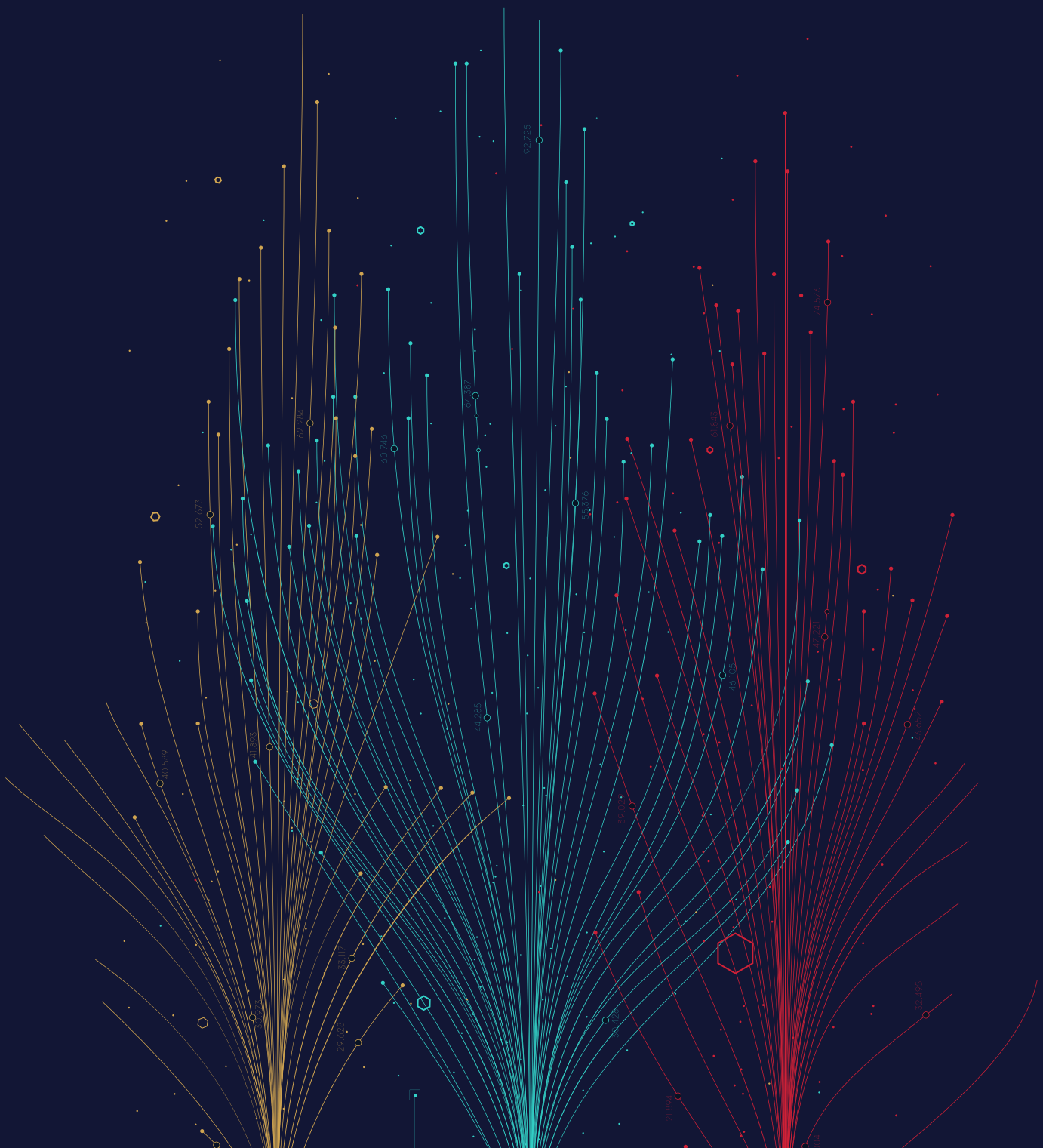
smarsh®

1LoD®

RISK DATA ACROSS THE 3 LINES OF DEFENCE



Firms are focused on addressing the quality of risk data through accountability, transparency and control, while also confronting an expanded set of interconnected risks and heightened supervisory and public expectations. Establishing data ownership and accountability in the 1LOD is a key first step.

Risk Data: Delivering a true data culture

Executive summary

- Banks will need upgraded analytics, new data and updated enterprise data strategies in order to manage existing risks more effectively and incorporate new risks into their programmes
- Data strategies must be better aligned with the 1LOD so that the primary creators and capturers of data are more accountable
- Definitions of 'independence' in the 2LOD and 3LOD must be re-examined to avoid unnecessary data duplication
- Data ownership is still unclear in 81% of organisations
- More than half of the institutions surveyed did not actively promote a 'single view of risk' across the organisation in terms of data
- 76% of delegates say their institutions have active programmes to improve data risk literacy
- Use of AI and real-time data visualisation is still a work in progress
- Chief data officers are assuming much of the responsibility for putting in place data culture, and for creating and implementing standardised data management principles
- 83% of delegates say their organisations encourage a data-driven culture

The coming data challenge

Banks have spent billions of dollars on improving the quality and collection of information used to manage specific risks in recent years. The constantly evolving market and regulatory environment has made this task much more difficult, particularly given the requirement for consent orders. Consequently, banks have fundamental questions about maintaining their existing data and building a next-generation data platform that will still be fit for use in the future.

Among these: how can they develop a data culture that is seen as mission critical and that adds value? Just as the business side has had to accept responsibility for conduct and other standards, how can banks persuade the business side to be responsible for the data it creates? How can organisations ensure that data flows are transparent without launching a massive and expensive effort to track data across legacy systems? And how can they monitor and report on data quality so that they can focus on improving those areas that are most critical to the enterprise?

To answer these questions and move ahead, banks have to look at the data and capabilities needed to manage both the traditional market abuse and conduct risks, and also new types of risks - for example, operational resilience, cyber or ESG risks. This means having the ability to analyse existing data in new ways to inform detection of these new risks. It also means gathering new data and adding it to the existing datasets and analytics to manage these new risks.

Data ownership is clear in my organisation?

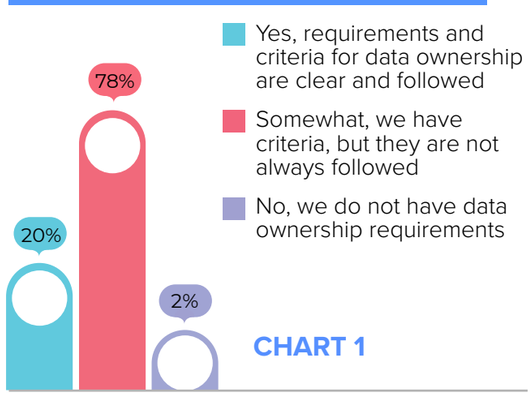


CHART 1

Who owns data and data strategy?

These challenges are forcing banks to look again at the issue of who owns enterprise data and data strategy. Participants in the Deep Dive reported a trend for making the enterprise data strategy align more with the 1LOD so that the primary creators and capturers of data are more accountable.

As one participant put it: "A big part of the problem is that everybody thinks they own the data, from the business all the way to IT. But the 1st line really needs to take over, as it has in cyber. Ultimately, it's the 1st line that creates the risk and so the 1st line needs to own and manage that data - and we also need to make sure that they don't just own the data, but also the technology architecture that supports it."

This in turn is prompting a rethink about data administration. One speaker explained what this means for their institution: "Every time I ask for a new attribute or a new file, I also have to evaluate whether that data is key or not key. I have to define control requirements along with my sourcing requirements; I have to capture and register metadata; I have to update data tracing as part of my normal change process. And all of this gets tested, just as we would do normal user-acceptance testing."

This requires new tools, new data skills and, potentially, changes in the skill sets required by the risk practitioner and auditor of the future.

In practice, a great deal of responsibility for these changes falls on the chief data officers, who are tasked with putting in place data culture and with creating and implementing standardised data management principles. Some attendees likened the process to the evolution of cybersecurity and cyber risk management over the past few years. This began as a retrofit to the organisation but now it is treated as a standalone risk to be owned by the 1LOD.

However, banks are not there yet. Asked whether data ownership is clear in their organisations, only 20% of respondents said yes (see chart 1).

The question of independence

If the 1st line owns the data, how do other risk functions maintain independence in their evaluation and use of data? As one participant put it. “Where does independence start when it comes to data? To retain my independence in the 2nd and 3rd lines, do I have to source my data completely independently?”

Most banks say ‘no’ in response to this question. Instead, the key is to develop a golden source upon which everyone can agree - and which different parts of the institution cannot change after its creation and capture.

“The best model is one central source of data that everyone can agree on. So, you get rid of the disagreements on data and then everyone can source what they need for their particular users, but you should have one golden source,” said one speaker. “So, for example, whether you have 1st line surveillance or 2nd line surveillance, they should all be consuming the same data. There’s no reason for it to be sourced from different places depending on who is sourcing it.”

Some attendees felt that there is still regulatory ambiguity in this area - that regulatory demands for 2nd and 3rd line independence implies a differentiation in the data sources they use. Others disagreed and said that the intent of the regulations did not preclude single golden sources. However, everyone agreed that it will take several years to achieve this.

At one bank, Internal Audit - traditionally a repository of data literacy, because arguing with other people’s data is a core competence - has set up its own analytics academy to help other risk functions to improve their data skills.

This example of collaboration reflects a general recognition that the silos that exist both in data and across the three lines need to be replaced with partnerships. Asked whether their firm has an established process of collaboration between various users and developers of data analytics, 72% of delegates said either that their data programme was already built around collaboration or that was the direction of travel (see chart 2).

To avoid the creation of silos within the company, one speaker’s bank had established a ‘data council’ for each business unit: these councils roll up into one at the group level. Matters requiring escalation are passed to an executive data council, which is made up of members of the group executive committee - the chief compliance officer, general counsel, chief risk officer, the CEOs from different divisions, as well as the bank’s chief operating officer.

A single view of risk

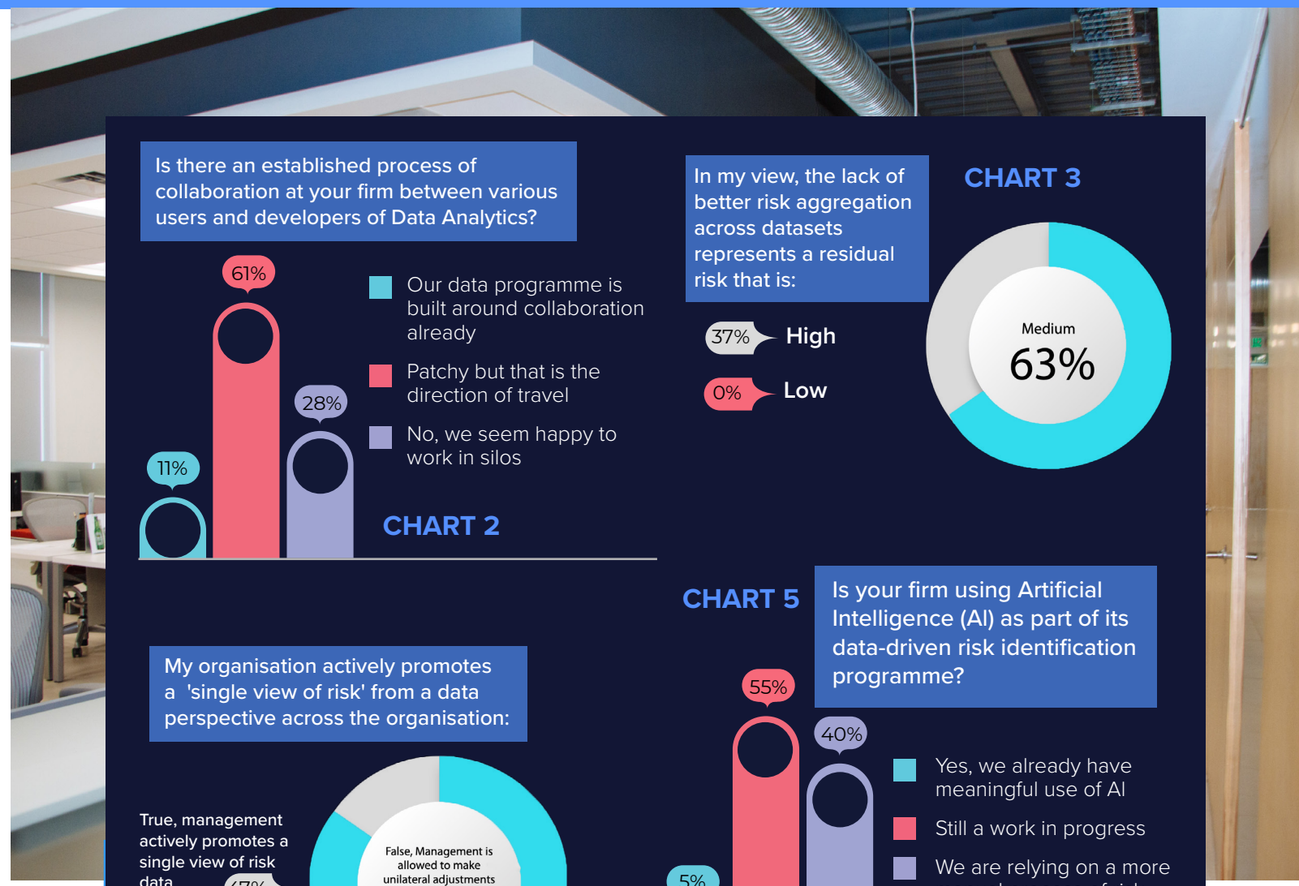
Reforms to data processes tend to start from a risk- management perspective. With a single view across the relevant datasets, banks are better-placed to identify risks, create and monitor controls and attest to the operation and effectiveness of those controls. This perspective can arise from taking a narrow technical view of data, which elevates the ideas of ‘trusted source’ and data consistency because of the need for databases and APIs to function without manual intervention and data normalisation. However, this is typically driven from a 2nd and 3rd line desire to improve regulatory compliance and governance in general, and to generate better metrics.

By not aggregating all of the relevant datasets, banks expose themselves to material risk. They miss individual risks contained in the data. They also miss potentially larger risks if they are unable to ‘connect the dots’ across multiple datasets that could reveal misconduct or outsized risk-taking.

Attendees agreed, although they did not think that the risk posed by data fragmentation was high. Asked what level of risk is posed by the lack of better risk aggregation across datasets, 63% said ‘medium’ (see chart 3).

As one speaker pointed out, “The minute you have fragmented datasets, then you have a lot of downstream adjustments and ultimately poor data quality and operational inefficiency”.

To identify as wide a range of risks as possible, banks need to aggregate across not only the obvious financial datasets, but also records of internal risk events such as audit findings, issues highlighted by 2nd line assurance functions or regulatory inspection findings.



In all these respects, the banks have some way to go. Asked whether their institutions actively promoted a ‘single view of risk’ from a data perspective across the organisation, 53% of attendees said ‘no’ (see chart 4).

There is also a long way to go when it comes to running artificial intelligence (AI) or machine learning (ML) analytics across risk datasets to try to identify risks more accurately. Ideally AI and ML engines would be run on fully aggregated datasets: they also require huge amounts of data to produce accurate output, so data aggregation is a likely precursor to the widespread implementation of these technologies.

Attendees reported fairly limited take-up of AI as part of their data-driven, risk-identification programmes, with just 5% saying they had ‘meaningful use of AI’ and 40% ‘relying on a more manual process of risk identification’ (see chart 5.).

“Deep insightful conversations and solutions offered by practitioners - extremely valuable to every organisation.“

COLIN WAN, CHIEF OPERATING OFFICER, STANDARD CHARTERED BANK

The visualisation shortcut

The problem with data aggregation is the cost and complexity of merging dissimilar datasets across multiple systems with also complying with security and privacy regulations. To avoid this, some insititutions have chosen to visualise the individual datasets and then run analytics across the sum of them (rather than aggregating data and then running analytics across the merged dataset).

To achieve this, firms need sophisticated data visualisation tools, which are still being developed. Asked ‘Is your firm using any real-time data visualisation tools as part of its data-driven risk identification programme?’, 59% of respondents answered that it was ‘still a work in progress’ (see chart 6).

Cloud considerations

Aside from visualisation across multiple datasets, the most obvious shortcut to large-scale data aggregation is the Cloud. Attendees felt that there are three core considerations with regard to moving to the Cloud. The first is cost: given the vast amounts of data that financial institution have to gather, store and analyse, the economics of Cloud storage and cloud applications are compelling.

The second is regulation: moving to the Cloud will be constrained by regulatory pronouncements on data usage, privacy and accessibility. Banks are still grappling with complex decisions concerning the operation of a multi-jurisdictional Cloud programme and the mix of public, private and hybrid Cloud. But recent large tie-ups between banks and infrastructure giants show that previous reservations are being overcome.

The third consideration is cybersecurity. All companies, not just in financial services, will need to decide whether they can secure their data better on the premises or by using third-party providers.

The overwhelming view of attendees was that to escape the insuperable problems of legacy technology, banks will have little choice but to move to the Cloud in the next two to three years. And most are already heading that way. Asked about the level of maturity of their firms in leveraging cloud-based technology for more efficient data management, 49% replied "medium" (see chart 7).

CHART 6

Is your firm using any real-time data visualisation tools as part of its data-driven risk Identification programme?

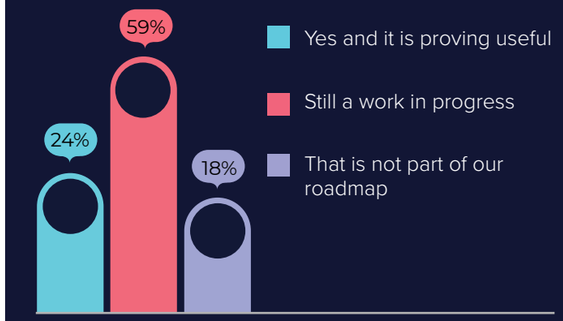


CHART 7

In my view, the level of maturity of my firm in leveraging cloud-based technology for more efficient data management is:

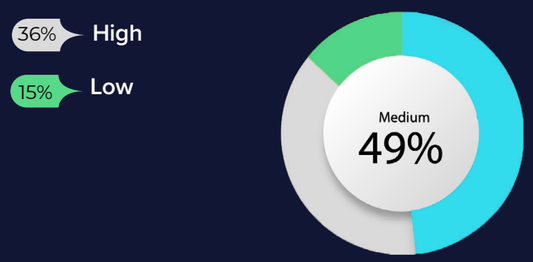
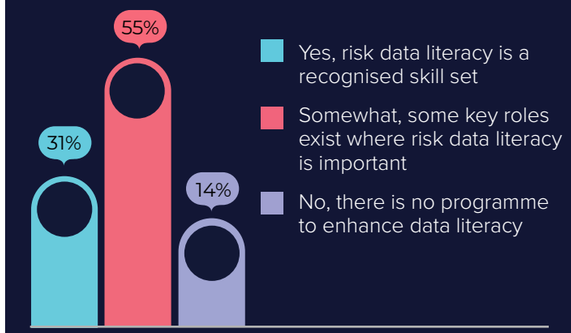


CHART 8

Does your organisation recongnise the importance of risk data literacy?



Data literacy

The increase in responsibility and accountability for data across the three lines will change the skill sets required. Senior management seems to accept this. When asked ‘Does your organisation recognise the importance of risk data literacy?’ only 14% of attendees said ‘no’ (see chart 8).

And when asked ‘Is your organisation open to improving data literacy and data skill sets across the 3 lines, 76% of attendees said ‘yes’ and that there were positive incentives driving that improvement (see chart 9).

Organisations are already investing in the necessary improvements to skills, with 72% of delegates reporting that their institutions had active programmes in place to improve data risk literacy or that there was training in development (see chart 10).

CHART 9

Is your organisation open to improving data literacy and data skill sets across the 3 lines?

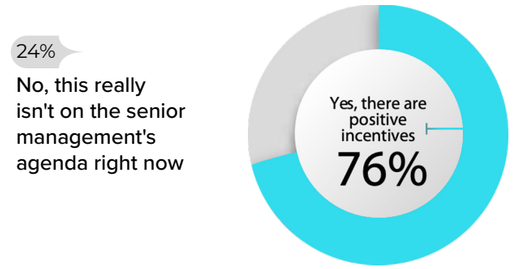
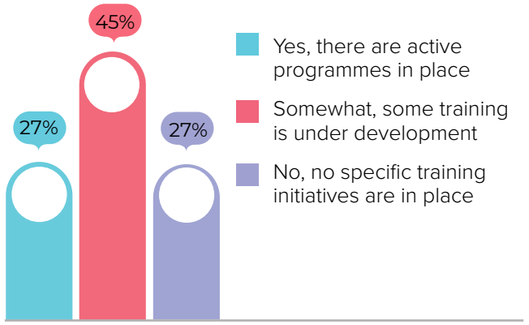


CHART 10

Does your organisation sponsor and provide practical approaches to improve risk data literacy, especially in high visibility risk data areas such as ESG?



Creating a data culture

Speakers agreed that one of the main goals is to create a data-driven culture across the entire organisation. How can banks 'democratise the use of data'? To what extent is broader data literacy the key to such a culture? And how can they create accountability for that?

As one speaker said, "The answer is that the culture starts with the policies, standards, expectations and accountabilities. And, again, accountability resides with the 1st line to adhere to the policies and standards that have been put in place. More generally though, data needs to be part of our DNA."

Here there is room for optimism. Asked whether their organisations encourage a data-driven culture 83% of delegates said 'yes' (see chart 11).

It was clear that organisations are at different stages of maturity in terms of how to manage and use data as a strategic asset, so it is natural to see a level of inconsistency across the industry. A good data strategy is founded on governance, ownership and delivery responsibilities. How banks build those foundations is still debated, but one speaker gave this advice:

"Don't think small, don't think about those one- or two- use cases. Think about where you'd like to take your organisation. Build an ecosystem - don't short-change the cultural aspects. And build bridges to the business: data teams need to be able to communicate with the business, not simply be the best data scientists out there."

"This was an interesting and unique session, in the sense that you had different people from varied backgrounds and corporates speaking out their views, and giving us a platform to hear them all - which usually we don't see."

KUSHAL TIKMANI, ASSOCIATE, HSBC

CHART 11

My organisation encourages a data-driven culture:

17%

False, there is no particular emphasis on enhanced use of risk data

"A highly recommended event to attend to keep yourself abreast of the latest topics in discussion."

JULIA TAN, ASSURANCE MANAGER, NATWEST MARKETS

"Well organised, topical and relevant."

DAVID TARLING, BUSINESS CONTROL MANAGEMENT, GLOBAL MARKETS HEAD OF RISK IDENTIFICATION, ASSESSMENT & INFRASTRUCTURE, J.P. MORGAN

"Panellists were knowledgeable and thought provoking. Use of polling was good to get consensus on where organisations were at. I would be keen to attend again."

ROBIN HAYES, INFO & TECH RISK SPECIALIST, ANX BANK

This information was taken from the Risk Data Across the 3 Lines of Defence Deep Dive on 29 - 30 June 2021.

For more information on 1LoD please visit: www.1lod.com