to attract the executive sponsorship and the budget needed to authorize the (sometimes sweeping) changes required at the enterprise level. In the absence of strong and sustained leadership commitment, support for initiatives and budgets can wax and wane. The result is that some surveillance programs are only partially implemented, or they're not maintained regularly enough to accommodate (1) changes in legislation and regulatory interpretations or, as new areas of business are pursued, (2) new markets entered or new strategies applied.

Figure 2: The core components of an energy trade surveillance program



Weak data management:

Many energy-trading organizations have implemented energy-trading and risk management (ETRM) systems to satisfy risk, credit, accounting, and other general business needs such as gathering trade and reference data. Such information is vital to monitoring trade activity and usually feeds into the trade surveillance system, yet ETRM systems are rarely programmed to factor in those critical compliance needs. This disconnect results in data that has often been aggregated to present valuable risk information but lacks the detail to support the trade, trader, or market surveillance required to maintain compliance. In addition, inadequate data sourcing typically results in gaps, so that the information the ETRM system does capture is incomplete or inaccurate.

Furthermore, many trading organizations rely on disparate data sources that have not been centralized for compliance reporting and oversight, resulting in inefficient manual processes and lack of real-time insights. Strong internal and external data management (covering areas such as trades, counterparties, electronic communication, voice data, market information, social

media, and regulatory filings) is essential to any surveillance program. Without it, energy-trading organizations have difficulty in identifying noncompliant trading behaviors against an evolving mandate. For example, the appearance of cross-market manipulation or wash-trading activity using only internal data often gets invalidated when considered in the context of broader market trading behaviors or in the context of hedging strategies or various e-communications. With the right data elements, such patterns can be detected automatically, thereby reducing false positives because the alerts are disqualified from the need for a forensic review.

Improper tuning: Compliance teams use trade surveillance systems to monitor and detect data patterns associated with anomalous or noncompliant trading. The systems originated in the financial services industry and are being repurposed for energy organizations, which sometimes requires significant configuration to meet the desired specifications. Our client work shows that many of these organizations struggle as they seek to accept the off the shelf capabilities.

Done correctly, system configuration addresses the gap between the preprogrammed rules that come with the system to guide data search and analysis and the firm's energy-specific trading, business, or operating environment. Without these subjective configurations, systems are less effective at catching relevant events, and they may fail to deliver the full benefit of the investment.

Still, even those organizations that have made the effort to configure may experience limited efficacy over time and not recognize it. As the rules and the regulatory scrutiny in the energy industry continue to evolve and gain more visibility, there is additional urgency for compliance teams to perform iterative reviews of the initial configuration. This critical step enables them to keep pace with the unique requirements of their sector and their business, resulting in a more intentional, specific compliance risk profile. Continual reviews may mean that particular rules shift in and out of relevance as regulators alter their focus or as business strategy changes. Furthermore, while organizations may have an interest in detecting *all* forms of noncompliance, many have quickly

discovered the impracticality of this ambition, and they have instated mechanisms to hone their monitoring systems to the particular subset that most applies, depending on the business and its risk profile.

Poor documentation and case management: In our experience, many energy-trading organizations underinvest in case management and suffer from inadequate documentation processes. For example, some companies do not retain histories of past alerts or breaches. Such lack of documentation can make it harder to respond promptly and fully to regulators and can make the process unduly costly and time consuming. Case management can help expose historical patterns of behaviors that may not be evident in a single-case incident. For example, if a trader is routinely found to be breaching position limits or routinely involved in possible market manipulation—even if the trader has been previously cleared of wrongdoings—a history of multiple alerts may indicate a higher-risk trader and possible deceptive acts, which may warrant further investigation.

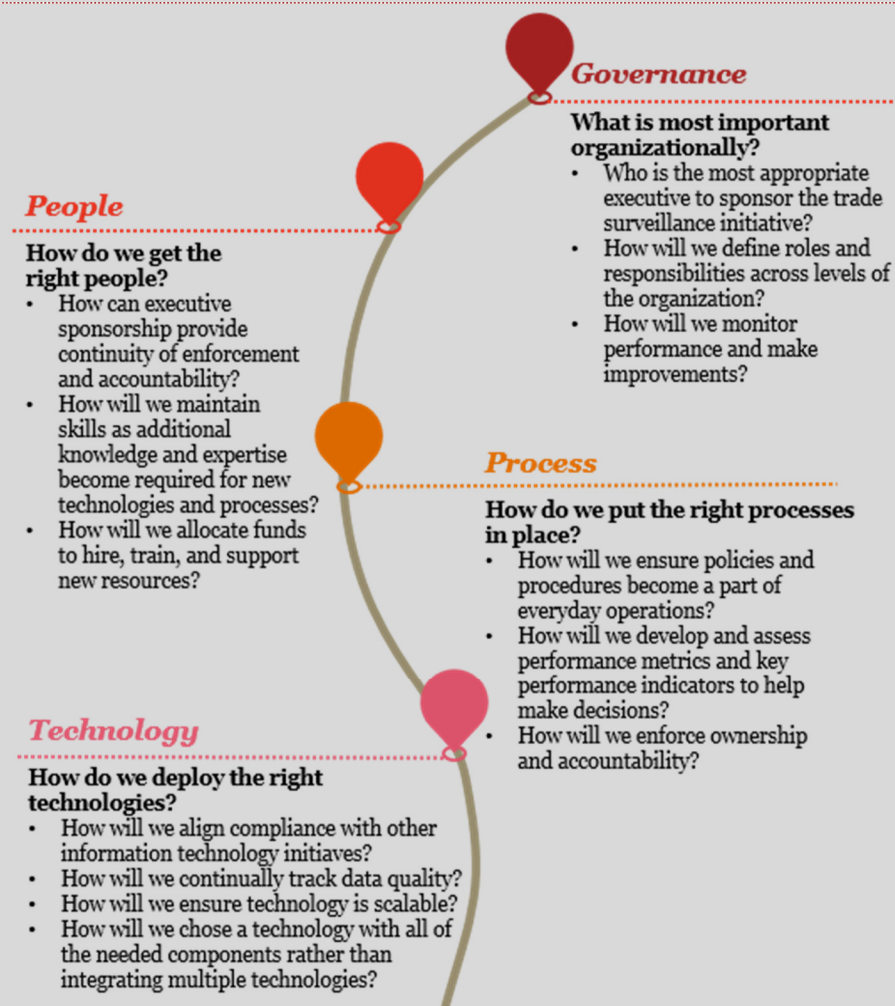
Best practices mandate documentation throughout the trade surveillance process. Documentation is especially critical during investigational stages because the information gets incorporated into the data used for tailoring and fine-tuning the trade-monitoring system. Documentation also supports active regulatory reviews by providing an audit trail and demonstrating quick cooperation with regulators. Organizations with strong record retention, case management, and documentation processes are far more likely to remain in good standing with regulators, especially because the FERC looks for good-faith effort ¹¹ in maintaining effective trade surveillance and due diligence.

¹¹ <https://www.ferc.gov/whats-new/comm-meet/2008/101608/M-3.pdf>.

The right questions to get back on track

Each trade surveillance program is of course unique to an organization, but the foundational elements required for sustained success are the same for all. Taking the time needed, at the outset of the implementation, to truly understand and then clearly define program goals, to gain buy-in and support, and to put a plan in place that will create and maintain the surveillance program will set the course for success. Asking the right questions—and getting the right answers—up front facilitates that planing (Figure 3). The same questions can also help redirect an existing surveillance program that is struggling to meet expectations.

Figure 3: Foundational questions to set the tone for success

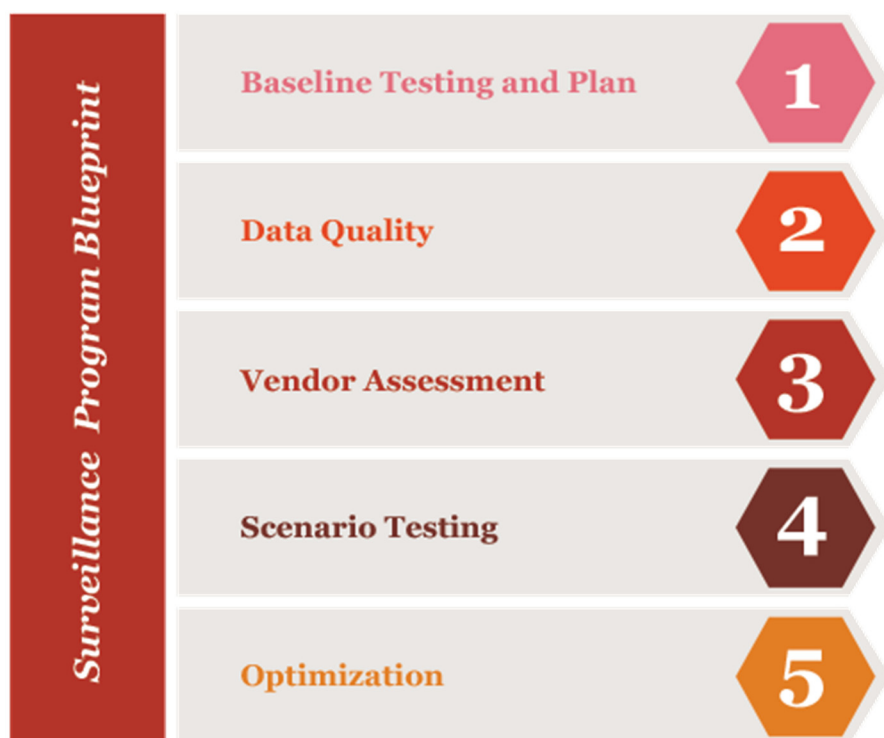


Customization is the key to keeping pace

Energy-trading organizations operate in a unique environment that comprises physical and financial assets, complex derivatives, hedging contracts, and global regulatory bodies. As a result, trade surveillance programs must be tailored not just to those industry realities but also to organizational risk profiles, operating footprints, and business needs.

And even though programs will vary according to which trading behaviors require the closest monitoring and which detection approaches are preferred, the trade surveillance model should be anchored to five common building blocks (Figure 4).

Figure 4: Build a customized trade surveillance program



1. Establish a baseline, a vision, and a plan

The implementation of effective trade surveillance requires establishing a baseline, determining a desired future state, and developing a plan for moving from one to the other.

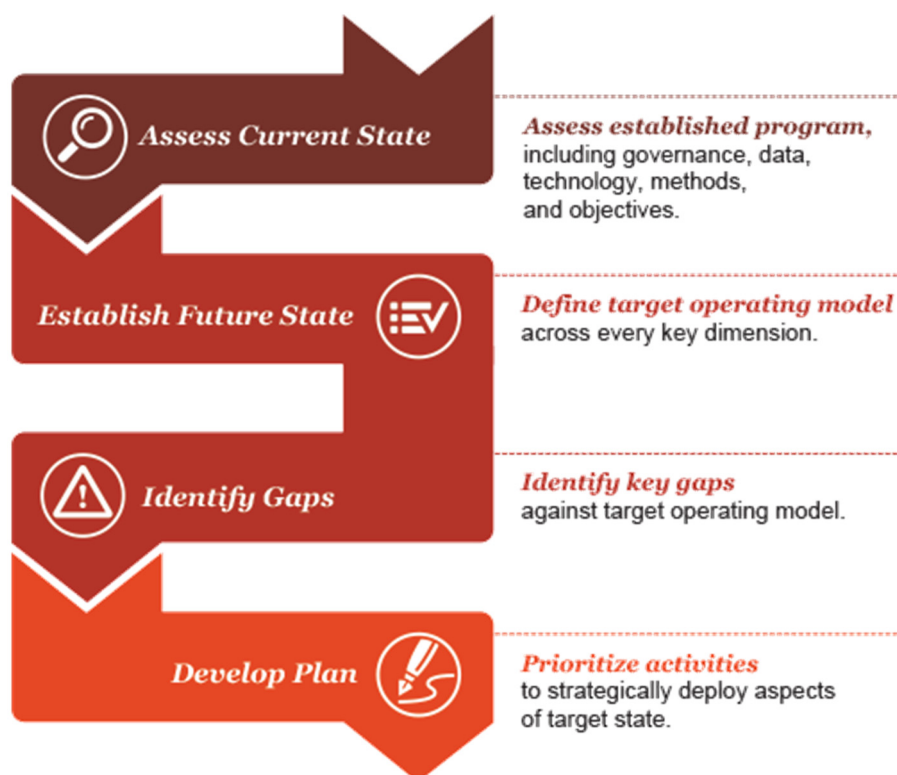
The baseline enables a compliance team to test the fitness of its trade surveillance program as a whole in order to flush out systemic and emerging issues proactively. A comprehensive assessment is also critical in order to determine where the

organization should focus its attention and resources. Otherwise, the organization might hone in on isolated areas that may not have much material significance, or it could unearth problems only after they have ballooned.

For example, one large energy trader went into its trade surveillance assessment believing that its documentation review processes were its greatest weakness, thereby making it harder and more costly to respond to regulatory queries. The firm assumed the solution would be to hire a

technology vendor that would automate some of those processes. However, when the firm conducted a detailed assessment of what it would take to go from good to great in the area of surveillance performance, the analysis uncovered a number of other, serious potential exposures—ones that would require more than just process automation to fix. Taking the time up front to define a target operating model, identify key gaps, and prioritize activities enabled the firm to pinpoint where it needed to focus its investment and resources (Figure 5).

Figure 5: A comprehensive assessment and plan can serve to focus the surveillance program on critical areas



2. Get your data house in order

Traders and compliance professionals must make sure the data they're using are accurate and sufficiently complete; they must integrate pertinent information from both internal and external sources to contextualize and validate scenarios and findings; and they must determine whether additional sources of information are needed. For instance, an energy-trading company might believe it has a potential issue on its hands if cross-market trading data seem to show that traders have intentionally lost money in one market in order to profit from another. However, the real issue may be that the monitoring system that tracks those positions has failed to take into account certain factors such as a hedging requirement, a complex layered strategy, market conditions, or even historical trends. That additional information can provide a more complete view, potentially proving that no wrongdoing occurred.

The granularity of the data collected is also important because regulators may request transactional-level details. Often, data coming into the

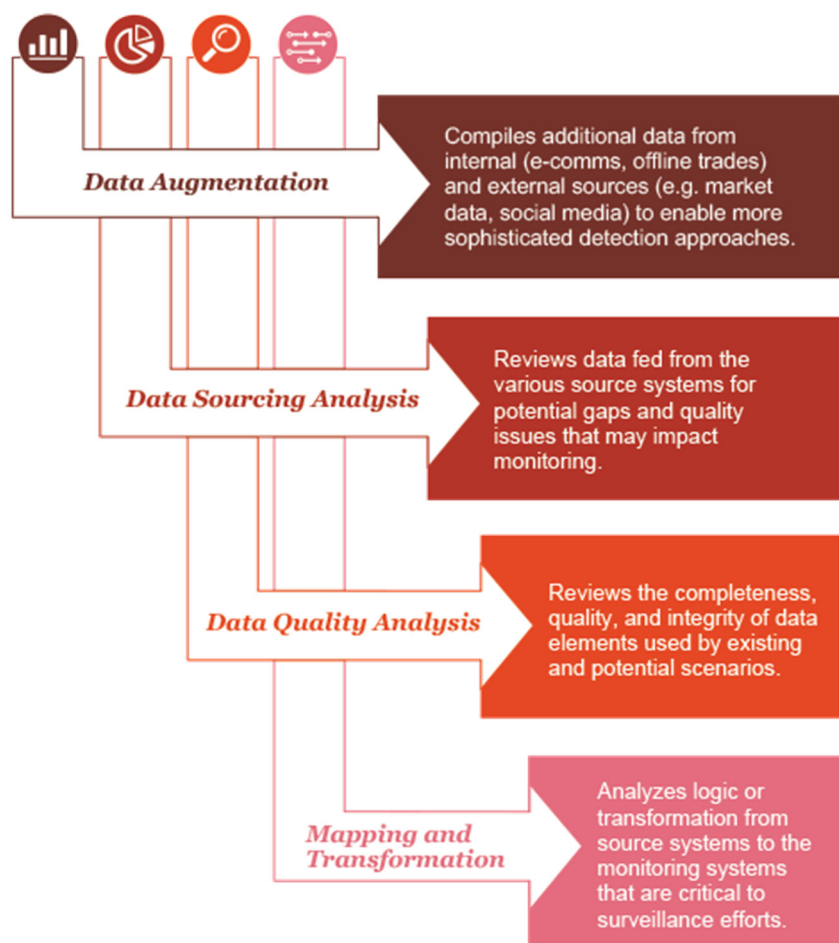
surveillance system have been aggregated for risk management, or other purposes, making it difficult for compliance teams to respond to regulators' requests. And even though there may be times that data do not exist in the format needed, the collection of more-granular, transactional-level data when possible will put surveillance firms in good standing with their regulators. This may also drive a policy update to require the creation or capture of the lower level data.

It's not enough to have well-sourced and integrated data systems, however. Organizations must check and regularly refine the quality of the data flows as part of a continual retuning process to keep up with changes in the business and operating environments. Data quality analysis can test for completeness, relevancy, and integrity. For example, it can check whether data are in the correct format, whether the correct translations and calculations are being made, and whether all data are accounted for.

Finally, a crucial component of the integration of data from source systems to a trade surveillance system is the conversion of the data so that it can go into the surveillance system without losing critical information. Correct mapping and transformation of the source data are especially important for

unstructured data that often lack the metadata to search or link them to appropriate transactions. Once converted, the data take the pertinent information contained in both the structured and unstructured data sets and makes it easily usable for further analysis (Figure 6).

Figure 6: A strong data management framework is essential for a successful surveillance program



3. Assess vendors

Most organizations will have to partner with one or more vendors to define and implement a desired monitoring program. How an energy-trading organization follows that selection process is critical. The firm must rightsize the solution to its specific set of compliance needs and determine which of several commercial (user, enterprise, server-based) and delivery (in-house, cloud, software-as-a-service) models would best support its target operating model from functional and cost points of view.

Organizations should take the following considerations into account when assessing vendors:

- **Functional fit:** A strong understanding of an organization's compliance drivers helps best define system requirements and more accurately score each tool's fit to the firm's specific needs.
- **Cost of ownership:** Many factors affect total cost—for example, licensed versus subscription, maintenance versus monthly fees, training, complexity to implement,

and time to value. An organization should have a full understanding of those elements and be able to determine which would work best for the firm.

- **Architecture compatibility:** To be effective, the platform should align with the organization's existing architecture standards and tools.
- **Strategic relationship:** Working with a vendor that demonstrates a vision compatible with the organization's long-term objectives and that has supported many customers with similar objectives will lead to a more successful outcome.
- **Depth of service:** In addition to technical expertise, a vendor with regulatory and energy-trading specialists on staff can help verify that a firm's system meets the unique requirements of the organization and the industry.

4. Conduct scenario testing

For energy organizations, scenario testing is one of the more challenging aspects of trade surveillance because of the inherently complex nature of energy trading. An ideal scenario test is able to detect suspicious patterns of behavior and then map out other connected areas that would also need to be taken into consideration to ascertain whether market abuse had occurred. For instance, cross-market manipulation may include sustained uneconomic trading in a physical position (price making) to benefit a related financial position (price taking). The ideal scenario test identifies both the price-making and the price-taking positions.

However, the majority of rules and scenarios a firm has in place either (1) are unable to provide the holistic view of elements that relate transactions to one another and are therefore sometimes inadequate for the risk the firm faces or (2) have deviated from specifications

over time due to lack of monitoring. An example of this is a hedging strategy that may change over time and may impact testing. In addition to being critical to scenario testing, understanding these changes and keeping clear records will help with explanation to regulators when they scrutinize declarations of bona fide hedges.

Scenario tests should be checked regularly for efficiency and effectiveness:

- **Detection logic testing** assesses whether existing and potential scenarios are aligned with current business intents.
- **Detection output evaluation** judges the effectiveness of scenario outputs by understanding current industry practices and circumstances, documenting historical alerts, and receiving feedback from investigators.

5. Optimize your systems

To facilitate continual and effective monitoring of trading behaviors, an organization should ensure that its detection approaches are up-to-date and should use correct metrics.

Those steps are instrumental in creating cost-effective programs that avoid excessive false alerts. Inappropriate threshold settings can lead to either (1) a high number of false-positives, resulting in excess alerts, which are difficult and costly to manage, or (2) false-negatives, resulting in dismissal of important areas, when in fact some should be escalated.

Many techniques are available to help organizations optimize and fine-tune their detection logic for improving system outputs and reducing constraints on resources. The following are a few examples of optimization approaches.

Segmentation is the process of monitoring and analyzing with the same threshold those entities behaving similarly—while having different thresholds for other entities—rather than applying one threshold across all entities regardless of their characteristics.

In Figure 7, an organization would generate many false-positives on desk 2 but would miss suspicious activity on desk 1 (false-negatives). Segments can be created using either qualitative or quantitative approaches, with leading practice requiring the use of both (Figure 8).

Figure 7: Applying thresholds to similar entities increases detection effectiveness

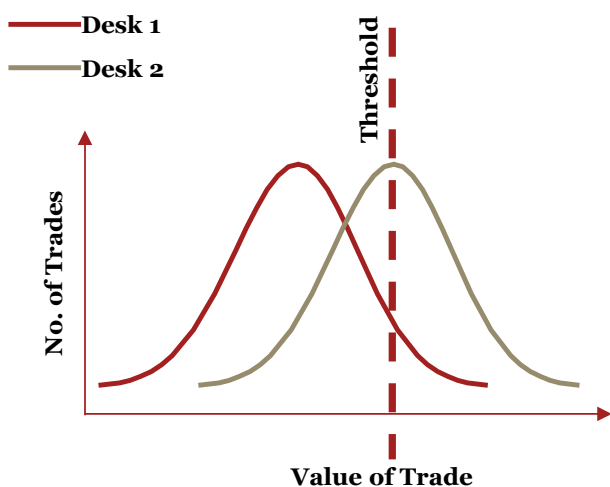
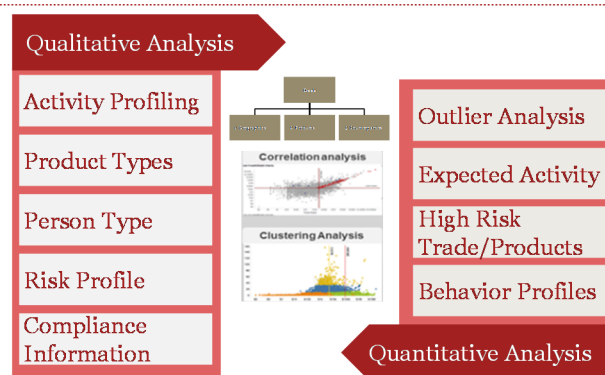


Figure 8: Top to bottom approach to segmentation



Threshold tuning is the process of calibrating a surveillance rule to generate more true-positive alerts and fewer false-negatives.

Many organizations spend most of their time focusing on reducing false-positives, but regulators are interested in the level of false-negatives. Sample data taken from both above and below the threshold can help calibrate the surveillance rule, thereby addressing both issues (Figure 9).

Risk scoring uses risk factors to indicate the overall relative risk of an alert. These scores result in a more robust and more efficient process of prioritizing, routing, and handling alerts (Figure 10).

Behavioral analysis

monitors, analyzes, and benchmarks behavioral trends related to trading activity. Evaluating behavioral trends by using advanced analytic techniques can help an organization further capitalize on its investment in surveillance technologies and increase the accuracy of its alerts. Key features include:

- The use of unstructured data analytics to monitor for high-risk communication, which can mature to include natural language processing techniques such as co-occurrence and sentiment analysis.

- The analysis of behavior patterns in communication, including type, frequency, and parties involved, which can mature to become network-analysis techniques.
- Enhanced confidence in observed rule breaches for high-risk scenarios by providing correlated patterns of behavioral anomalies to accompany structured data observations.

By continually optimizing trade surveillance programs, organizations can make more-informed trade decisions such as recognizing market areas with high risks or areas where possible manipulation has occurred. An optimized system can also reduce costs as efficiency and effectiveness increase.

Figure 9: Sample data can be used for threshold calibration

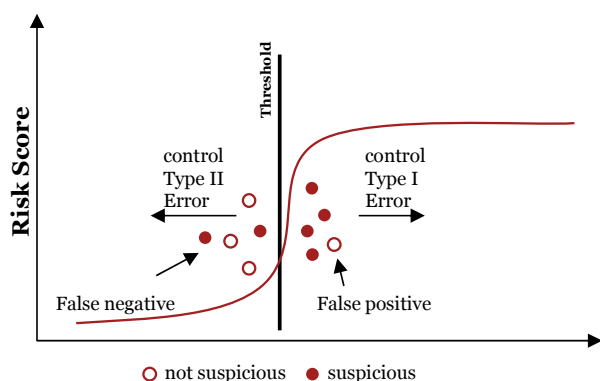
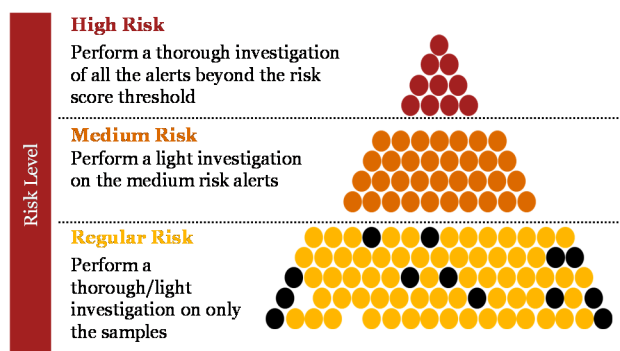


Figure 10: Alert risk scoring can increase the efficiency of the investigation process



Some immediate actions that compliance officers can take to improve their trade surveillance programs include:

- Perform a risk and current state assessment to refresh your view on your risk priorities and existing compliance coverage.
- Develop a future state roadmap that considers governance, policy and procedures, technology, continuous monitoring, and case management, and includes a clear implementation plan to address identified gaps.
- Evaluate vendor offerings against the specific requirements detailed in the future state roadmap.
- Configure the firm's surveillance system to the firm's specific requirements and trading environment, taking into account data quality and optimization.

Beyond the compliance goal

Given regulators' increased mandates, increased levels of authority, and increased abilities, the challenge for organizations that want to stay ahead of oversight has probably never been more imposing. As fines and penalties continue increasing in frequency and severity, energy-trading organizations are moving away from the wait-and-see disposition that many used to adopt.

With regulators able to tap sophisticated software and data sets, organizations have to embrace the advanced approaches discussed here and fine-tune their trade surveillance programs so they can safely manage their regulatory, reputational, and financial risks. The benefits of doing so go beyond remaining compliant in that the data extracted by compliance functions can provide real actionable value for the wider organization.

***To have a deeper conversation about
optimizing your trade surveillance
system, please contact:***

Seth Rosensweig

Principal
Phone: (646) 471-6762
seth.rosensweig@pwc.com

Charlie Sanchez

Managing Director
Phone: (713) 356-4201
charlie.sanchez@pwc.com

David Dorleans

Director
Phone: (713) 356-6408
david.e.dorleans@pwc.com