



International data assurance: market briefing

June 2023

Contents

The international data assurance market	2
Introduction	2
What is data assurance?	4
Research approach	5
The terms used in this briefing	6
Key findings	6
Findings	8
Market segmentation	8
Data assurance through the supply chain lens	10
Demand for data assurance through the lens of data holders	12
Demand for data assurance through the lens of data users	14
The global data assurance market: summary	16
Conclusion	17
Appendix: Profile of survey respondents: by country	18

About

This paper was produced by the Open Data Institute (ODI) and published in June 2023. It summarises research for the ODI on the demand for data assurance services. This research was carried out by Metia Group in the second half of 2022. The lead author of this paper is Emma Thwaites. If you want to share feedback by email or get in touch, contact the ODI's data assurance lead, Angela Baker, at angela.baker@theodi.org

This report is published under the [Creative Commons Attribution-ShareAlike 4.0 International licence](https://creativecommons.org/licenses/by-sa/4.0/).



How can it be improved? We welcome suggestions from the community in the comments

The international data assurance market

Data assurance is crucial for building trust in organisations. Open Data Institute (ODI) research shows that people working in the global data assurance market believe it will grow by 60% — from \$3.5bn to \$5.6bn (US dollars) — over five years. However, businesses face significant challenges in their data assurance strategies, including breaches and reputational risks. Existing technical solutions are often costly, complex and ineffective, leading to low customer satisfaction. Our research found a high demand for data assurance products and services but gaps in affordability and effectiveness. As demand for data assurance services continues to increase, there is a growing requirement for recognised practices, standards and codes of conduct that can provide credibility and trust to suppliers and consumers.

Introduction

Data assurance (see page 4) is critical for boosting trust and confidence in organisations. According to research for the ODI, workers in the global data assurance market expect it to grow by 60% over five years, from \$3.5bn — in 2022 — to \$5.6bn (US dollars) in 2027.¹ However, businesses need help with their data assurance strategies and challenges. These include data breaches, reputational risks and regulatory compliance issues. According to research cited in Harvard Business Review, 68% of companies lack good systems to demonstrate trustworthy data practices. They risk losing 150% of their stock prices if they don't address this.²

¹ Metia for the ODI (2022), '[Market demand for data assurance services](#)'.

² Harvard Business Review (2018), '[A Strong Privacy Policy Can Save Your Company Millions](#)'.

Existing data assurance solutions, such as digital software tools and consultancy, are often costly, complex and ineffective, leading to low customer satisfaction. Yet our market research, conducted by Metia for the ODI,³ found high, and growing, demand for data assurance products and services as companies seek to build confidence with customers, stakeholders and the public.

The research looked at **the market for business-to-business data assurance products and services**, aiming to better understand the challenges businesses face. It revealed that consumers include data managers, C-suite leaders and compliance officers. Gaps in the available products and services include the need for more straightforward, affordable solutions and more effective ways of assessing and demonstrating trustworthiness.

The ODI believes that adopting data assurance products and services can help organisations to build trust in organisational data practices and data. It can also help them to change their beliefs and behaviours around data sharing across organisational and geographical boundaries. By addressing the gaps in available services and products, simplifying language and raising awareness of the value of data assurance, the ODI aims to help organisations improve their data practices, reduce risks and build trust with stakeholders.

This briefing about the international data assurance market summarises key points from our research and shares our expectations for how the market may develop over the next four to five years.

³ Metia for the ODI (2022), '[Market demand for data assurance services](#)'.

What is data assurance?

The ODI defines data assurance as ‘the process, or set of processes, that increases confidence that data will meet a specific need, and that organisations collecting, accessing, using and sharing data are doing so in trustworthy ways’.⁴ The ODI emphasises the importance of data assurance in building confidence and trust. Data sharing is restricted because governments and organisations that could share or reuse data cannot assess datasets’ trustworthiness or other organisations’ data practices.

Data assurance supports dataflows across the whole data spectrum,⁵ from closed to open. This includes **internal dataflows** (generated and used within an organisation) and **external dataflows** (the use of data received from third parties external to an organisation, data shared with third parties from an organisation, and the reuse or sharing of open data). This enables business and public service innovation.

Data assurance improves the trustworthiness of the dataflow in several ways by assuring the organisational data practices and the data itself. The common factors likely to be important when assessing whether data sharing and reuse (dataflows) are trustworthy are:

- **Organisational governance and internal oversight:** the extent to which there is a clear strategy for data and data policies; processes are in place to identify and manage risks; and there is leadership with the responsibility, accountability and capacity to deliver
- **Privacy:** the level of protection given to the data of employees, customers and partners
- **Security:** the extent to which systems, policies and processes keep data secure and protected. This might include adherence to common cybersecurity standards

⁴ ODI, [‘Data assurance: Building trust in data’](#).

⁵ ODI, [‘The Data Spectrum’](#).

- **Quality and accuracy:** the extent to which the quality and consistency in how data is collected, used and shared meets required standards or specifications
- **Ethics and transparency:** the extent to which an organisation states and adheres to ethical principles and sustainability standards, and is open to public scrutiny
- **Data access processes:** the extent to which policies and procedures surrounding data sharing, provision and access are embedded and resourced
- **Skills and knowledge:** the extent to which the knowledge, training and learning required to collect, use and share data in trustworthy ways is understood and in place
- **Engagement and accountability:** the extent to which the interests and concerns of data stakeholders are actively sourced and addressed, and that the organisation can be held to account if necessary

Research approach

The market research conducted by Metia for the ODI used a multi-method approach, including primary and secondary research and analysis of publicly available and ODI-provided sources. It also included a bespoke, multi-country survey. The survey investigated the appetite of data holders and users for data assurance products and services and the offerings of assurance providers.⁶ The survey involved professionals responsible for the assurance of external data, including data assurance service providers on the supply side and data holders and data users on the demand side. It covered five markets: the UK, Germany, France, the USA and Singapore.

⁶ The survey was fielded between 21 July 2022 and 7 August 2022. The target sample size was 750 and the achieved sample was 791 participants.

The terms used in this briefing

External and internal data types — our definitions

- **External data** encompasses data that organisations intend to use, or that can be used, outside of their own organisation. This includes data received from third parties, data shared with external entities and open data.
- **Internal data** refers to data intended for use within organisations or data that is considered confidential or market-sensitive and which cannot be shared externally. This type of data is referred to as internal-only data. Internal data can be generated either by third parties externally, through their franchises, or within organisations themselves.

***Please note:** this market research included respondents who work with external data or a blend of external and internal data, and excluded respondents who work with internal-only data.*

Data assurance organisation categories

- **Data assurance service providers** are organisations offering data assurance products and services to other organisations.
- **Data holders** are organisations using external data assurance services in order to assure the quality and consistency of the data they hold and share with third parties.
- **Data users** are organisations using external data assurance services in order to assure the quality and consistency of the data that they don't hold themselves but that is shared by third parties and used within, or by, the data users.

Key findings

- The data assurance market is composed of internal and external data. Respondents estimate it to be worth \$3.5bn (US dollars) in 2022 and it is projected to grow to \$5.6bn (US dollars) by 2027
- Data holders are the dominant category in each of the five markets surveyed
- Assurance of external data boosts organisations' trustworthiness and 92% of respondents allocate a budget for external data assurance products and services
- However, two thirds (66%) of respondents believe that data assurance supply does not fully meet their needs
- The market is in its infancy, with solid potential for future development
- The market is dominated by well-educated, male, millennial tech professionals from IT, financial and manufacturing sectors who prioritise mitigating risk, complying with legal requirements and boosting the trustworthiness of organisations
- The market understands assurance to be associated with security and protection but more education is required on external data assurance, including how it builds trust
- The majority of data assurance providers are millennials, and data holders primarily operate within the IT industry, although are less dominant in this sector than service providers
- Data users come from industries similar to data holders, with banking/financial/investment management being less prominent
- Organisations with 500 to 5,000 employees have the highest representation across the data assurance segments
- Data holders and data users are typically in organisations exceeding 1m in revenue⁷

⁷ In local currency.

Key metrics at a glance

\$3.5bn

Data assurance market size, 2022 (USD)

\$5.6bn

Data assurance market size, 2027 (USD)

66%

of data holders and data users believe that data assurance supply does not fully meet their needs

94%

of data holders and data users believe that external data assurance boosts organisations' trustworthiness

92%

of respondents allocate budget for external data assurance products and services

63%

of respondents agree that increasing market demand for data sharing is the key driver behind external data assurance growth

Source: Metia Group – Market Demand for Data Assurance Services report – May 2023

metia

Figure 1. Data assurance market key metrics

Findings

Market segmentation

Our survey revealed that organisations with between 500 and 5,000 employees have the highest representation across data assurance segments – service providers, data holders and data users. Data holders and users are typically in organisations that exceed 1m in revenue.⁸

The IT industry dominates the market

The IT industry is the leading sector in data assurance, with 20% of survey respondents coming from this field. Within the IT segment, 38% of service provider respondents come from companies with 1m to 10m annual turnover,⁹ whereas 29% of data holders are from companies with a turnover of 50m to 100m and over.¹⁰ Data users within the IT segment were from three equally important company sizes: 19% of respondents work for companies with a turnover of 100m or more; 19% for companies with a turnover of 25m to 50m; and 19% for companies with a turnover of 1m to 5m.^{11,12}

Established organisations are more prevalent

The survey found that established organisations with more than 10 years of experience are more likely to work with external data assurance and that the IT industry is more inclined to adopt data assurance practices.

Younger organisations are less prominent in all data assurance sectors, but those established in the three-to-five-year range are more prominent in working with data for external use only.¹³

⁸ In local currency.

⁹ Ibid.

¹⁰ Ibid.

¹¹ Ibid.

¹² Metia for the ODI (2022), '[Market demand for data assurance services](#)', p. 36.

¹³ Ibid, p. 37.

Data assurance is important for organisations

Across all three data assurance categories — service providers, data holders and data users — most respondents report to the Chief Information Officer/Chief Technology Officer (CIO/CTO; 31%), the Chief Executive Officer (CEO; 19%) or the Chief Operating Officer (COO; 13%). This indicates the importance of data assurance to the C-suite in the organisations surveyed.¹⁴

The global profile of survey respondents

- The research shows that **45% of data assurance service providers come from the USA**, and 89% offer both internal and external data assurance services
- Among service providers, 66% work for companies established for over 10 years
- **Data holders** interested in data assurance are typically between 31 and 40 years old, have between three and five years of experience, and work for companies that have been established for more than 10 years
- **Data users** are typically between the ages of 36 and 40, have between three and five years of experience in data assurance, and work for companies with over 100m in annual turnover¹⁵
- Overall, 66% of respondents work for companies that have been established for over 10 years¹⁶

For a more detailed view of survey respondents by country, please see the Appendix.

¹⁴ Metia for the ODI (2022), '[Market demand for data assurance services](#)', p. 38.

¹⁵ In local currency.

¹⁶ Metia for the ODI (2022), '[Market demand for data assurance services](#)', pp. 50–52.

Data assurance through the supply chain lens

Data assurance providers generally operate in a limited geographical market, with many targeting customers in their home country and neighbouring regions. North America and Western Europe are the key markets for established providers.¹⁷

Data assurance services are typically offered as part of a broader portfolio of services, with around 46% of survey respondents reporting that data assurance generates between 20% and 49% of their company's turnover. While most providers offer a blend of data assurance services for internal and external data, some providers offer data assurance services exclusively for external data.

Assurance of external data is expected to grow strongly in the next five years, with 98% of service providers believing this to be likely.

The IT and banking/financial sectors are the primary target for external data assurance offerings, with providers anticipating moderate growth in these industries. Providers expect the automotive, healthcare and retail sectors to be in the next wave of growth. Higher demand for external data assurance services is anticipated due to the increasing sophistication and volume of data that organisations use in their daily operations, combined with stricter regulatory requirements concerning data protection and security.

Data assurance service providers see a lack of quality control and data governance as crucial pain points. 50% cite these two factors as the most common issues data holders and users attempt to address with data assurance services. In addition, a third cite the following challenges as critical customer issues:

- **Data compliance:** Assuring that external data is conforming to all significant regulations, including GDPR, CCPA and DSAR¹⁸
- **Sourcing and collection:** Assuring that external data is collected and sourced in an ethical and equitable manner
- **Data curation:** Assuring that external data is maintained, updated and cleansed in a trustworthy manner¹⁹

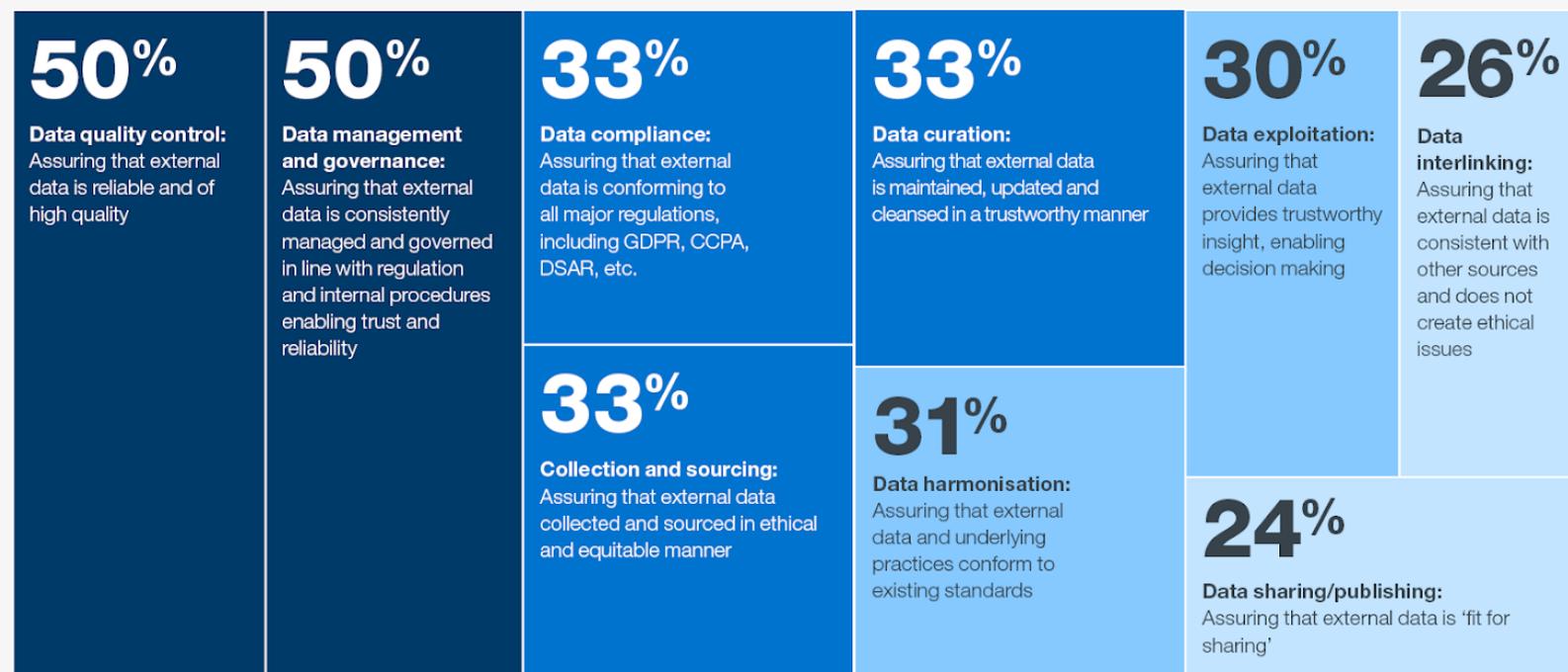
¹⁷ Metia for the ODI (2022), '[Market demand for data assurance services](#)', pp. 50–52.

¹⁸ The General Data Protection Regulation, California Consumer Privacy Act and Data Subject Access Request.

¹⁹ Metia for the ODI (2022), '[Market demand for data assurance services](#)', pp. 53–69.

The lack of quality control and data governance are seen as key pain points by data assurers

Service providers attitudes towards key pain points on the demand side



N=141

Source: Metia Group – Market Demand for Data Assurance Services report – May 2023

metia

Figure 2. Service providers' attitudes towards pain points in the demand side

Demand for data assurance through the lens of data holders

Organisations that hold data are the primary market serviced by data assurance providers. Most data holders operate in a single country or on a multi-country basis, with only a minority operating globally or regionally.²⁰

Data holders use data assurance products and services to improve the quality of their data, minimise risks, promote wider data sharing between organisations, comply with regulations, and enhance their reputation and status.

Most data holders demand a blend of internal and external data assurance services and believe that data assurance positively impacts their organisation's trustworthiness.

Data quality (41%), governance (41%) and compliance (37%) are the top challenges that data holders want to overcome. They think that the data assurance services they need exist, but there are gaps, particularly in the availability of solutions tailored to their specific needs.

In most organisations, the decision-making authority for external data assurance procurement rests with the CEO, CTO or CIO.

Data holders are ready to invest in external data assurance, with a considerable proportion allocating between 100k and 250k a year.²¹ Data holders are consciously taking steps towards improving external data assurance and data sharing.

Most data holders operate locally and 62% have a budget of less than 250k a year.²² However, investment in external data assurance is expected to rise in the near- to mid-term, with 60% of data holders expecting a moderate increase in investment in the next five years. Overall, data holders say they prefer working with suppliers that are approved by a data standards body, with 29% preferring an accredited practitioner.²³

²⁰ Metia for the ODI (2022), '[Market demand for data assurance services](#)', pp. 71–84.

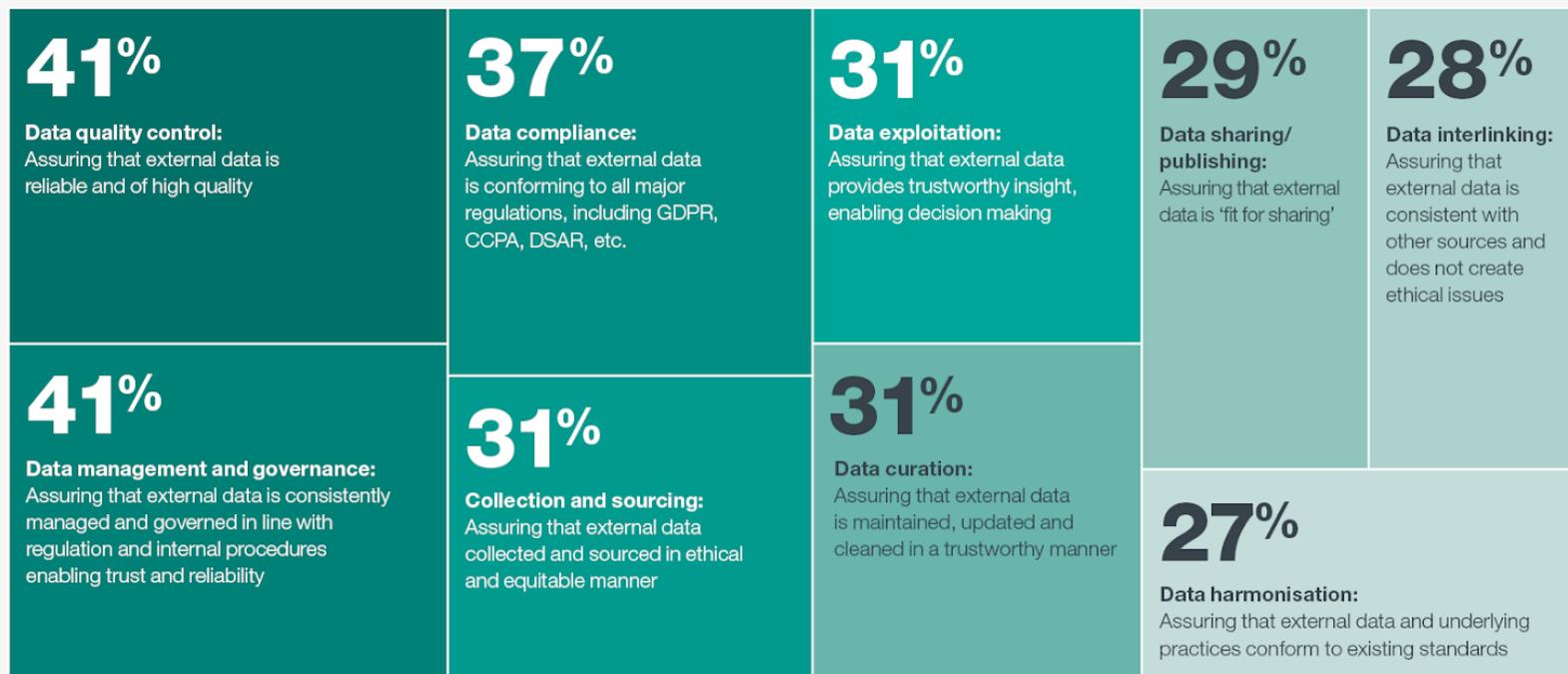
²¹ In local currency.

²² Ibid.

²³ Metia for the ODI (2022), '[Market demand for data assurance services](#)', pp. 71–84.

Data quality, governance and compliance are the top-3 challenges data holders are looking to solve

Data holders' attitudes towards the key pain points of external data assurance



N=414

Source: Metia Group – Market Demand for Data Assurance Services report – May 2023

metia

Figure 3. Main challenges faced by data holders

Demand for data assurance through the lens of data users

Overall, our research indicates there is demand for external data assurance among data users, particularly in Western Europe (71%). The assessment of this demand suggests that data users typically operate at the national level in single- or multi-country markets, with only a minority of regional or global organisations. Data users seek to improve quality and minimise risk by using external data assurance.

Regulatory compliance is the leading concern for data users when sharing internal data in the market.

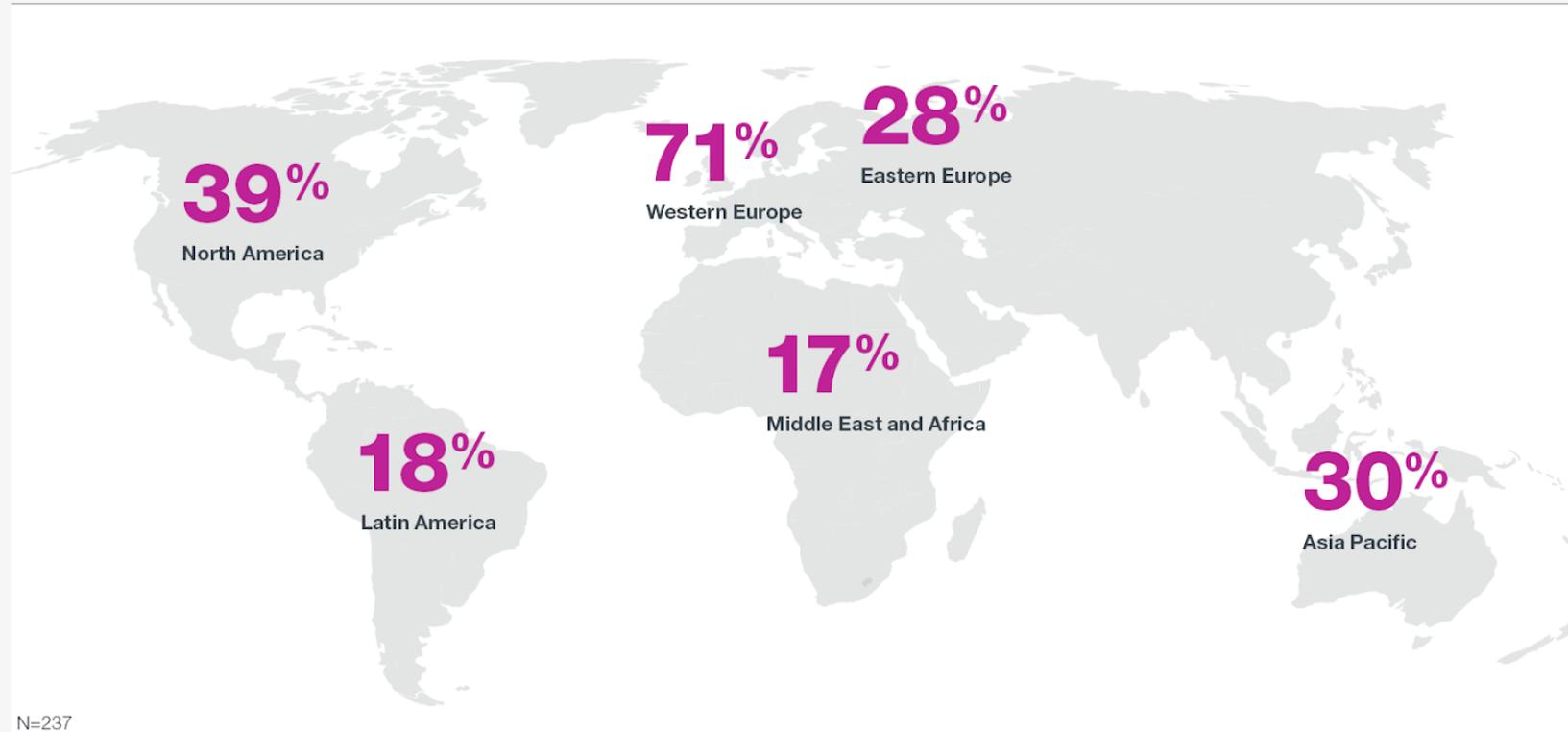
Our research found that 38% of data users believe that data assurance has a highly positive impact on their organisation's trustworthiness, while 58% believe it has a moderately positive impact.

Data users seek to solve three key challenges: data quality, compliance and governance (42%, 41% and 37%, respectively).

A significant segment of data users believes there is scope for an expansion of external data assurance solutions. The largest segment (39%) reports that while the data assurance market is currently addressing a few of its fundamental problems, there remain gaps in the services provided by the market.

Western Europe is the dominant region for data user demand

Geographic distribution: Percent share of regions where data users currently operate



Source: Metia Group – Market Demand for Data Assurance Services report – May 2023

metia

Figure 4. Data user demand in external data assurance

Over three-quarters of data user organisations report external data assurance decision-making by the CEO, CTO, CIO and COO. Most data users have a budget above 50k²⁴ for external data assurance, while only a limited number (mainly smaller organisations) have no budget at all.

Data users expect to expand their investment in external data assurance over the mid-term. 63% anticipate a moderate increase of up to 20% a year during the five years from August 2022. A further 13% of respondents to our survey foresee more significant growth of more than 20% a year.

The research found that affordability is an issue; reported by 18% of data users. The range of external data assurance products and services is often not accessible because they are beyond the organisation's budget, and the procurement process for external data assurance can also be detailed and lengthy.²⁵

Overall, nearly three-quarters of data users trust suppliers more if a data assurance standards body recognises them:

- 25% of data users would prefer a supplier who is **an accredited practitioner** of a data standards body/code of practice
- 26% of data users would prefer a supplier who is **certified by a** data standards body/code of practice
- 22% of data users would prefer a supplier who **works in partnership with** an official data assurance standards body²⁶

²⁴ In local currency.

²⁵ Metia for the ODI (2022), '[Market demand for data assurance services](#)', pp. 85–98.

²⁶ Ibid.

The global data assurance market: summary

- The global data assurance market was estimated to be worth between **\$2bn** and **\$4bn** (US dollars) in 2022, according to respondents who could estimate its size.
- Growth in the market is predicted, with **85%** of respondents expecting the external data assurance market to grow over five years, driven by the increasing demand for data, ever-evolving technological capabilities, and rising regulatory pressures.
- Despite some pessimism, the market may be worth as much as **\$5.6bn** (US dollars) by 2027.
- Europe is regarded as a region that will grow strongly, while North America is the most developed data assurance market. Latin America is gaining momentum, while the Middle East and Africa are the least developed markets but have the potential for exponential growth. The Asia Pacific region contributes significantly to the global data assurance market and generates stable growth.
- Currently, assurance of external-only dataflows remains a niche market. **98%** of respondents agreed that the exclusively external data assurance segment comprises just **3%** of the market. Solely internal data assurance also has limited appeal, with just **6%** of the market. The most significant section of the market is currently in the assurance of data that is meant for internal use but can be shared externally. Respondents consider this to account for an estimated **80%** of the market.
- There is a movement towards preparing internal data for external use, driven by industry developments such as the push towards open banking, GDPR and new privacy laws, and a broader movement toward sharing data by regulators and the public sector.
- On a global level, organisations are more likely to have a budget **below 50k** than **above 1m**,²⁷ partially indicating the smaller size of organisations currently active in the market for data assurance.
- Over half of survey respondents estimate that **between 6% and 20%** of their organisation's external data assurance budget is spent on purchasing products and services from third-party suppliers.
- The majority spend at least some of their budgets externally, with only **7%** spending **98% to 100%** of their budgets in-house.²⁸

²⁷ In local currency.

²⁸ Metia for the ODI (2022), '[Market demand for data assurance services](#)', pp. 99–131.

Conclusion

External data assurance is becoming more critical as organisations use growing amounts of external data. This has created a challenge in the credibility and trustworthiness of external dataflows, with regulatory requirements increasing.

This market is dominated by professionals who prioritise mitigating risks, complying with legal requirements and boosting trustworthiness. This creates demand in the market for products and services, enabling professionals to be assured that external data complies with legal and regulatory frameworks and that any risks are well managed.

Demand for enhanced external data assurance services is driven by the higher volumes of data that organisations use in their day-to-day operations. **Data holders and users** want to increase the trustworthiness of their organisations to external stakeholders, and **service providers** recognise the need for transparency in standards and the quality of delivery of data assurance. Although there is variation in the budget allocated to data assurance – based on industry and organisation size – 53% of data holders and data users spend between 6% and 20% of their budget with third parties. While external data assurance is mainly executed by in-house teams, over half of organisations seek outside help for at least some process elements. Yet, there are still gaps between the demand and supply sides around the priorities for key market provision. There is an opportunity for service providers to understand the needs of data holders and data users better.

Survey respondents anticipate that the global data assurance market will grow by 60% over five years – from \$3.5bn in 2022 to \$5.6bn (US dollars) in 2027 – driven by increasing requirements around data externalisation. There is a significant and growing demand for data assurance services that can provide tailored solutions and bespoke pricing structures to meet the specific needs of data holders and data users.

As the demand for data assurance services increases, more agile and customised products and services will be essential for meeting the needs of this fast-moving market. At the same time, the requirement for recognised practices, standards and codes of conduct will grow. These will set the bar, ensuring standard protocols for emerging products and services and allowing the safe and equitable flow of data across organisational and geographical boundaries.

Appendix

Profile of survey respondents: by country

UK

In the UK, **university-educated millennials drive the data assurance sector**, with 36% of survey respondents holding data management or data transformation/project manager titles and 22% working for companies with 1,000 to 5,000 employees. 17% of respondents work for companies with 1m to 5m GBP turnover. 80% of respondents hold a bachelor's degree or higher, and 40% have 15 years or more of work experience.²⁹

Germany

The survey indicates that **regulatory compliance is a key aspect of data assurance in Germany**, and 28% of respondents are responsible for their company's compliance. Most respondents hold IT specialist/manager/engineer titles and have at least a bachelor's degree. Most respondents are male, with 45% aged between 31 and 40. 36% have 15 years or more of work experience. Additionally, 30% of respondents have worked in the data assurance space for three to five years.³⁰

France

The French data assurance market **has a higher share of female workers than other markets**. The survey showed that 52% of respondents are male. Overall, 87% of workers are in full-time paid employment. 32% of respondents hold executive/implementation positions, and 29% hold IT specialist/manager/engineer titles. Most respondents (87%) have at least a bachelor's degree and 35% have 15 years or more of work experience. 31% of respondents have worked in the data assurance space for three to five years, and 24% are between the ages of 31 and 40.³¹

USA

US experts have a longer tenure in data assurance than their European counterparts. 14% of respondents work for companies with a turnover of 5m to 10m USD. 30% of respondents hold leadership positions, while another 30% deal with the delivery and execution of strategies. Around 19% of respondents come from companies with 51 to 200 employees, and the same share comes from companies with 501 to 1,000 employees. 33% of respondents hold an IT specialist/manager/engineer title.

²⁹ Metia for the ODI (2022), '[Market demand for data assurance services](#)', p. 44.

³⁰ Ibid, p. 46.

³¹ Ibid, p. 47.

83% of US respondents have a bachelor's or higher degree. 30% have five to 10 years of work experience, and 32% have worked in data assurance for three to five years. 41% of respondents are aged between 31 and 40, and 59% are male. 82% are in full-time, paid employment.³²

Singapore

In Singapore, **most data assurance experts work for large conglomerates**, with a quarter in organisations with a turnover above 100m SGD. 38% hold managerial positions. 93% of respondents have a bachelor's degree or higher, and 30% have 15 years or more of work experience. The largest age group is 31 to 40 (41%), and 75% of workers overall are male. 34% have worked in data assurance for three to five years.³³

Profile of survey respondents by country

% of respondents who are	UK	USA	Germany	France	Singapore
Male	61%	59%	73%	52%	75%
Aged 31–40	38%	41%	45%	42%	38%
Bachelor's degree or higher	80%	83%	73%	87%	93%
Worked in the field 3–5 years	37%	27%	30%	30%	34%
Worked in the field 5–10 years	26%	32%	23%	31%	25%
Worked in the field 15+ years	11%	9%	8%	8%	5%
Employees in full-time paid employment	83%	82%	80%	87%	91%

Table 1. Characteristics of people in the international data assurance market (Source: Metia for the ODI (2022), *Market demand for data assurance services*)

³² Metia for the ODI (2022), '[Market demand for data assurance services](#)', p. 45.

³³ Ibid, p. 48.