kx | it's about time

The Need for Consolidated Surveillance and Supervision

The Changing Regulatory Focus

The move from principles-based to rules-based regulation after the financial crisis of 2008 did not fully work, as evidence of continued malpractice clearly shows. Is that a poor reflection on the regulator's ability to define the rules to stop abuse, or does it merely confirm the sad reality that man is better at defying laws than defining them? Either way, it wasn't successful, so a new approach is required for detecting financial crime.

The problem is, miscreants know well how to circumvent the rules seeking to detect them, which is what makes it so difficult for the various lines of defence to catch them. That, in part, is why the regulatory focus is now less on strict adherence to the static rules they define and more on the broader area of conduct risk that underpins them. So now it's about taking a wider view, looking across the organization, and across the behavioral spectrum, to identify and thwart financial crime.

Taking a Wider View

Traditional black-box based compliance has had limited success in detecting fraud because its focus is too restrictive. While individual transactional analysis is important, contextual analysis needs to survey a wider spectrum. It's now accepted that detection is not just about individual systems and trades, it's not just about fixed limits and parameters, it's not just about siloed reports and audit trails – it's about all the interactions, dependencies, changes, communications, patterns and behaviours across the trade lifecycle and the organization, that standalone alerts and static rules simply don't catch. It's about signs that might not be apparent in individual solutions but may be revealed using techniques like statistical analysis, machine learning and natural language processing on the broader data flow that surrounds them.

Evidence of crime is not just in the trade that makes the undue profit.

It's in all interactions around it – the email that suggested it, the tweet that flagged it, the call that confirmed it, the news release that followed it.

It's in swathes of data that supervisors need, but don't have easy access to.

Evidence of insider trading, for example, is not revealed solely in the trade that makes that undue profit, but it may become evident across the price discovery process that precedes it, the email that suggested it, the tweet that flagged it, the call that confirmed it and the news release that followed it. And it's not in just one instance, it's in the regularity of it happening, the links between the parties involved, their overlapping social networks and possibly their employment history. So, it's in e-Comms, social media, trade history, user profiles and a broad swathe of data that supervisors need but don't have easy access to.

That's where consolidated surveillance comes in.

The Value of Consolidation

Consolidated Surveillance aggregates the disparate and expansive data sets required by both humans and machine learning techniques to identify the actions and links that may infer malpractice. A machine learning algorithm can traverse mountains of data much more diligently than a human. It can parse documents according to pre-defined lexicons more rigorously. It can correlate times and actions more forensically. It can comb haystacks for needles in a way humans cannot. It is incredibly powerful, but it still cannot outperform man in at least one area – it cannot smell a rat. That's where data consolidation helps, in enabling humans to not only validate what algorithms may suggest, but to possibly identify things they didn't.

With easy access to consolidated data, supervisors can, for example, perform event-by-event analysis to view the emails, voice call transcripts, text messages, internal trades and counterparty codes that suggest cross-department collusion. They may spot subtle nuances and coincidences that either confirm or undermine a suggested finding or alert. They may spot something completely new that the existing rules didn't identify. That in turn feeds back into the ongoing training loop of the machine learning algorithm that refines the regulatory taxonomy and improves the next round of surveillance.

In short, consolidated data fuels both machine learning and supervisors in effective, accurate and dynamic detection of financial crime.

Supervisors may spot something completely new that the existing rules didn't identify. That in turn feeds back into the ongoing training loop of the machine learning algorithm that refines the regulatory taxonomy and improves the next round of surveillance.

The Challenges of Consolidated Surveillance

If consolidated surveillance is so good why is it not widely adopted?

Part of the problem is that most organizations still have massively siloed systems. They exist because regulatory requirements were often addressed consecutively, and in isolation, in the order they were received rather than strategically as a service requirement. Given time constraints it was understandable. When people talk about the 3Vs of Big Data they could equally be talking about the volume, velocity and variety of regulation faced by banks. It was estimated that at one point there were over a thousand initiatives worldwide with each imposing heavy burdens on meeting regulatory demands and honoring shareholder obligations. They were onerous, far reaching and complex.

Inaccuracies arising from poor quality and missing data have resulted in untold risk residing in false negativities, and the high operating costs of investigating false positives.

Each alone is bad, both together is probably terminal.

The challenge in meeting regulatory requirements was not in knowing what to do, as that was reasonably well defined, it was more in how best to do it. Unfortunately, the survivalist tendency of resorting to spreadsheets, bespoke code changes and one-off interfaces has been seen to have yielded pyrrhic victories - providing solutions for today but problems for tomorrow.

As a result they face problems of data quality, data duplication and integration that have resulted in the untold risk residing in false negatives, and high operating costs in investigating false positives. Each alone is bad, both together is probably terminal. And they are more prevalent today than many would care to admit.

But there is a solution.

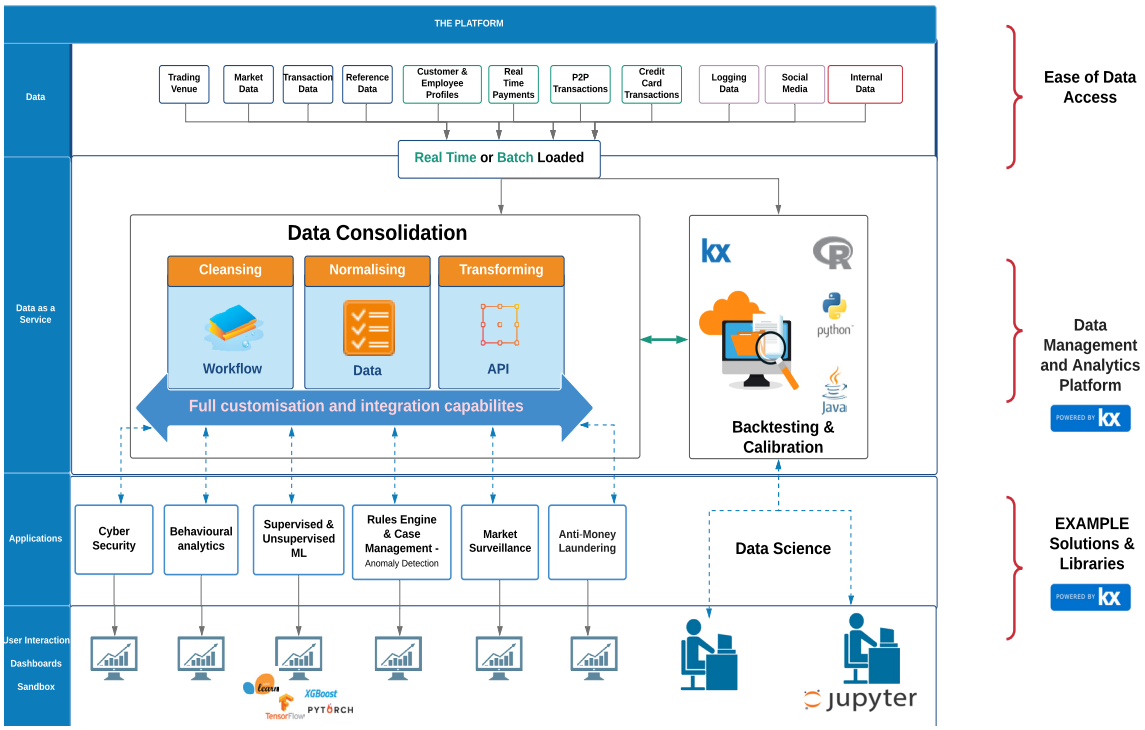
Right Approach, Right Architecture

What is required instead is an integrated architecture that combines full lifecycle data management and processing

- Data capture from multiple sources including exchanges, OTC, internal, social media, voice transcripts and other documents.
- Centralized data management for cleansing, normalization and transformation.
- Flexible consumption giving controlled access to the data in the appropriate format.
- Accompanying analytics capabilities to parse, process and evaluate data.
- A scalable and efficient architecture that can analyze the massive volumes of price discovery post execution and communications data without farms of servers.
- A visualization layer for displaying and distributing the results to the right people at the right time.

The result is an enterprise platform that simultaneously addresses multiple regulatory and jurisdictional obligations, using a common source of trusted data with a comprehensive data lineage. Controlled and audited flexibility of data model, scenarios, models, alerts, behavioral profiling analytics and case management provides the perfect platform to meet the ever changing regulatory requirements and the expectation of continuously improved monitoring. By being configurable to each bank's specific operating models, the platform is equally applicable to all lines of defence. Dynamic determination of parameters, sophisticated standard and bespoke algorithms and contextual analysis, together with comprehensive backtesting delivers significant productivity improvements.

In support of a "buy and build" philosophy, the platform offers an open architecture including open interfaces, the facility to reuse and extend functionality in multiple languages, together with integration to a wide range of machine learning libraries. With unparallelled performance the platform offers both real time and retrospective analysis for huge volumes of data on a low hardware footprint. In short it's a flexible platform for all current and future surveillance and data analysis requirements where reuse of data provides completeness, accuracy and timeliness.



Tactical and Strategic Value of Consolidated Surveillance

While regulatory compliance was once seen as a troublesome business overhead a more enlightened view is that the regulatory requirements are the underpinnings of better and more efficient processing. You can only report (accurately) what you know and the data remediation, process re-engineering and processing infrastructure required to fully satisfy regulations can help to reduce risk, improve decision making and run the business more efficiently – but only if addressed in a strategic manner as a program of change rather than as isolated, tactical projects. Patch solutions, that great tactical refuge, may satisfy short term demand but will almost certainly compromise longer term advances leaving deadlines met, but dead ends set.

That philosophy is captured by the Basel Committee on Banking Supervision in their fourteen principles for data and risk aggregation and reporting capabilities that were drafted in response to the inability of many banks to accurately or quickly consolidate their global risk exposure (as was evident during the 2008 global financial crisis).

14 Principles of BCBS	
Governance and Infrastructure	• Define a strong data aggregation and risk reporting governance framework • Design build and maintain a robust data architecture and IT infrastructure
Risk Data Aggregation	• Achieve accurate and reliable aggregation using automation where possible to minimise errors • Ensure completeness of data throughout the organisation across appropriate silos, assets, and departments etc. • Timeliness - ensure data can be fully aggregated in a timeframe appropriate to the underlying risk • Adaptability – provide the capability for flexible ad-hoc, on-demand reporting as may be demanded in exceptional circumstances
Risk Reporting Practices	• Accuracy - Risk management reports should accurately and precisely convey aggregated risk data and reflect risk in an exact manner • Comprehensiveness – scope and depth of information should be commensurate with associated risk • Clarity and usefulness – reports should be clear, concise and relevant • Frequency should be set appropriately but with flexibility for increase in times of need • Distribution should be targeted appropriately and maintain confidentiality
Supervisory review, tools and cooperation	• Supervisor review to ensure compliance • Apply Remediation where required • Cooperate with counterparts in other jurisdictions

Lines of defence need to address the reality that their current approaches are deficient, myopic and operationally expensive. They are deficient because they are limited in data, myopic because they are limited in scope and costly because they are inefficient and hard to maintain. The resolution to all three is consolidated surveillance based on broader data sets enabling wider multi-factorial analytics over a common platform that ensure completeness, accuracy and timeliness of results. Further cost savings accrue by eliminating duplicate interfaces, infrastructure, technology stacks, alert management and support teams teams making existing regulations less expensive to manage and new regulations easier to implement.

Consolidated Surveillance, Behavioral insight

At a societal level, law enforcement is challenged by the metric of success. Do high detection rates indicate the efficiency of the detector or are they testament to on-going prevalence of the problem. The greater goal is deterrence. Multiple alarms and arrests at airport check-ins do not inspire confidence in passengers. It's their absence that does, as if perpetrators believe the likelihood of being caught is high they are less likely to proceed with their crimes.

Banks face a similar challenge in evaluating the efficacy of their surveillance results. Isolated systems performing isolated checks may confirm that individual rules have not been broken, but fail to detect an overarching pattern that indicates something suspect. To do that they must, like law enforcement and counterterrorism agencies, introduce behavioral analysis that acts on consolidated data to reveal evidence like an increase in emails to a new recipient, simultaneous back-to-back trades with an internal counterparty, near-but-not-quite limit breaches that had not previously been seen.

They need consolidated surveillance.

Lines of defence need to start thinking less like judiciary in interpreting crime and more like law enforcement in anticipating and thwarting it.

About Kx

Kx has been at the forefront of data driven solutions for the last 25 years. The core technology, specifically built to analyze and identify behavioural patterns across huge volumes of real time and retrospective data is used by every Tier 1 Bank in the world. The unique combination of leading edge technology and a large body of technical and capital markets expertise, makes Kx the right partner to deliver a strategic consolidated platform for both current and future regulatory obligations together with continuous improvements in risk-based profiling and productivity.

Surveillance and regulatory clients include banks, regulators, exchanges, brokers, proprietary trading houses and investment firms globally.

Kx Solutions

Kx for Surveillance

Kx for Surveillance is the world's first integrated platform for consolidated multi-factorial detection and investigation of market abuse, financial crime and fraud. Delivered with a complete library of MAR, eComms and AML models, new models can be added and easily incorporated into the comprehensive alert, workflow and case management infrastructure with full contextualized, granular-level investigation tools.

Kx Data Refinery

Kx Data Refinery provides a complete suite of tools for managing data from ingestion through to consumption by multiple parties in a consistent and controlled manner. Built on Kx technology, our solution combines the speed and performance kdb+ with powerful analytics and the rich visualization of Kx Dashboards.

Kx for Flow

Kx for Flow is a HTML5 white label foreign exchange trading platform offering users the ability to create bespoke liquidity pools and distribute price information to clients and markets. Our comprehensive turn-key solution provides in-depth risk management functions as well as real-time in-memory analytics.

For a discussion on how Kx could help your specific requirements, please contact **sales@kx.com**

Head Office
3 Canal Quay,
Newry,
BT35 6BP
N. Ireland
Tel: +44 (0)28 3025 2242

Belfast
The Weaving Works
Ormeau Avenue
Co Antrim
BT2 8HD, N. Ireland
Tel: +44 (0)28 9023 3518

Dublin
6th Floor, Block A,
1 George's Quay Plaza,
Dublin 2, D02 Y098
Rep. of Ireland
Tel: +353 (0)1 630 7700

London
5th Floor,
Cannon Green Building,
27 Bush Lane,
EC4R 0AN, United Kingdom
Tel: +44 (0)207 337 1210

New York
45 Broadway,
New York,
NY 10006
USA
Tel:+1 (212) 447 6700

San Francisco
535 Mission St,
14th Floor
San Francisco, CA 94105
USA

Toronto
31 Lakeshore Road East
Suite 201
Mississauga, Ontario
L5G 4V5 Canada
Tel: +1 (289) 329 0636

Ottawa
300 Terry Fox Drive,
Kanata, On,
K2K 0E3
Canada
Tel: + 1 (613) 216 9095

Sydney
22 Pitt Street,
Sydney,
NSW 2000
Australia
Tel: +61 (0) 2 9236 5700

Singapore
One Raffles Quay,
North Tower #30-03,
Singapore
048583
Tel: +65 6592 1960

Hong Kong
Level 66, The Center,
99 Queens Road,
Central
Hong Kong
Tel: +852 3965 3181

Tokyo
20F Shin-Marunouchi
Center Building,
1-6-2 Marunouchi,
Chiyoda-ku, Tokyo,
Japan 100-0005
Tel: +81 (0)36-634-9799