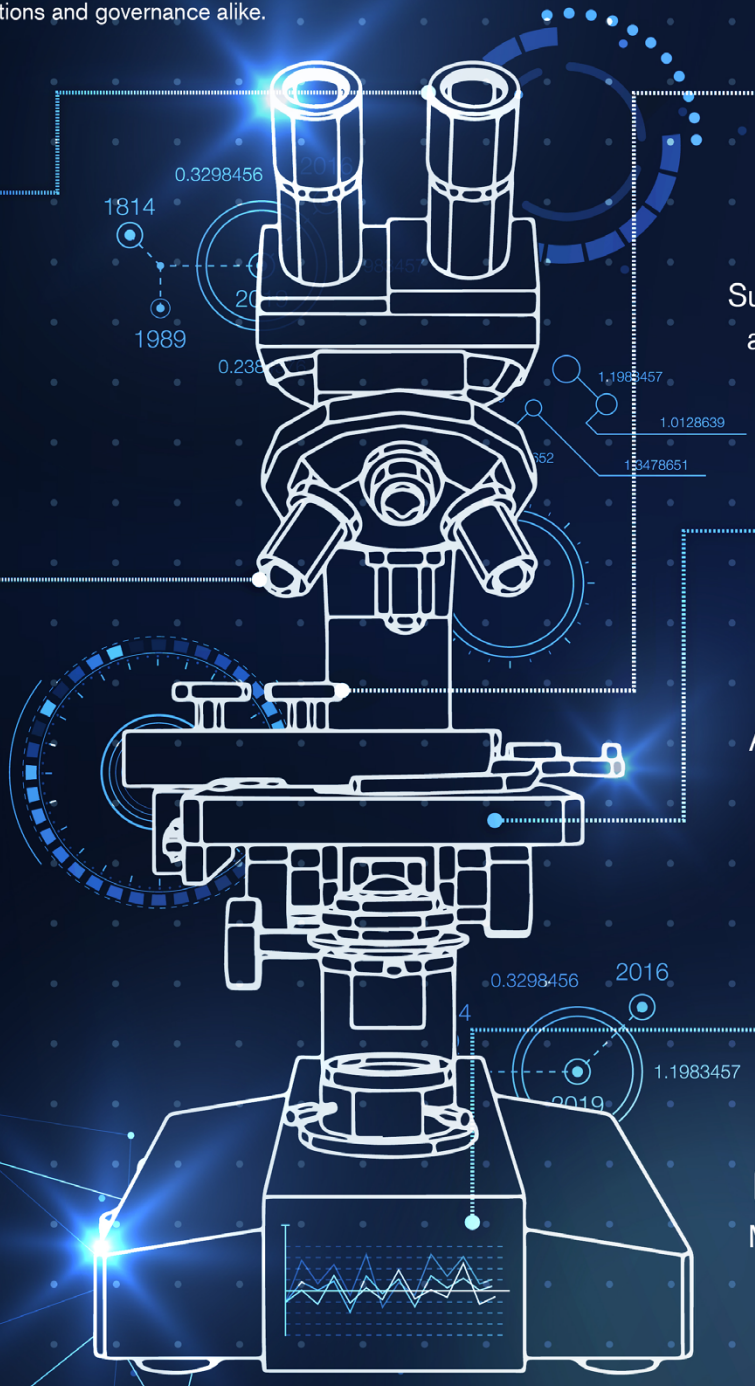
MARKET ABUSE MONITORING GOES FORENSIC

FIRST AND SECOND-LINE OF DEFENCE SURVEILLANCE OF POST-MIFID II MARKETS

The regulatory shift from MAR to MiFID II will impact more market participants, across more asset classes with more stringent requirements for Market Abuse Monitoring than ever before, requiring careful consideration of technology solutions and governance alike.



OTC AND HYBRID MARKETS

Forensic analysis of Voice and Electronic Media

CROSS-ASSET

Surveillance of cross-function and cross-asset strategies

MARKET STRUCTURE

Adaptability to fast-evolving new venues and trading mechanisms

REAL-TIME

Access to accurate and sequential structured and semi-structured data

ORDERS AND TRADES

Many new quote and order mechanisms (i.e. in Fixed Income)

GreySpark Partners has significant experience in analysing requirements, sourcing relevant systems and optimising surveillance strategies across first and second-line-of-defence areas.

For more information please visit:
greyspark.com

greyspark partners

Market Abuse Monitoring Goes Forensic

For those overseeing the orderly conduct of trading, the Market Abuse Regulation (MAR) in mid-2016 introduced some significant challenges. Specifically, MAR extended the scope of surveillance to orders as well as trades in order to capture the intent to abuse the market, and it applied to more asset-classes, to name but a few of the changes.

MiFID II builds extensively on this already onerous regulation, impacting more trading participants than ever before and across many more of their transaction flows. Add to this the challenges that come from the new, sometimes less-structured datasets and rapidly evolving market structures of fixed-income and structured products, and the requirements on systems and controls begin to look much more complex. Newly defined Organised Trading Facilities (OTFs) and Systematic Internalisers (SIs) must consider the heady mix of over-the-counter, voice and communications surveillance, alongside the exacting real-time requirements of Direct Electronic Access (DEA) and Algorithmic monitoring mandated by the now-notorious Regulatory Technical Standards of RTS6. What is common to them all is that they require very careful planning and consideration… and if that is not challenging enough, for many market participants this all must be achieved against a backdrop of budget-restrictions and more rigorous governance requirements.

> ***"The solutions available and their relevance and ease of implementation vary enormously, making analysis and vendor choice critical"***

Quote-driven markets, cross-asset monitoring and unstructured data

Those intimately familiar with the challenges cite cross-asset and cross-function monitoring and the need to converge OTC, voice and electronic communications into a single time line, as the main pain-points, closely followed by the requirement for audit and replay associated with the proof of regulatory due diligence. The uptick to holistic surveillance of these multi-dimensional market structures and regulatory changes are as fundamental as a shift from old-school policing to advanced forensics… Sherlock Holmes meets high tech Scenes of Crime…

Depending on the asset-reach and trading activities of the market participant, the solutions available and their relevance and ease of implementation vary enormously, making analysis and vendor choice critical.

If approached correctly though, well-defined governance, systems and controls not only have the potential to achieve compliance, but also to replace complex manual processes and minimise impact on IT spend and headcount, whilst improving oversight and efficiency.

That process involves;

- detailed analysis of the transaction flows and desks, especially the cross-functional and cross-asset flows
- understanding and sourcing the critical order, quote and trade data
- accurate definition of user roles, restrictions and accountability
- training material and full documentation of algorithms
- gap analysis of existing platforms and controls
- vendor analysis related to real time and forensic surveillance monitoring platforms
- migration to those newly selected technology platforms/ monitoring environments, and
- optimisation of alerts and procedures.

GreySpark Partners have extensive experience in reviewing, sourcing and implementing first and second-line of defence systems and controls as part of a one-off or retained engagement.

About GreySpark Partners

Founded in 2009, GreySpark Partners is a niche capital markets e-commerce, e-trading, risk and risk management consulting firm that specialises in providing advisory and consulting services to a wide range of Tier I and Tier II investment banks in Europe, Asia-Pacific, the US and globally. GreySpark consultants also work with asset management firms, hedge funds, institutional investors, private banks and wealth management companies – as well as exchange operators, FinTech providers and trading technology companies – to facilitate change and deliver technology to broader financial markets community.

GreySpark's specific areas of expertise include pre-trade risk management and algo documentation, cybersecurity, research-based IP creation and advisory, regulatory implementation and change management and software development services across a range of traditional and bespoke business, management and technology consulting services. ■