Financial Crime Data Survey

2021 EMEIA report

September 2021

Building a better working world

Creating a brighter future for financial services

At EY, we are focused on building a stronger, fairer and more sustainable financial services industry. The strength of our EY teams lies in the proven power of our people and technology and the way they converge to reframe the future. This is how our EY professionals are helping to build long-term value for financial services clients.

ey.com/fs

Contents

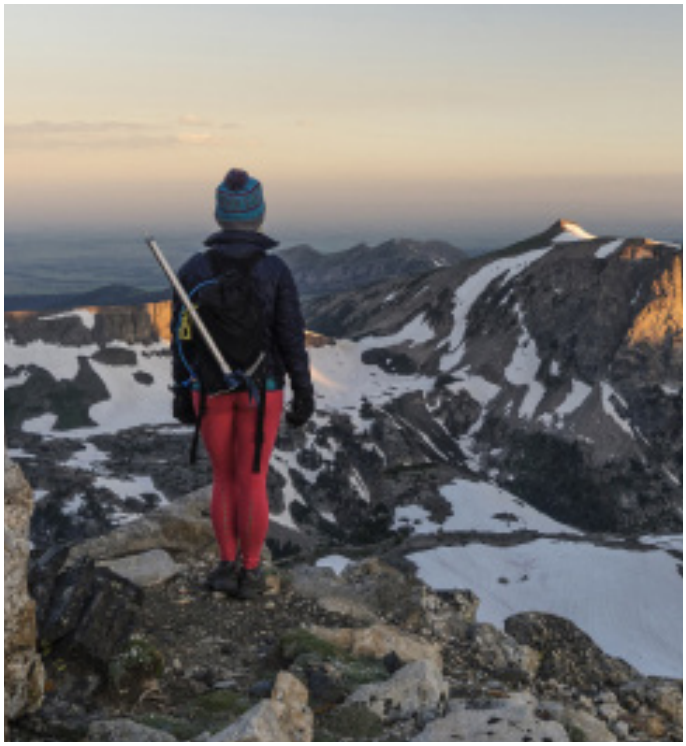
Executive summary

Introduction

While significant quantitative analysis has been produced covering the use of data in many financial services contexts and domains, there is limited analysis covering data within an EMEIA[1] financial crime context.

In response, EY teams conducted an EMEIA-wide Financial Crime Data Survey of financial institutions. The survey focused on the impact of data on systems and processes, data strategy and data investment within a financial crime context.

The survey ran during Q1 2021, and interviews were conducted directly with the participants, capturing comments and discussion topics.



Scope

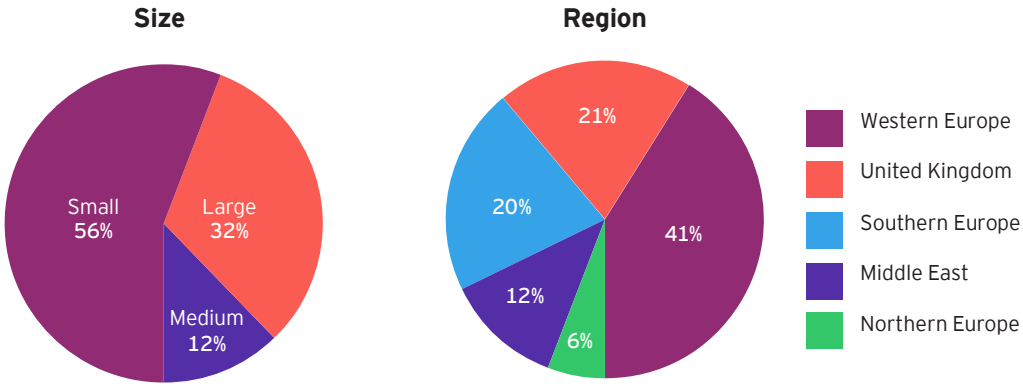
- The Financial Crime Data Survey provides a view of current and future EMEIA data-related solutions.
- The survey covers financial crime data management topics such as systems, investments and strategy.
- The survey brings together insights from compliance, technology, data and analytics professionals across EMEIA financial institutions.

[1]EMEIA - Europe, the Middle East, India and Africa

Figure 1: Survey participants by size and region

34
participating financial institutions

Q1
2021



Large financial institutions, defined as institutions with total assets above US$250 billion, medium-sized financial institutions are defined as institutions with total assets of US$90–$250 billion and small financial institutions defined as institutions with total assets below US$90 billion.

Financial crime is generally defined as any activity that involves fraudulent or criminal behavior for the purposes of personal financial gain. It involves a spectrum of criminal activities and may be committed by individuals or groups that are involved in activities such as: money laundering, terrorism financing, fraud, tax evasion and identity theft.

Key themes

Four themes emerged from the Financial Crime Data Survey:

Data quality and data governance are the key concerns for financial institutions
The most frequent challenges according to respondents stemmed from technology (such as lack of data standardization, accessibility, sourcing and data structures). Highly cited root causes included fragmented systems, operational silos, legacy technology, poor data capture controls and lack of sponsorship or senior leadership buy-in.

Despite increased investment in data management technologies, satisfaction with data management capabilities is still low
Despite the increased investment and greater focus on new technology partnerships to improve the effectiveness and the efficiency of data operations, overall satisfaction with data initiatives is low. Respondents cited the need for cost-effective, sustainable (and scalable) solutions for financial crime risk detection and investigation. There was a demand to better use, innovative technology (such as workflow, analytics and process automation) to improve and accelerate risk detection and remediation.

Delay in addressing data challenges is impacting the effectiveness of financial crime controls and limiting the delivery of business benefits
Financial crime has been a hub for data innovation as financial institutions have more freedom in how they can use customer data for the purposes of detecting and preventing criminal activity. Most institutions feel there is a potential to derive increased business benefit from data innovation. More needs to be done to leverage the full potential of data across all financial crime domains to demonstrate business benefits at speed. Respondents cited the need to elevate senior leadership buy-in to help drive improvements in data management capabilities.

Financial crime teams struggle to benefit from enterprise data initiatives
Enterprise level data initiatives, such as cloud migration or innovations in data operating models, are not high on the priority list for financial crime teams, which could be because financial institutions are still operating in a broadly reactive manner.

The way forward

Reliable and accurate data is central to a successful anti-financial crime program. Financial service firms today face the challenge of dealing with ever-higher data volumes, while coping with legacy systems, a lack of sophisticated controls and often low levels of leadership buy-in.
There are three key aspects for a successful financial crime data program:

1. Strong data foundations
Assigning a data leader who can be entrusted with enterprise-wide data responsibilities and overall data strategy is a vital step in ensuring a well-run and scoped data-backed anti-financial crime program, regardless of the size of the organization. The data leader will ensure data is seen as central across the business and aligned to business goals.

2. Ecosystem and enterprise
Data ecosystems need to respond to technology innovations and regulatory changes, often leveraging data partnerships and external data providers. FinTechs and RegTechs will also play an important role, and institutions will need to embrace this disruption to gain value and improved financial crime prevention.

3. Capability and value creation
A visionary data leader will foster innovation and continually improve data management capabilities through data and analytics to boost information sharing, collaboration, compliance and security. The enablement of technologies such as artificial intelligence will help in handling the vast volume and variety of data created by a myriad of technologies, to improve data management capabilities.

There are opportunities to reduce operational cost but also, more significantly, identify intelligence-led and data-driven ways to tackle financial crime.

Overview of participants

EY teams conducted a targeted survey of data management challenges and their impact on financial crime processes and systems, across a range of financial institutions. This section contains an overview of the survey's participants to provide a background for the analysis and findings presented in the next section.

Geographic coverage

The participants were 34 financial institutions from Europe. The most common region of primary operation was Western Europe (41% of the participants). Other financial institutions were from the UK (21%) and Southern Europe (21%) , with the remaining from the Middle East and Northern Europe.

Figure 2: Region of primary operation

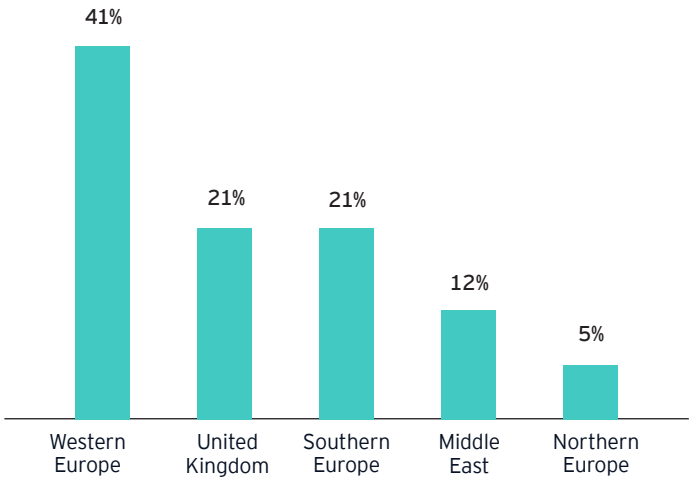
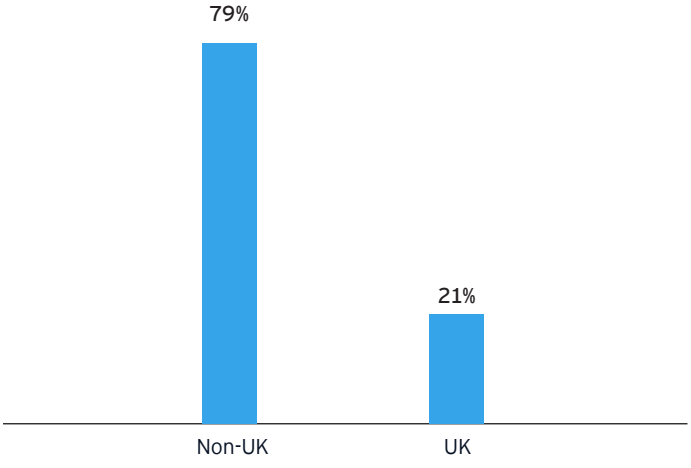


Figure 3: UK vs non-UK primary operations

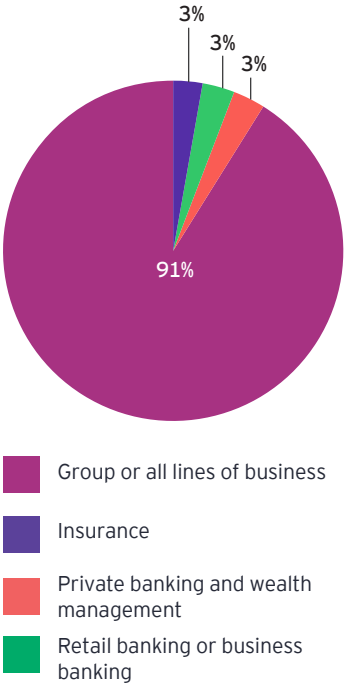


[1] Countries per region: Western Europe (Austria, France, Switzerland), Southern Europe (Italy, Malta, Spain), Northern Europe (Sweden), Middle East (Kuwait, Oman, Qatar)

Sector

The distribution of participants represents a good mix across financial services sectors, with 91% indicating that they are involved in all lines of business. However, asset management and markets were not present in the distribution.

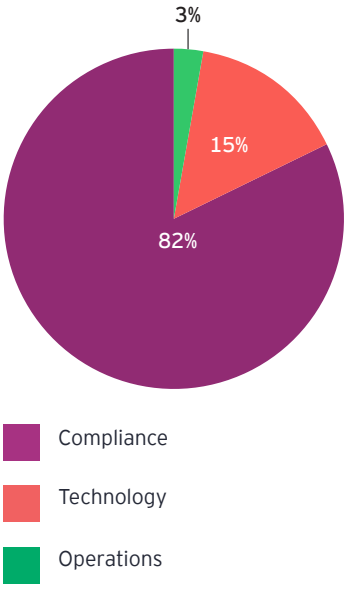
Figure 4: Distribution by sector



Primary role

Most participants identified themselves as compliance leaders, but in many cases they were supported by technology and analytics representatives within the business function.

Figure 5: Primary role of survey participants



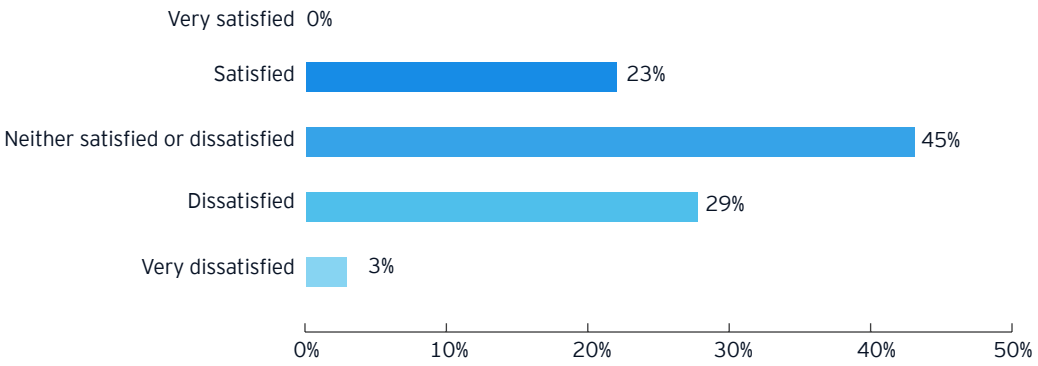
Detailed analysis: systems

Data quality and data governance are key concerns for financial institutions

1.1 Overall satisfaction of data capabilities

It is worrying that nearly a third (32%) of respondents were dissatisfied or very dissatisfied with their data capabilities. With only a quarter (23%) satisfied, it is clear there is much to improve in financial institutions' data capabilities.
The key reasons given for dissatisfaction were fragmentation and lack of clarity in data governance, quality and lineage, as well as issues with data sourcing and accessibility. Some respondents also stated that there is a lack of investment in this area and greater need for automation of controls and processes.

Figure 6: How satisfied are you with the overall effectiveness of your data capabilities?



Top five themes for dissatisfaction

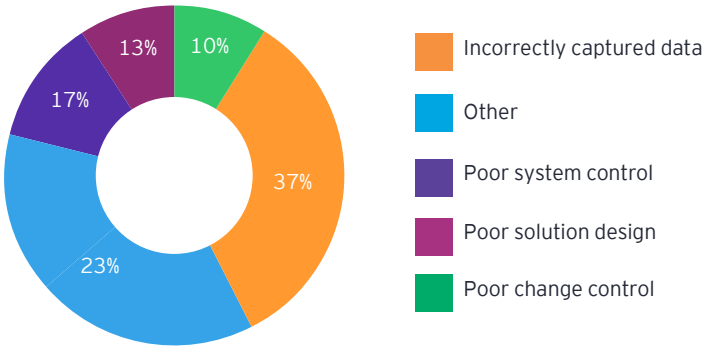
- Improvement needed in data governance, quality and lineage
- Fragmented data framework and reconciliation issues due to complex legacy systems
- Data sourcing and accessibility
- Greater need for automation of controls and processes
- Lack of investment in data capabilities

1.2 Primary root cause of data issues

The responses here underlined the clear message throughout the survey that data quality, controls and governance are the key concerns impacting financial institutions.

Incorrectly captured data was the biggest root cause of data issues. This reflects the journey left for many firms to improve the quality of their base data.

Figure 7: What are the primary root causes of data issues affecting financial crime systems, processes and controls?



Themes from participants that selected 'Other'

- Lack of data management prioritization
- Insufficient management of legacy systems resulting in duplication of processes, high costs and lack of data control
- Internal knowledge gaps
- Unsatisfactory data (e.g., not structured or formatted, poor quality from data providers)

Lack of funding is a key challenge in tackling data management issues

1.3 Key challenges in tackling data management issues

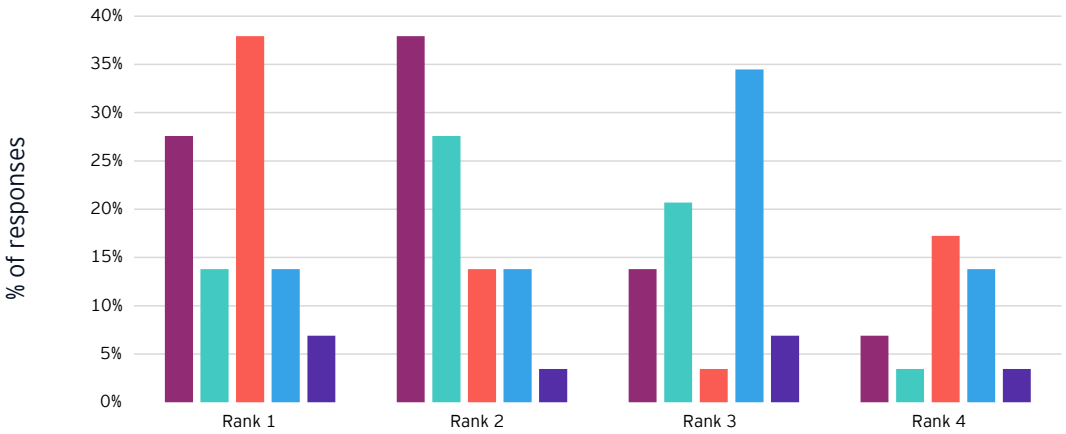
It is important to note that the three biggest challenges flagged around improving data management at the enterprise level – insufficient funding, poor data management and ineffective controls – are often interlinked. This means a well-thought-out and coordinated strategy will be needed to overcome these barriers.

Other notable challenges included:

- Data culture – shifting the mindset of organizations and sponsors when it comes to data initiatives
- Knowledge and skills gap, which is linked to insufficient funding for data-related learning and development
- Siloed data modeling across the organization

Figure 8: What are the key challenges in improving data management at the enterprise level?

(1 = most applicable, 4 = least applicable)



Ineffective management of data

e.g., governance model not robust (unclear ownership of data, weak or unenforced policies); data quality management driven primarily by regulatory compliance needs

Lack of capability

e.g., lack of data management expertise, inefficient data architecture, manual effort required for reconciliation and remediation of data quality issues

Insufficient funding

Not to the level required for enterprise-level data quality and management programs; lack of business buy-in for value of data quality management

Ineffective controls

e.g., poor quality of data entry at system of origin with no or limited validation, multiple data warehouses or disparate systems with no common data model

Other

Any other challenges

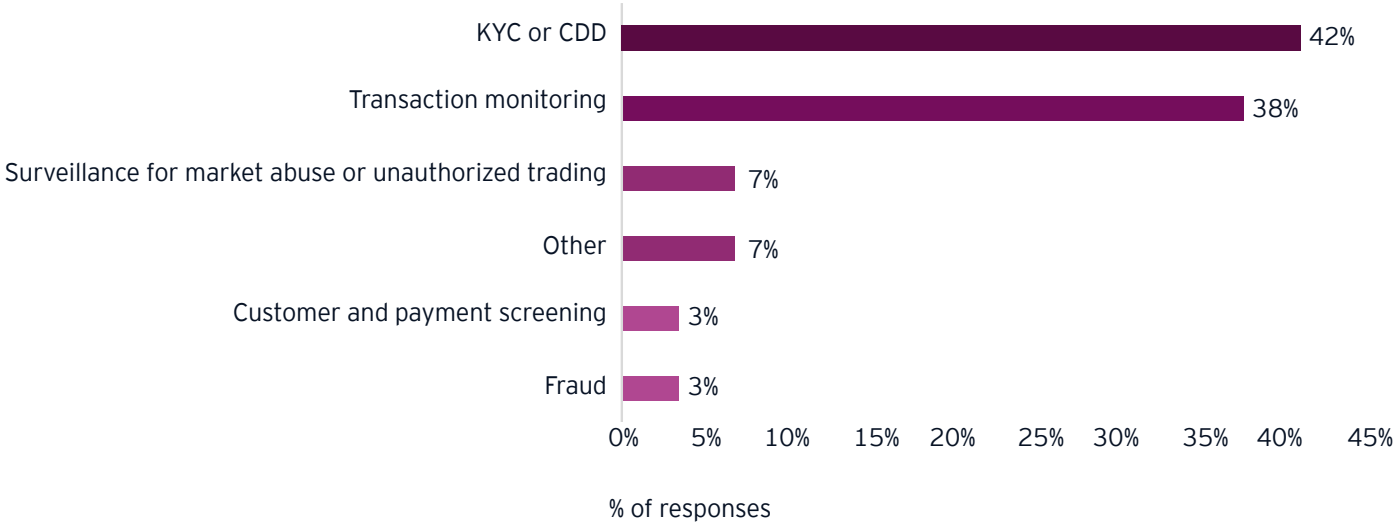
Complacency in actioning these data issues is impacting the effectiveness of financial crime controls

1.4 Impact of data issues on financial crime domains

While all financial crime domains are impacted by data issues, there was clear sentiment that the key areas impacted were Know Your Customer (KYC) or Customer Due Diligence (CDD) and transaction monitoring. This may reflect the high reputational and regulatory scrutiny in those areas. It underlines that poor quality data is a clear impediment to the effectiveness of financial crime controls, seriously impacting the usefulness of detection and decisioning.

The majority of participants also felt financial crime domains are equally interlinked and therefore all suffer from data issues.

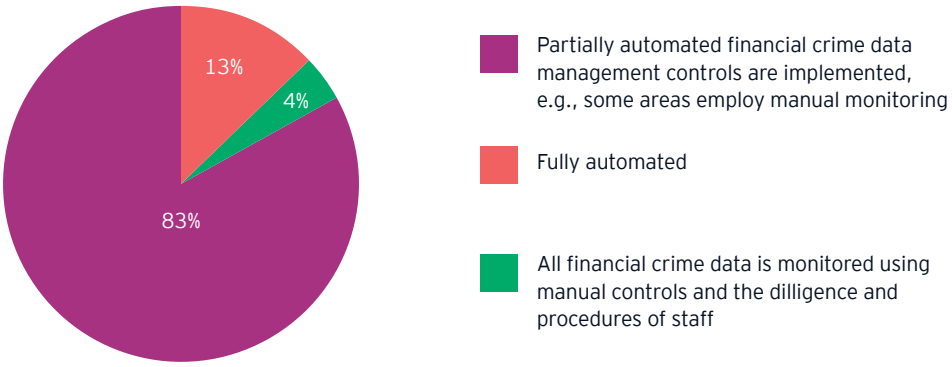
Figure 9: Which of the following financial crime domains is most negatively impacted by data issues?



1.5 Level of automation of data controls

The low levels of automation likely reflect the foundations are not in place for most firms to apply such technology at the present time. The issues flagged, such as poor automation of data quality or a lack of integration, are fundamental issues that need to be resolved before firms can move to full automation, and the efficiencies and cost reductions that brings.

Figure 10: How automated are the financial crime data management controls within your systems?



Partially automated due to:

- Poor automation of data quality monitoring
- Lack of integration or data reconciliation controls between different data sources
- Lack of data availability in required format; some manual work required
- Cloud adoption underway to improve automation
- Legacy system complexities

Although systems are largely able to handle data volumes for financial crime processes, the majority have cited limitations and challenges

1.6 Data processing and volumes

The majority of participants indicated that their systems are able to handle the volumes of data required for financial crime processes and controls without adverse business impact.

EY teams dissected this further to compare the responses from large or medium-sized vs. small financial institutions, shown on the next page.

Figure 11: To what extent are your systems able to handle the volumes of data required for financial crime processes and controls without adverse business impact?

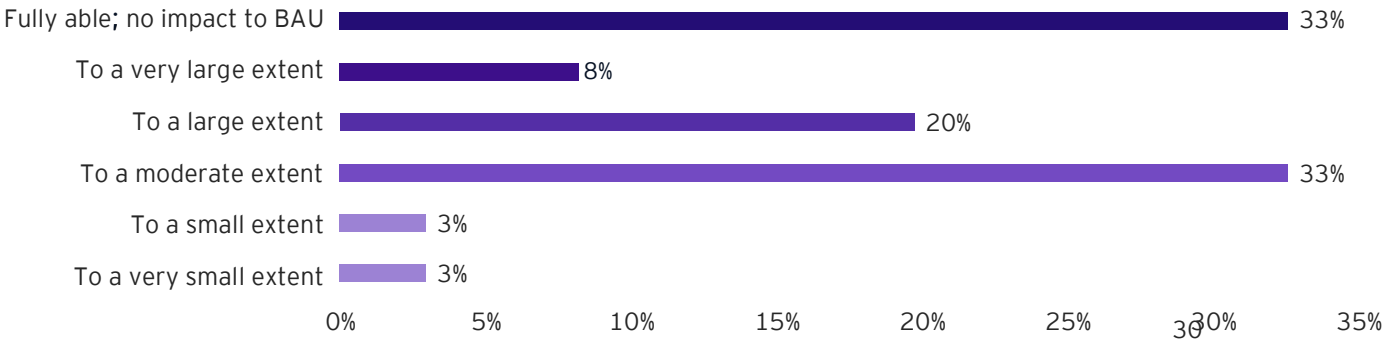
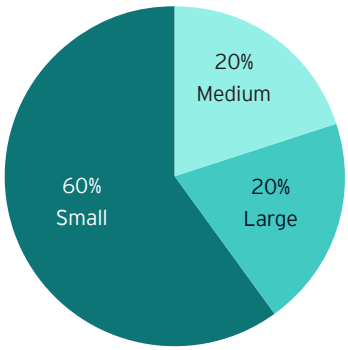


Figure 11a: Data processing and challenges comparison by large or medium-sized vs. small financial institutions

33% of participants deem their systems fully able to handle large data volumes



Characteristics

Large or medium-sized:

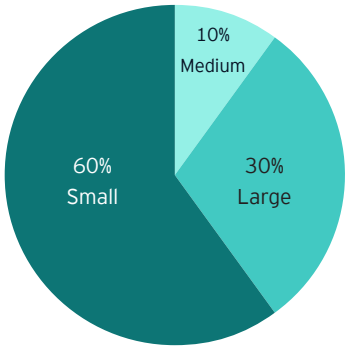
- Sufficient operational capacity to meet increased volumes
- Investment in big data to centralized systems

Small:

- Data processing is quick and robust
- Recently started fully automating which will lead to higher volumes

---

33% of participants consider their systems able to handle the volumes to a moderate extent



Characteristics

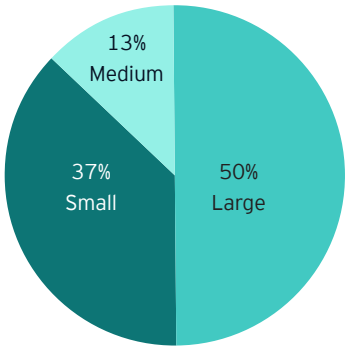
Large or medium-sized:

- Legacy systems
- System limitations, i.e., spikes in data volume causing processing issues

Small:

- Fragmented systems, resulting in processing and data provisioning challenges
- System limitations
- Training lack of knowledge

27% of participants consider their systems able to handle the volumes to a very large or large extent



Characteristics

Large or medium-sized:

- Legacy systems and scalability
- Systems limitations, i.e., not able to process real time or data types

Small:

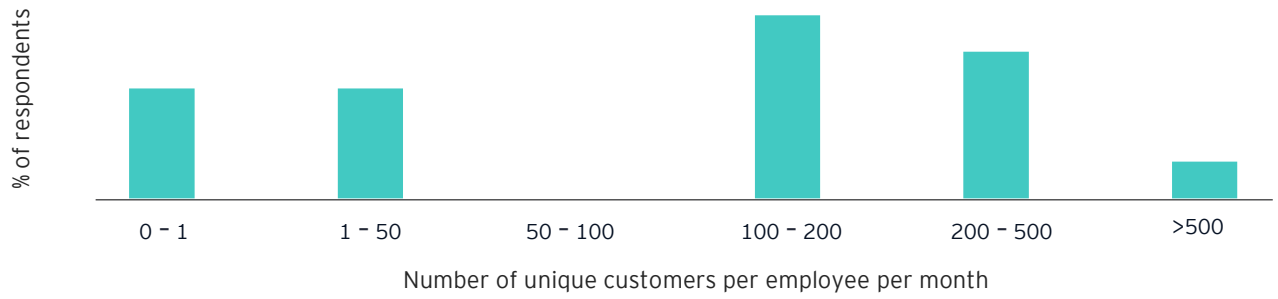
- Historical data and reconciliation with third-party data
- Architectural challenges when data changes

Data processing volumes vary across financial institutions, although there are minor skews in numbers of customers and transaction processes, as well as employees working on data initiatives

1.7 Customer data processing and volumes

29% of participants have between 100 and 200 unique customers processed by financial crime systems per month per employee. The range varies significantly, with the lowest being 0.04 transactions and the largest 707.41.

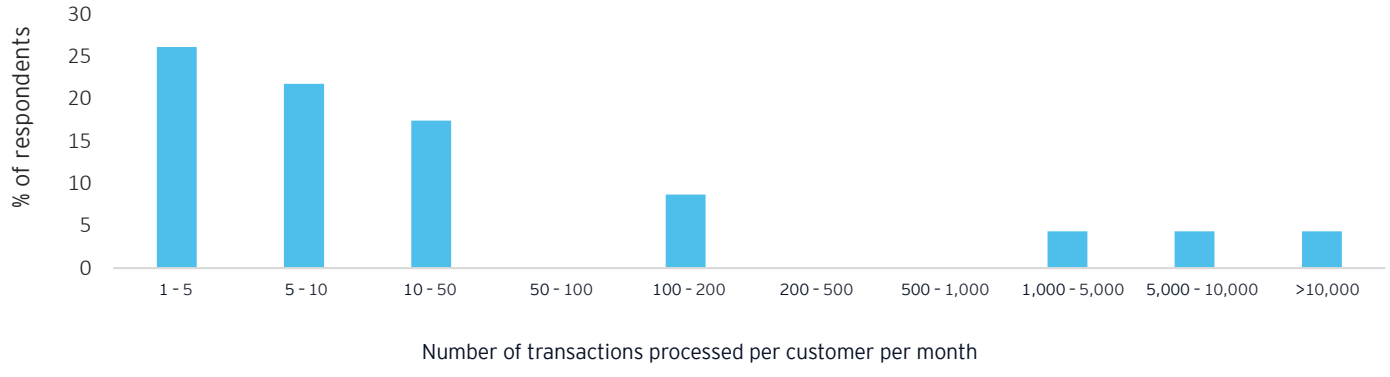
Figure 12: Number of unique customers processed by financial crime systems per employee per month



1.8 Transaction data processing and volumes

Seventy-seven percent of the participants process between 1 and 50 transactions per customer per month. However, this range varies significantly across the population, with the lowest number of transactions per customer per month being 0.01 and the largest 10,000.

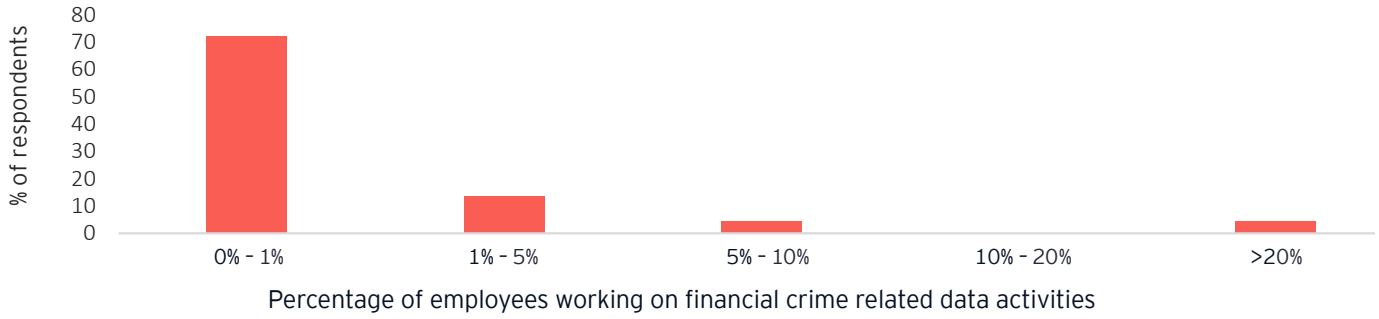
Figure 13: Number of transactions processed by financial crime systems per customer per month



1.9 Employees working on financial crime data

For 45% of participants, the percentage of employees working on financial crime related data activities is between 0.00% and 0.10%. One respondent has over 20% of their employees working on such activities. This is a small financial institution based in the Middle East with fewer than 500 employees, which is focused on improving its data system infrastructure and training its staff to improve data literacy.

Figure 14: Percentage of employees working on financial crime related activities

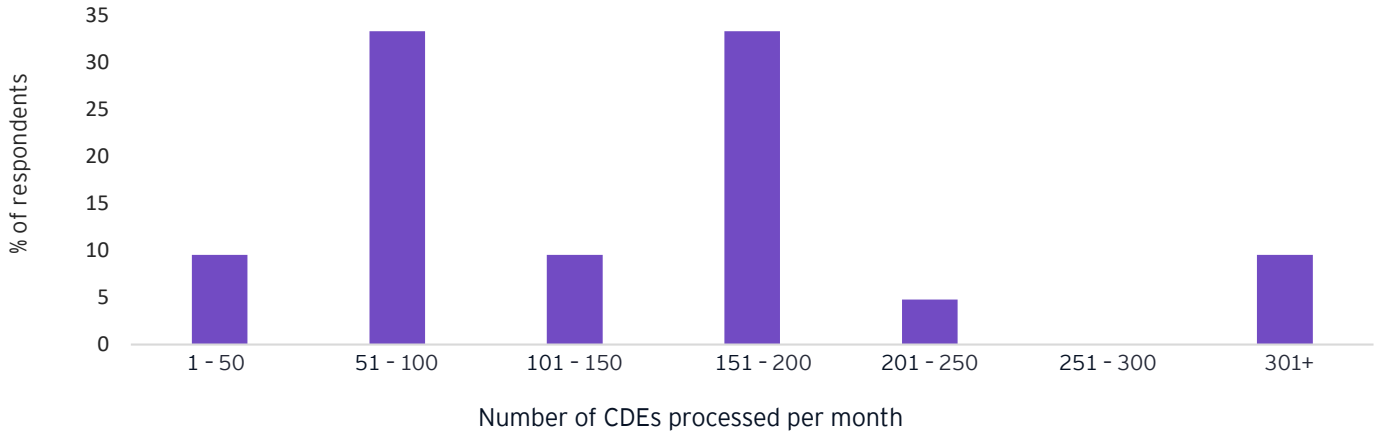


Critical Data Element (CDE) volumes vary, with CDEs managed adequately in general

1.10 CDEs

CDEs are defined as data elements that are deemed materially important to one or more business processes. In terms of volume of CDEs that financial institutions are processing on a monthly basis, two-thirds of participants indicated that they have between 51 to 200 CDEs.

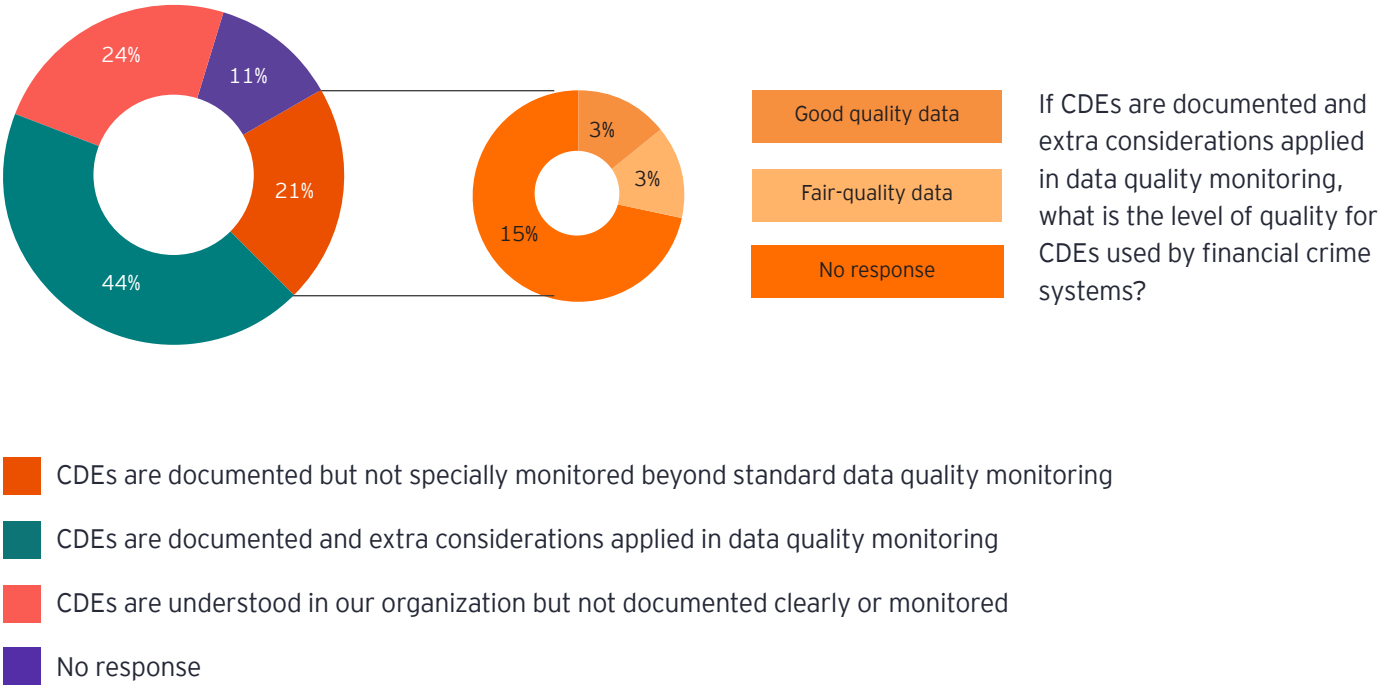
Figure 15: What number of CDEs are processed per month?



Although nearly half of the financial institutions specified that their CDEs are understood and documented, they also indicated that the CDEs are not specially monitored beyond standard data quality monitoring processes.

Approximately a quarter of the participants indicated that CDEs are understood in their organization but not documented clearly or monitored. Lastly, 21% of participants noted that CDEs are documented and extra considerations are applied for these in data quality monitoring. Of these participants, one-third were large global financial institutions, which have well-established financial crime controls.

Figure 15a: Are CDEs understood, documented and monitored in your organization?



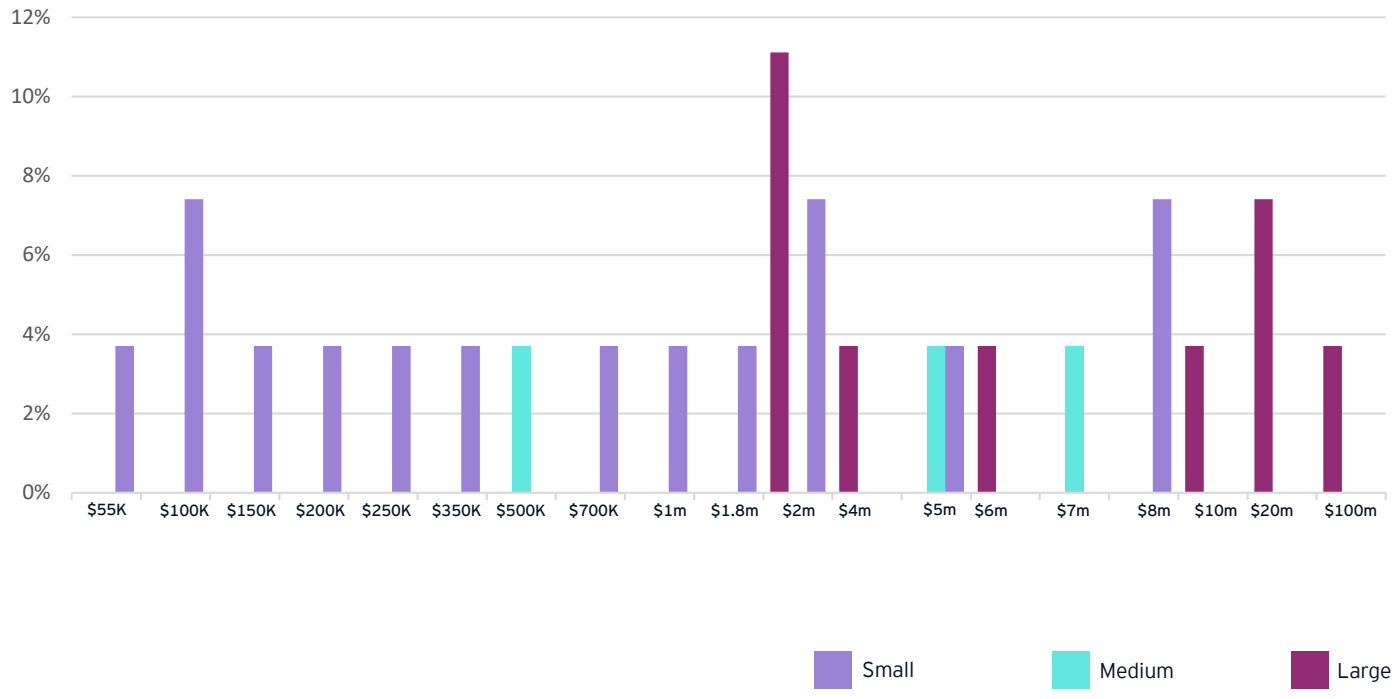
Detailed analysis: investment

Despite increased investment in data management technologies, satisfaction is still low

2.1 Level of current spend in 2020

The level of spend on financial crime-related data initiatives in 2020 shows that over 60% of participants have spent US$50K–US$2.5m, most of these are primarily small-sized financial institutions. The medium-sized and large financial institutions have mostly spent in the range of US$2m–US$100m.

Figure 16: What was the level of spend on financial crime-related data initiatives through the calendar year 2020

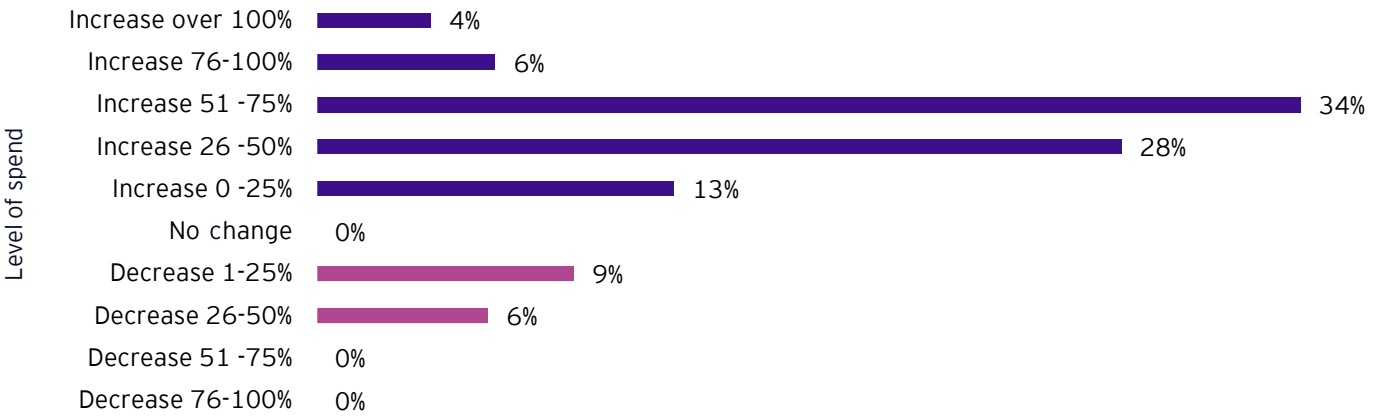


2.2 Level of expected spend in next financial year

In the next financial year 2021–22, 85% of participants have indicated that they expect their spend on financial crime data initiatives to increase. This reflects the increased focus on financial crime, as regulatory and public scrutiny continues to be high. It may also reflect the low satisfaction that many respondents indicated in section 1.1.

For these financial institutions looking to increase spend, the planned increase is around 50%–75%, with 10% committing to an increase of over 75%. On the other hand, 10% of participants noted that they will be decreasing their spend by up to 50%.

Figure 17: How is your spend on financial crime data initiatives expected to change in the next financial year?

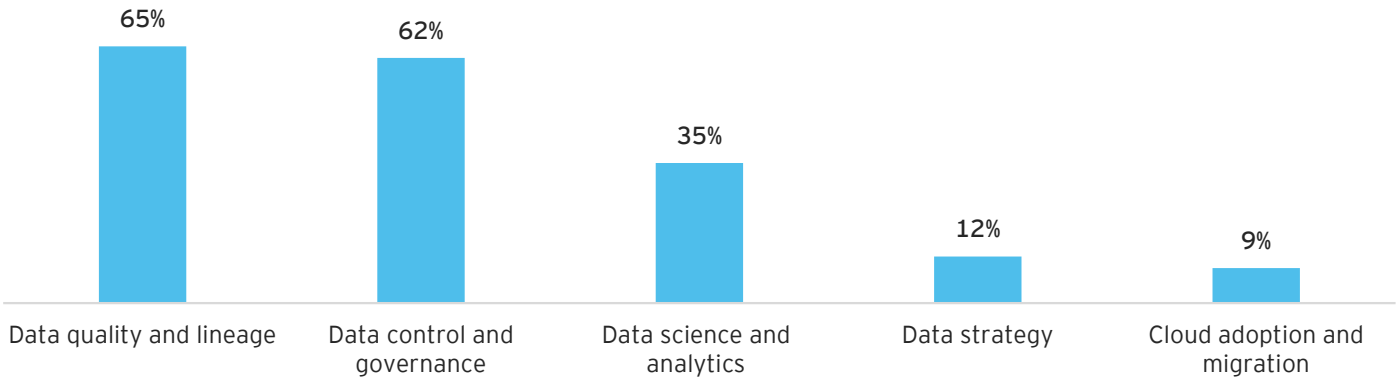


2.3 High-priority data initiatives for investment

The two data initiatives ranked as the highest priority are data quality and lineage, and data control and governance. Data science closely follows, which is linked to process automation, fraud detection and advanced analytical capability. This is unsurprising, given these are fundamental in allowing better monitoring of financial crime and the future use of technology in this area.

In EY teams view, the low importance placed on cloud adoption and migration indicates that, while it might be an important enterprise-level initiative, it is currently a low priority for those in financial crime teams.

Figure 18: Which data initiatives do you class as high priority?

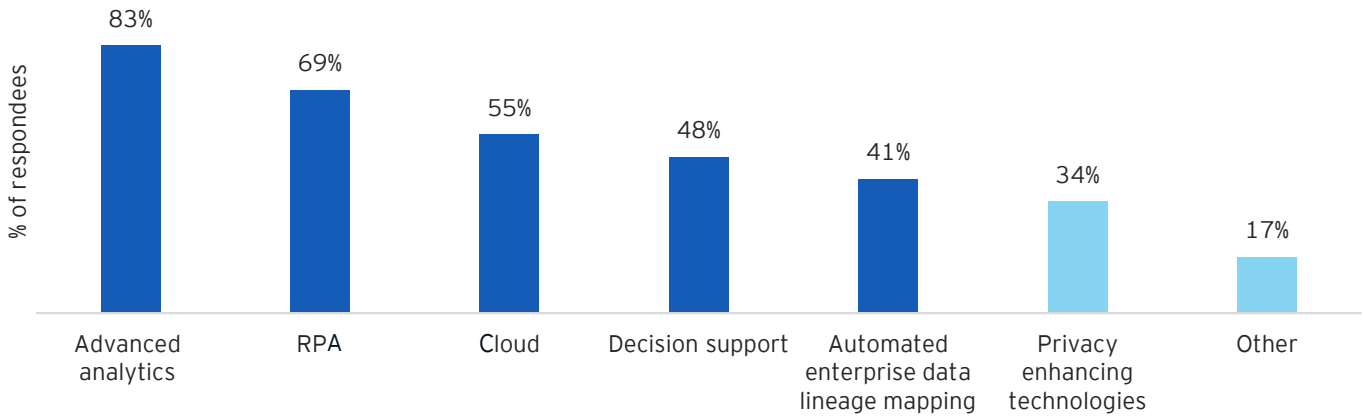


2.4 Investment in technologies

A large proportion of expected investment is earmarked for technology. The majority of participants have indicated that they have or are planning to invest in advanced analytics, (including artificial intelligence, machine learning, predictive modeling, network and entity analytics) and robotic process automation (RPA).

In EY teams view, planned spend on RPA indicates a demand for cost reduction and optimization. Participants looking to invest in analytics, are interested in driving insights to reduce operational inefficiencies. Both of these capabilities would indicate that participants are moving to a higher point on the maturity curve, where cost (rather than effectiveness) is becoming more critical.

Figure 19: Have you, or are you, planning to invest, in any of the following technologies to help manage your data to support financial crime processes and controls?



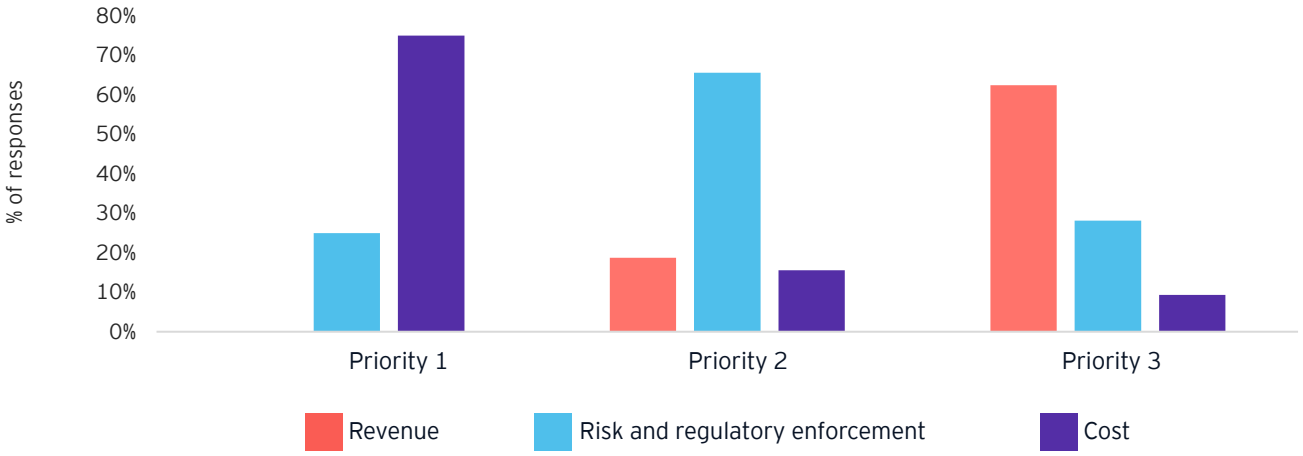
Deeper and more sustainable cost efficiency is the key driver for future investment in data capabilities

2.5 Investment triggers

The majority of participants indicated cost as the number one trigger for investment in data initiatives. This reflects the wave of new regulatory requirements that has driven up compliance costs, while increased capital requirements, slow economic growth and historically low interest rates have all reduced returns – resulting in financial institutions seeking to lower operating costs including risk management costs.

In EY teams view, deeper and more sustainable cost efficiency is the key driver for future investment, and improved return-on-investment performance can be realized by leveraging new data-related capabilities.

Figure 20: What are the likely triggers to drive investment in data initiatives over the next financial year?

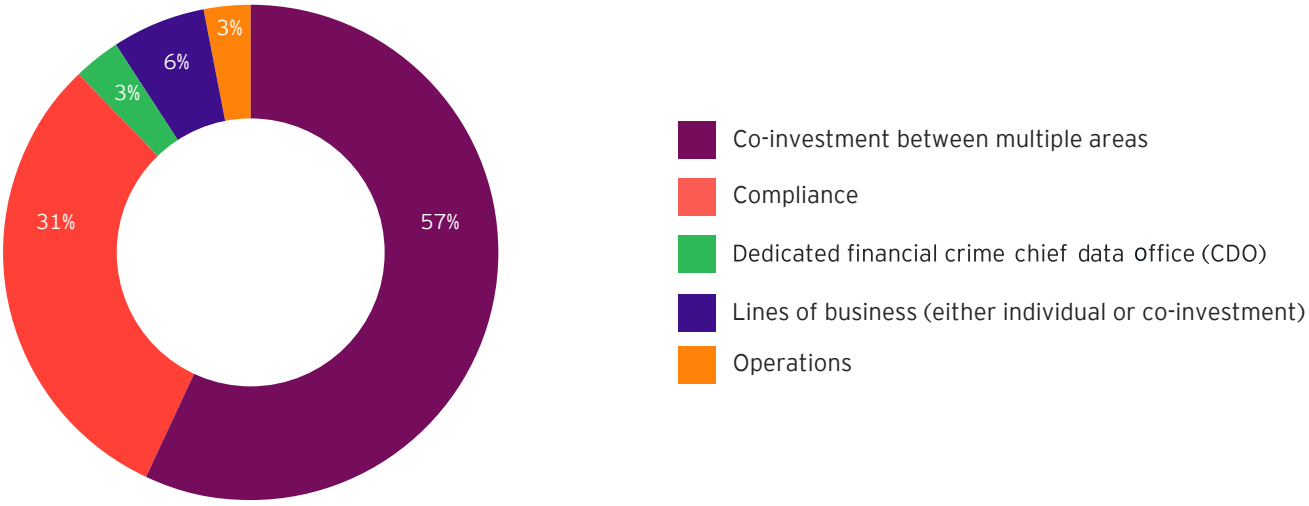


2.6 Source of funding and investment

It is encouraging to see that for over half of respondents, the source of funding is co-investment between multiple areas of the organization. Often firms suffer from a siloed approach to fighting financial crime.

For example, approximately a third of participants indicated compliance as the primary source of funding. Compliance plays a leading role, reflecting the increased scrutiny from financial regulators on data management and robust data controls.

Figure 21: What are the different types of funding for data management initiatives?



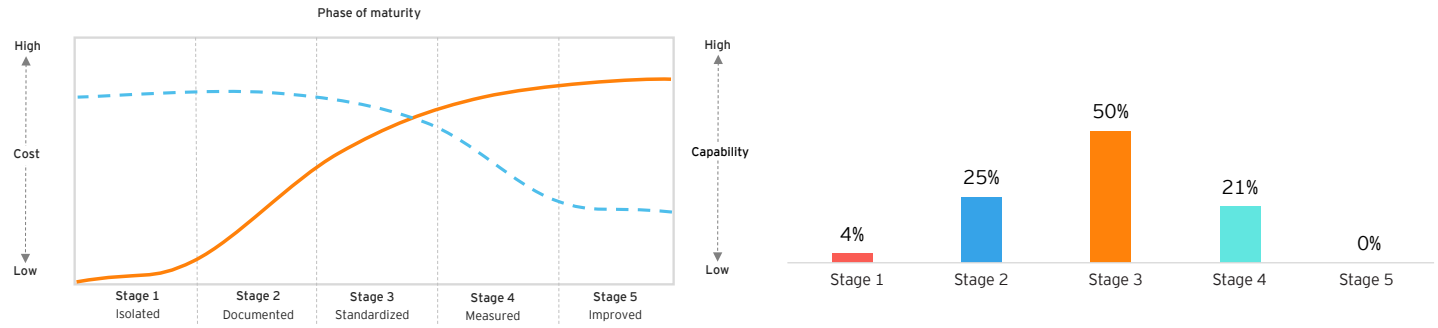
Detailed analysis: strategy

Maturity varies across participants, largely due to regulatory scrutiny, levels of investment and buy-in

3.3 Data maturity model self-assessment

The majority of participants feel they are on route to standardizing their data management capabilities through transformation programs currently underway, but more needs to be done to leverage the full potential of data across all financial crime domains. Organizations at the higher end of data maturity are looking to increase spend in intelligent technologies (such as RPA), suggesting a need for cost reduction and optimization. Financial institutions at the lower end of data maturity are looking to increase spend in analytics to help drive insights to improve operational inefficiencies.

Figure 22: Where would you place your data management capabilities on the following maturity model?



Stage 1 - Isolated	Processes are performed in an ad hoc manner, primarily to allow a specific project to be executed. Actions are usually related to repair rather than prevention.
Stage 2 - Documented	The organization has people with appropriate skills and understanding of data management. Processes are developed and implemented at a department or data subject area level.
Stage 3 - Standardized	Standard data management processes are deployed and used consistently across the organization. A data management framework provides structured guidance to deal with non-standard requirements.
Stage 4 - Measured	Process measurement metrics are defined and used to monitor performance. Anomalies are detected and processes re-engineered as appropriate.
Stage 5 - Improved	Focused on continual improvement of data management processes to support the organization's strategic use of data to drive business success. Sharing, and use of, best practice occurs.

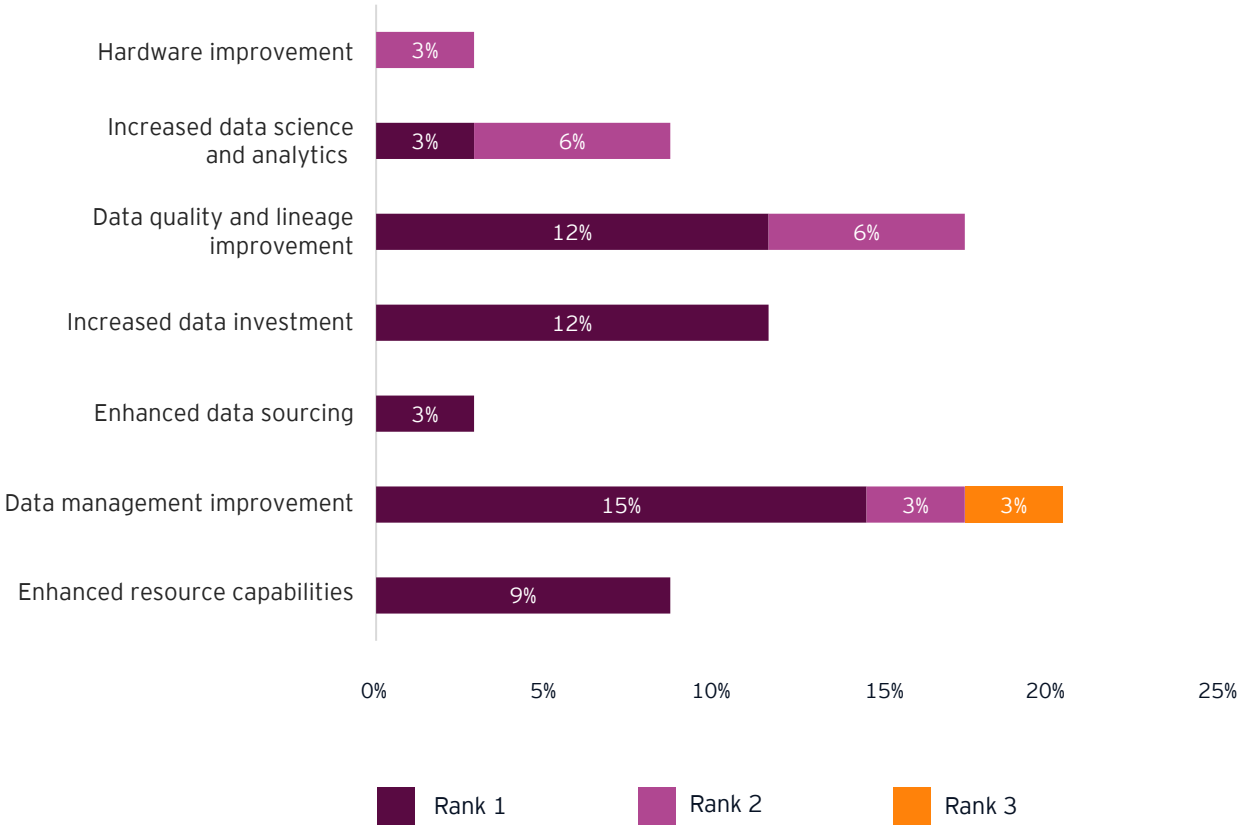
Optimizing data management and quality capabilities are key to future plans

3.4 Future outlook

Most of the participants' future plans with regard to data management involve improving their systems or processes and increasing the investment in, and quality of, data.

Financial institutions recognize that quality data holds the key to current and future regulatory compliance, competitive success and winning the fight against financial crime. Therefore, data quality related controls must be embedded into their existing enterprise risk management framework.

Figure 23: What are the key areas of focus and investment when it comes to improving your data management capabilities?



Conclusion

The way forward

Good data is fundamental to a successful anti-financial crime program. The key challenge is managing the quality of ever-increasing data volumes, which is exacerbated by legacy architecture constraints, poor data governance controls and lack of leadership buy-in.

The delays in tackling these data challenges are an impediment to the effectiveness of financial crime controls, which rely heavily on data being available and of high quality. Data issues and poor architectural design limit a financial institution's ability to detect suspicious activity, rendering detection and decisioning ineffective and making thorough investigation challenging.

The way forward requires more than just fixing data. The focus should be on how to elevate stakeholder engagement and buy-in to enhance data capabilities across the organization. EY anticipates investment in intelligent technologies will drive greater insights and help with cost reduction and optimization. In the EY organization's view, the key elements required for a successful financial crime data program will be:

1. Strong data foundations

A critical component for establishing a strong data foundation is appointing a data leader to be entrusted with enterprise-wide data responsibilities and overall data strategy, regardless of the size of the organization. The data leader will need to begin by ensuring that data is recognized as a central asset throughout the financial institution. This requires a compelling vision, aligned to business goals, an expanded scope of data governance and a structure of accountability for data to drive change.

The focus should be on getting the basics right to accelerate the remediation of legacy quality issues, improving data integrity and the effectiveness of financial crime systems. It is fundamental that the data leader builds a strong team that understands the value of data and empowers it appropriately. Data leadership should look to boost data literacy across the financial crime function, to maximize synergies throughout the organization.

2. Ecosystem and enterprise

The data leader will undeniably play a strategic role in aiding financial institutions to adapt and transform their data ecosystems in response to emerging technology innovations, regulatory changes around data reporting and data privacy, advanced analytics and intelligent automation.

By driving integration and interaction of financial crime systems and processes within the wider enterprise and beyond, both financial crime and business stakeholders can identify opportunities, which could include leveraging data partnerships and external data providers.

Financial services and the prevention of financial crime is being disrupted by FinTechs and RegTechs. It is vital that all financial institutions embrace this disruption to derive increased business value and improved financial crime prevention.

3. Capability and value creation

A visionary data leader develops and implements a data strategy with a set of competencies that work in concert. These competencies should all play an important role in improving data management within the financial crime function and expose new datasets for deeper, proactive analysis of criminal networks.

Fostering innovation and continually improving data management capabilities and maturity will ensure that organizations remain effective and relevant. This can be done by leveraging emerging data and analytics technologies to improve information sharing, collaboration, compliance and security to support critical business objectives.

The enablement of technologies such as artificial intelligence will help in handling the vast volume and variety of data created by a myriad of technologies, to improve data management capabilities including data quality through smart data validation techniques or automating processes for cleaning data, data traceability and agility through integrated decisioning architectures that deploy analytics on common data across the entire customer lifecycle.

EY expects artificial intelligence to play a greater role in fighting financial crime, to stay ahead of technology savvy criminal networks. By utilizing natural language processing techniques and network analytics, financial institutions will have deeper access to criminal networks through unstructured datasets and tools that analyze the morass of unchartered data in real time. Fostering innovation while leveraging emerging data and analytics technologies will aid more advanced financial crime capabilities. Furthermore, data analytics that utilize machine learning to adapt to changing behaviors to spot fraud, will help achieve results in a systematic, prioritized and automated way.

There are opportunities for data management to not only drive efficiencies and operational cost reductions, but, more significantly, to identify intelligence-led and data-driven ways to tackle financial crime.

Contacts

Patrick Craig
Leader
EY EMEIA Financial Crime Technology
E: pcraig@uk.ey.com

Munmun Kumar
Manager
FS Consulting Ernst & Young
LLP E: mkumar1@uk.ey.com

EY | Building a better working world

EY exists to build a better working world, helping to create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

What makes EY distinctive in financial services
Over 84,000 EY professionals are dedicated to financial services, serving the banking and capital markets, insurance, and wealth and asset management sectors. We share a single focus — to build a better financial services industry, one that is stronger, fairer and more sustainable.

EYG no. 008740-21Gbl
ED NONE

ey.com/fs