Stand out for the right reasons

PwC Market Abuse Surveillance Survey 2016

Survey respondents expect to increase their investments in surveillance solutions substantially, in the next 12-18 months, with the majority projecting between

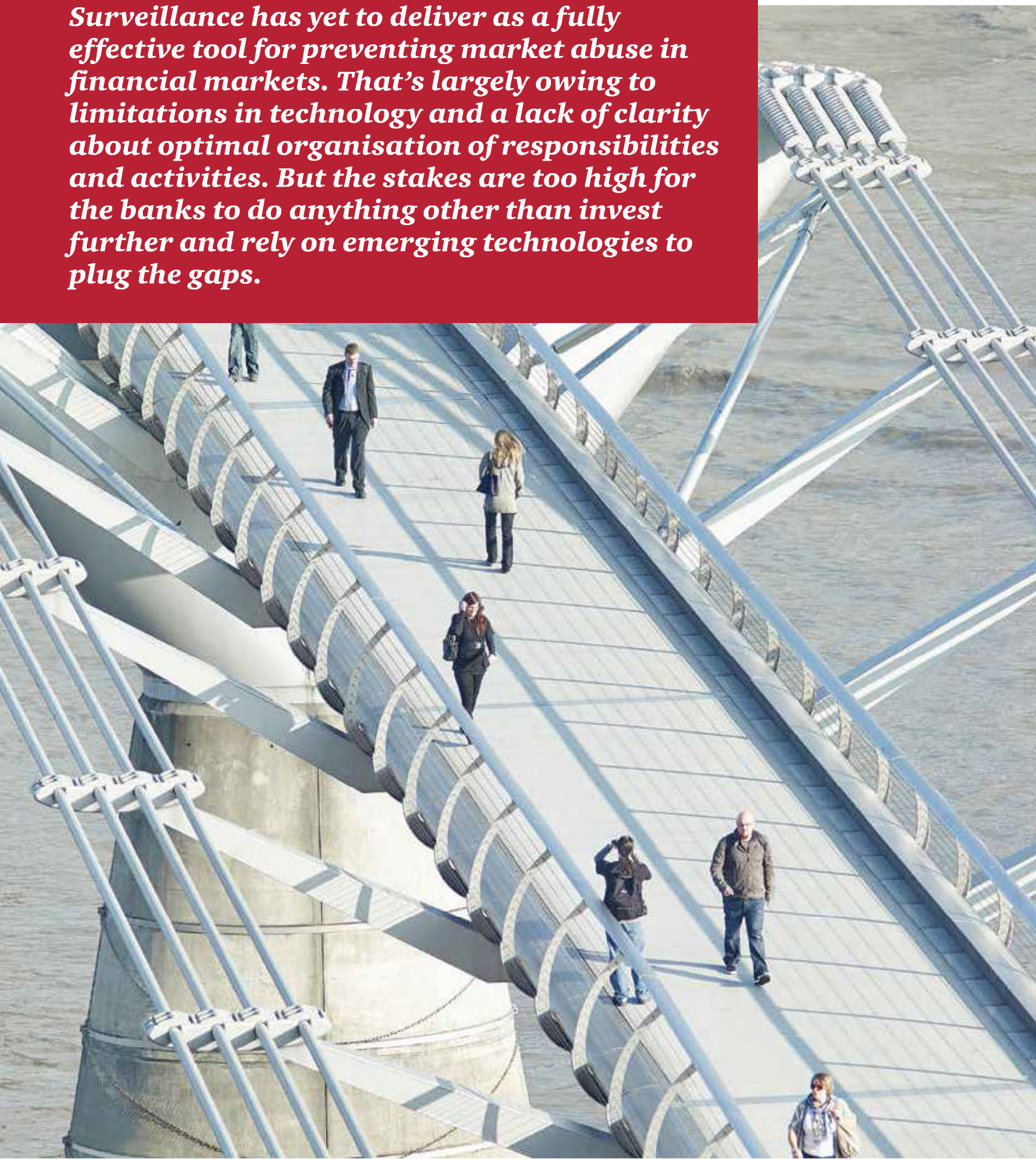
£5m *and* **£10m**

in additional spending.

pwc

www.pwc.co.uk

One of the biggest challenges in financial markets is how to conduct effective surveillance to spot market abuse and rogue trading. Surveillance has yet to deliver as a fully effective tool for preventing market abuse in financial markets. That's largely owing to limitations in technology and a lack of clarity about optimal organisation of responsibilities and activities. But the stakes are too high for the banks to do anything other than invest further and rely on emerging technologies to plug the gaps.



PwC Market Abuse Surveillance Survey 2016

In the last five years, financial institutions have incurred losses from rogue trading incidents, and have been investigated and fined over allegations across a range of market abuses. Interbank rate and foreign exchange market manipulation have cost the banks over $19bn in fines globally[1]. The FCA alone issued in excess of £1.4bn in fines relating to these issues between 2013 and 2015[2]. Regulators increasingly expect banks to monitor communications and trading activity to help identify and prevent future instances of market abuse.

However, over 140,000 people work in banking in London alone. That equates to tens of billions of emails, messages and phone calls every year. In a fast moving environment, those communications often use highly colloquial language and rapidly evolving terminology. And to be truly effective, surveillance needs to be able to spot new or emerging forms of abuse - likely to involve only a few traders and a handful of transactions – in this ocean of data. The question is whether banks can really use surveillance as an effective tool to prevent future instances of misconduct, market abuse and rogue trading, reading every message and checking every trade, or are the challenges too great?

Surveillance survey

To gauge banks' estimations of the challenge and to provide more transparency to the market, we developed a survey focused purely on surveillance. Our aim was to help understand:

1. *How banks are responding to regulatory developments*
2. *Whether any industry standards are emerging*
3. *How surveillance capabilities compare across the sector*

In all, twenty of the largest global banks participated in the survey, each with a significant presence in EMEA. The survey was conducted during December 2015 and January 2016.

Key findings

Banks are taking surveillance seriously and backing that commitment with investment. They are building bigger teams and increasing their surveillance spending. Firms expect to increase their investments in surveillance solutions substantially, in the next 12-18 months, with the majority projecting between

£5m *and*
£10m *in additional spending.*

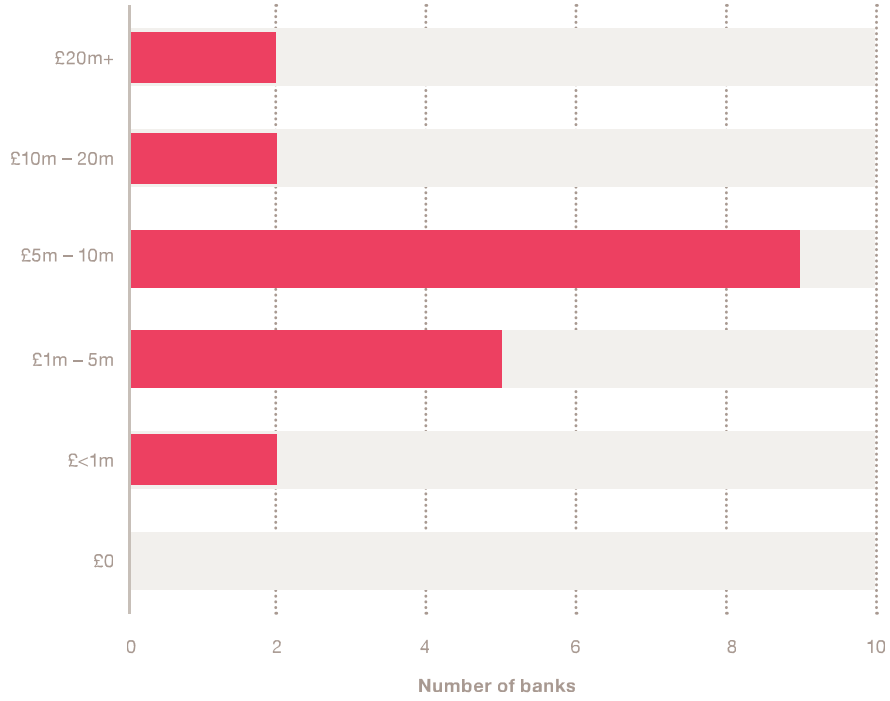
[1]http://www.bankofengland.co.uk/markets/Pages/fmreview.aspx#

[2]http://www.fca.org.uk/firms/being-regulated/enforcement/fines/2015
http://www.fca.org.uk/firms/being-regulated/enforcement/fines/2014
http://www.fca.org.uk/firms/being-regulated/enforcement/fines/2013

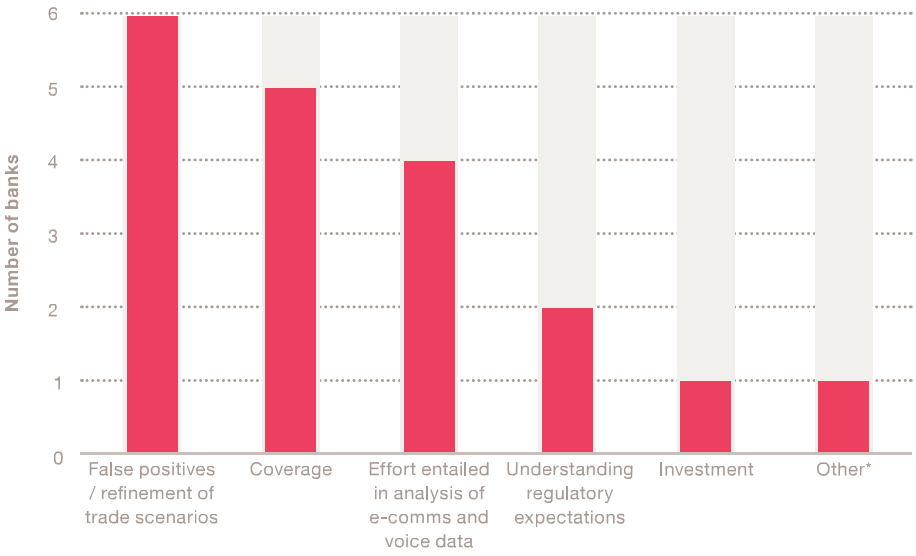
Banks are still concerned about the regulatory direction of travel and the impacts that this may have on additional requirements for surveillance. Specific concerns they raise include the EU market abuse regulations and possible extensions of the scope of surveillance required across both asset classes and trading processes.

As well as future uncertainty, it is clear today that technology is not yet working as well as banks need it to. The survey found widespread dissatisfaction with error rates and the high cost of reviewing inaccurate alerts from automated monitoring of both electronic messages and trade patterns. In particular, more than 65% of tier 1 firms believe that the number of false positives (electronic messages or events incorrectly flagged as high risk) currently generated by trade surveillance systems is unacceptably high.

What is the planned indicative investment spend on surveillance in the next 12 months?



Which of the following are the biggest surveillance challenges faced by your organisation?

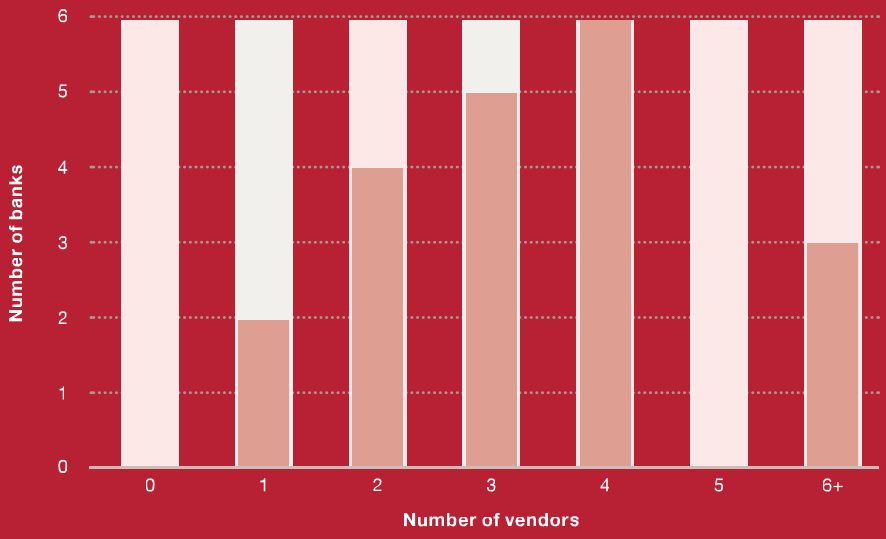


* 'Other' was selected by one respondent, who specified "Quality of data"

It is clear that one solution really does not fit all. 70% of respondents are using three or more vendors to execute their surveillance requirements. Each vendors approach is slightly different and banks are having to cast a wide net to gain some comfort. There is still a lack of convergence in this market – something wanted by the users of surveillance, but not necessarily being fully addressed by the vendor market.

Banks are steadily expanding the teams tasked with reviewing thousands of flagged messages every day. Teams listening to 'phone calls' are also growing, as automated phonetic and transcription voice technologies are increasingly being looked at but are not yet seen as a proven substitute for manual review. And while spending is expected to rise as teams expand further, the criticality of getting surveillance right means banks are largely reluctant to explore outsourcing or other cost saving initiatives. Only 15% of those surveyed have outsourced second line of defence surveillance activities, and only 24% have considered doing so.

How many technology vendor organisations do you use across surveillance?



80%

of respondents expect the cost of e-communications surveillance to increase or significantly increase in the next 12 months

10%

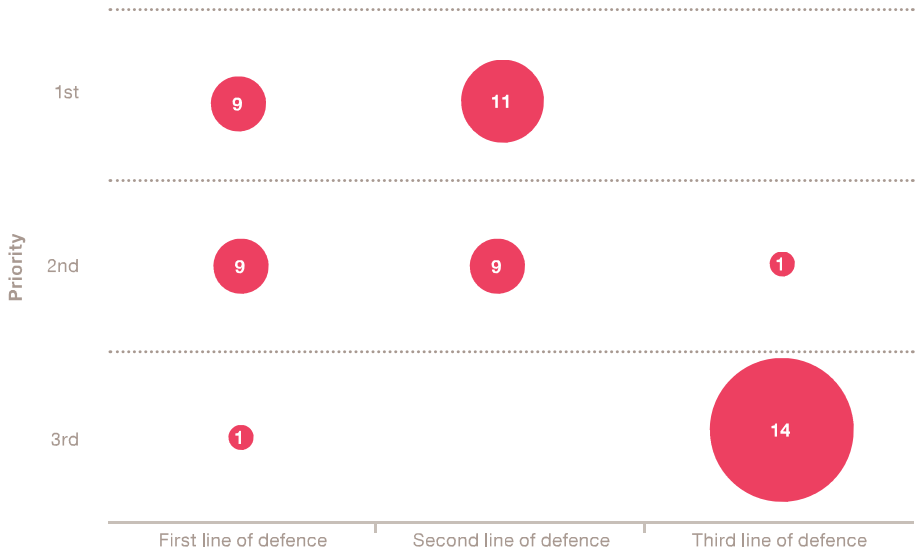
of respondents run automated key word search over voice calls on desk phones

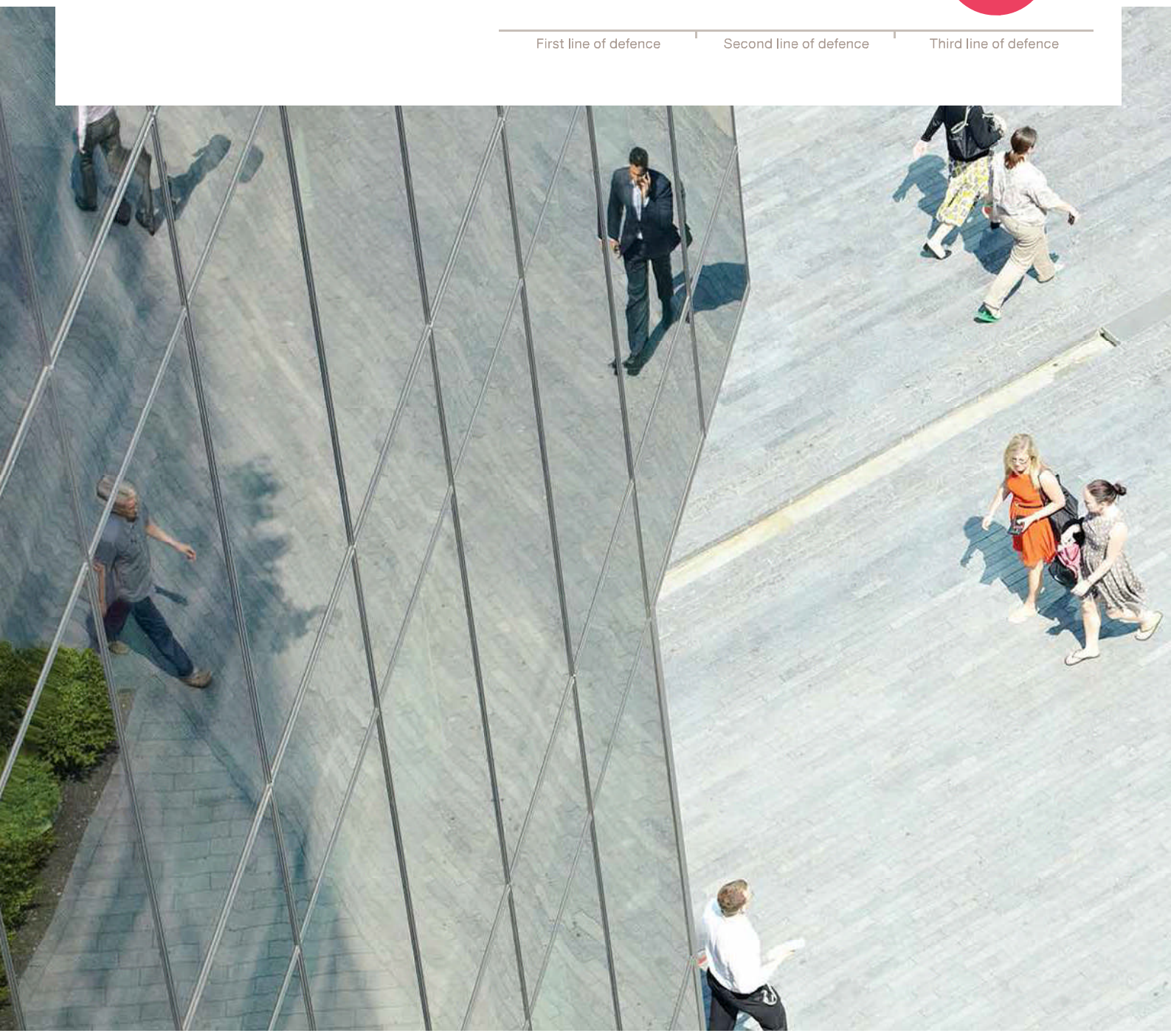
5%

perform automated searches of voice calls on cell phones

Deciding where surveillance activities are performed and by whom is still a work in progress for most. Some larger banks are handing greater responsibility to front office teams, but others are still working out where responsibilities should lie between the first and second lines of defence (Compliance).

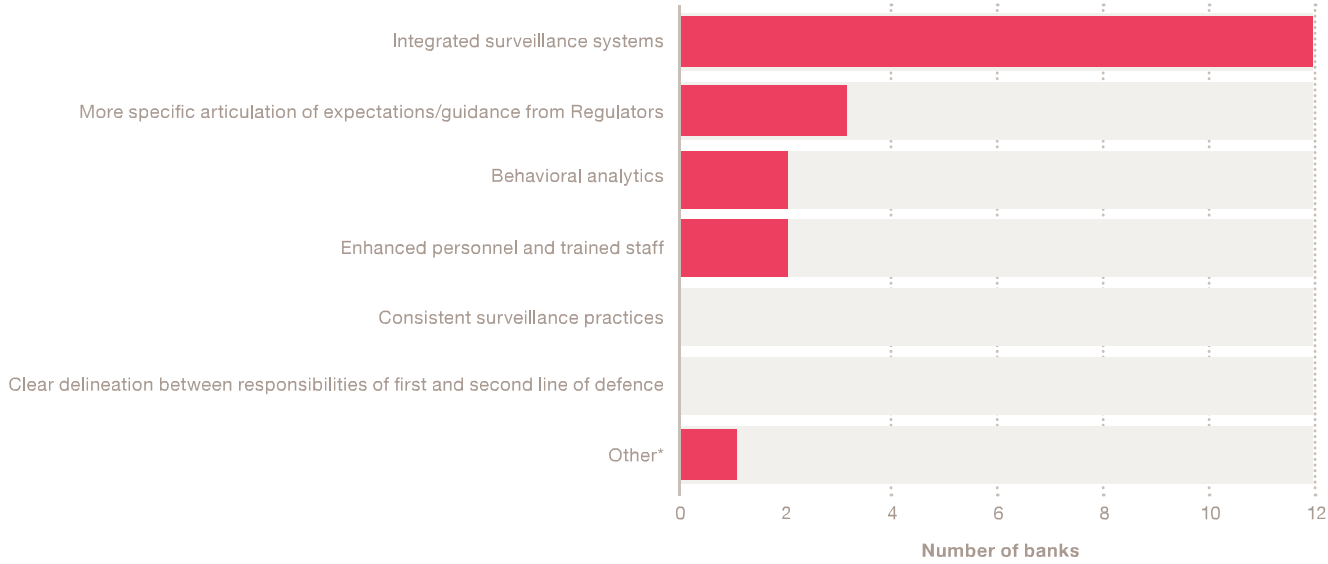
Which operations do you consider surveillance to be part of, in order of priority?



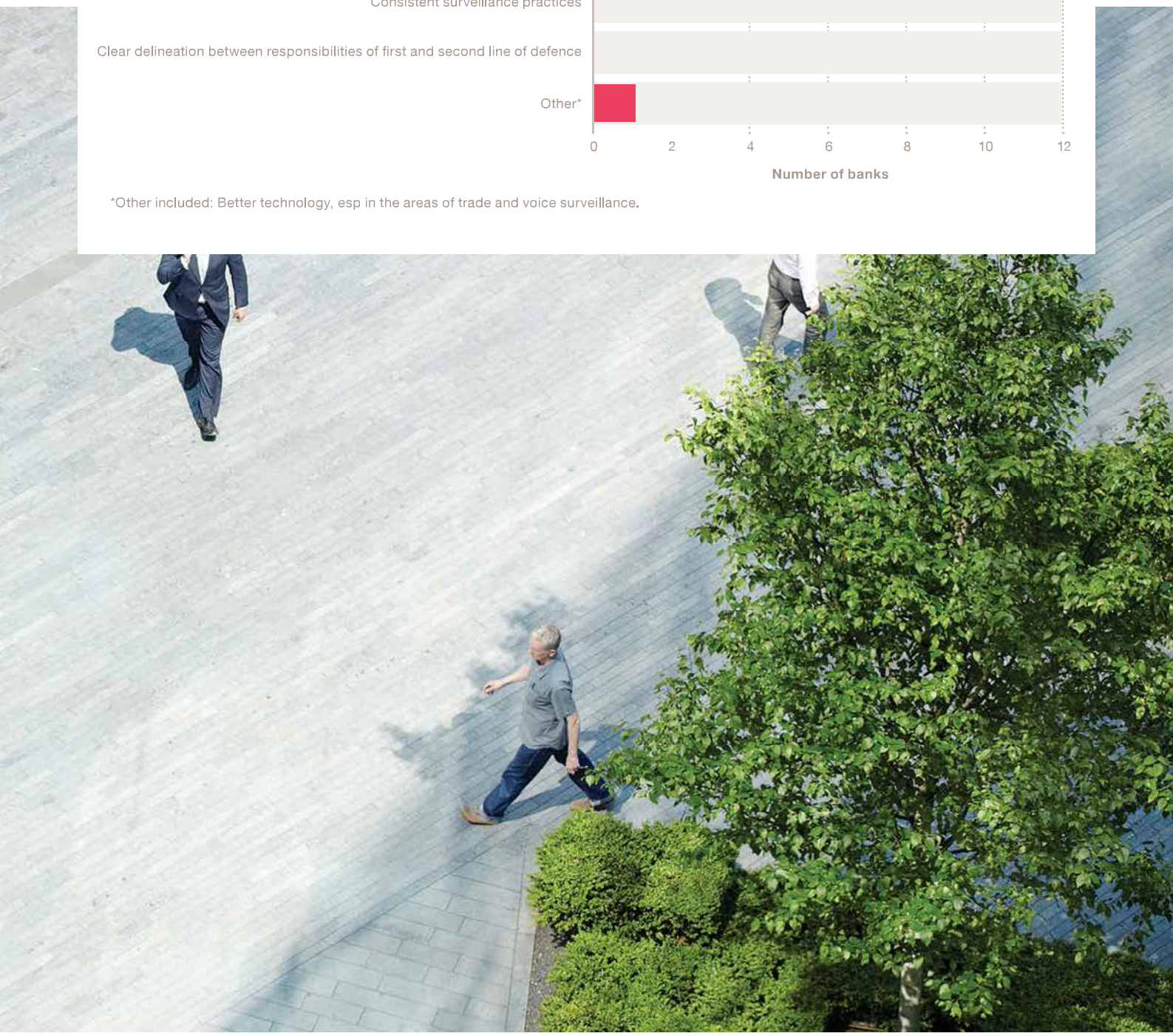


Which option would enhance your surveillance function the most?

While current surveillance technology has clear shortcomings, banks appear hopeful that a newer breed will rise to the challenge. More than half of the firms in the survey indicate their intention to develop more integrated capabilities from the data they collect and believe achieving this will make the greatest impact in enhancing the capabilities of the surveillance function. Achieving those capabilities will depend heavily on the use of technologies, such as big data and advanced analytics. Accordingly, banks in the survey will invest an estimated total of £156m on top of current spend to improve surveillance over the next 18 months.



*Other included: Better technology, esp in the areas of trade and voice surveillance.



Key questions

The survey highlights that banks are taking surveillance very seriously, and backing that commitment with extra investment and larger dedicated teams. But a number of fundamental questions remain.

Are banks truly on top of trader chatter?

Many banks use lexicons – libraries of the key words and phrases that may indicate suspicious behaviour – to support their surveillance of the millions of messages they generate each day.

But are lexicons dynamic and agile enough to capture the increasingly subtle and obfuscated language that traders use? Historic investigations across the financial services sector have highlighted how criminally-minded traders use code words and creative slang to disguise abusive behaviour.

Will natural language processing techniques or new advances in voice analytics provide a better result, or will the growing sophistication of wrong doers mean they continue to elude detection?

Is surveillance technology really delivering?

Over the past 18-24 months, we have seen a number of new entrants to the surveillance market, providing a genuine alternative to traditional vendors. These new surveillance vendors seek to address aspects of the "big data" conundrum, tackling the challenges of analysing large volumes of data structured in myriad forms quickly enough to prevent potential abuses occurring.

While the innovation driving vendors to bring new ideas and approaches to surveillance is welcome, is there a danger that the proliferation of choice and analytical advancements is causing more confusion rather than clarity? And even with advances in analytics is the quality of surveillance relevant data in the banks good enough to support their effective use."

Surveillance –primarily a first-line activity?

The Front Office has always been accountable for running its business responsibly the Front Office assumes accountability, acting as the first line of defence for the institution and stopping potential issues at source.

However, historically, it is Compliance in the second line of defence that has held responsibility for surveillance. But why should this be the case when it is employees in the Front Office that are most likely to lose out? Does it not make more sense to place surveillance in the first line of defence?

It seems evident that those running the business (and who may be personally liable if things go wrong) should have control over surveillance, providing the information needed to take the right decisions at the right time. The regulatory direction of travel suggests this shift needs to happen. But are institutions on board? Do Front Office and Compliance agree on this? And, how will Compliance's role transform to ensure the business is still policed?

Our approach to risk and regulation

Stand out for the right reasons.
Financial services risk and regulation is an opportunity.

At PwC, we work with you to redefine the way risk and regulation is seen. Actively embracing change is a powerful way to enhance your reputation, secure long-term growth, sustainable profits and to deliver value to customers. With our help, you won't just navigate around potential problems, you'll also be positioned to get ahead.

we support you in four key areas.

Alert

By alerting you to financial and regulatory risks we help you understand the position you're in and how to comply with regulations. You can then turn risk and regulation to your advantage.

Protect

We help you to prepare for issues such as technical difficulties, operational failure or cyber attacks. By working with you to develop the systems and processes that protect your business you can become more resilient, reliable and effective.

Adapt

Adapting your business to achieve cultural change is right for your customers and your people. By equipping you with the insights and tools you need, we will help transform your business and turn uncertainty into opportunity.

Repair

Even the best processes or products sometimes fail. We help repair any damage swiftly to build even greater levels of trust and confidence.

Working with PwC brings a clearer understanding of where you are and where you want to be. Together, we can develop transparent and compelling business strategies for customers, regulators, employees and stakeholders. By adding our skills, experience and expertise to yours, your business can stand out for the right reasons.

About the Authors

Graham Ure

Partner
Surveillance data and technology
T: 020 7804 9428
M: 07889 644672
E: graham.ure@uk.pwc.com

Graham leads the UK Forensic Data Analytics practice, providing technology based services focused on the detection and investigation, prevention and remediation of financial crime. He advises clients on financial crime and surveillance, and building upon a firm view of global regulators' expectations in this area has supported financial institutions in developing their surveillance operating models and selecting and implementing monitoring and surveillance technology.

Rukshan Permal

Director
Market abuse
T: 020 7212 6398
M: 07595 611533
E: rukshan.permal@uk.pwc.com

Ruk has significant experience of investigations and remediation programmes at large Financial Services institutions. He has recently conducted a review of a global Investment Bank's FX trading operations, focused on business practices, conduct and controls. Ruk has also led regulatory reviews on how organisations are structured and controlled to mitigate the risk of market abuse or unauthorised trading, often deploying surveillance as a means of control.

Stephen Shelton

Director
Surveillance data and technology
T: 020 7212 4218
M: 07711 562022
E: stephen.b.shelton@uk.pwc.com

Stephen specialises in data analytics and technology for regulatory and compliance purposes in Financial Services, with a particular focus on trade and electronic communications surveillance. He has over 18 years' experience working in the area of data management and analytics of structured and unstructured data and focuses on deli t and value from large volumes of complex data.

Roger Braybrooks

Partner
Front office supervision
T: 020 7804 3473
M: 07740 241086
E: roger.braybrooks@uk.pwc.com

Roger has over 15 years' industry experience covering front-to-back markets operations, risk and controls. He has substantial experience of front-to-back processes, based on work at several leading banks. Most recently, he provided delivery oversight for a review of the processes, controls, business practices and conduct across the FX business (Front Office) of a global Investment Bank.

www.pwc.co.uk

PwC helps organisations and individuals create the value they're looking for. We're a network of firms in 157 countries with more than 195,000 people who are committed to delivering quality in assurance, tax and advisory services. Find out more and tell us what matters to you by visiting us at www.pwc.com.

Design Services 30075 (02/16).