Data assurance: what is it and why do we need it?

February 2023

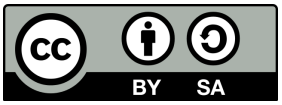
Contents

About

This report was researched and produced by the Open Data Institute, and published in February 2023. Its lead author is Matt Davies, with contributions from Lisa Allen, Miranda Sharp, Emma Thwaites, Gavin Freeguard and Angela Baker.

To share feedback please contact the ODI's Policy team at policy@theodi.org.

Comments? Please email us: policy@theodi.org



Executive summary

Data assurance is essential to enable trusted and trustworthy data practices.

We're living in a data age. Across all sectors, governments, businesses and organisations collect, maintain and share ever-expanding volumes of data. Data is used to create new products, services, insights and analyses, enabling previously untapped economic activities to thrive. Access to data can help us tackle the biggest challenges we face as a society, such as the climate crisis, and improving access to healthcare.

Data and data infrastructure are now major determinants of economic growth. The UK government's National Data Strategy aims to 'unlock the value of data across the economy', and the European Union's European Data Strategy notes that access to data is 'essential for innovation and growth'.

Every organisation is a data organisation, involved in some form of data collection, maintenance and sharing. While businesses, governments and other organisations – as well as the people and societies they serve – stand to benefit immensely from data, legitimate concerns remain about how data is, or might be, used. Unlocking the value of data requires that the individuals and organisations, who collect, maintain, share and use data, are trusted.

We define data assurance as 'the process, or set of processes, that increase confidence that data will meet a specific need, and that organisations collecting, accessing, using and sharing data are doing so in trustworthy ways'.

Data assurance tools and practices can help to provide confidence that the data is trustworthy throughout its lifecycle and there is strong evidence that data assurance is key to trustworthy data management. Individuals and businesses are more willing to share data, and use data that is shared by a third party, when strong governance and assurance mechanisms are in place. In the same way as organisations adhere to best practices in financial or people management, organisations should also adhere to data assurance practices.

At the Open Data Institute (ODI), we believe there is a need to go beyond the current legal requirements as they are not sufficient across all areas. This is vital if we are to build trust in data and unlock the significant economic benefits of data sharing. We believe that data assurance will help those creating, using or sharing data to assess, build and demonstrate trustworthiness in data and data practices.

The ODI aims to provide support and direction for data assurance activities, including proposing norms and principles that help guide and reinforce trustworthy behaviours. This helps provide guidance and direction for organisations to build trust in their data practices and datasets.

We continue to work with partners, stakeholders and collaborators to explore this important and rapidly developing area.

1. The need: trust in data flows

We're living in a data age. Data is collected, maintained, shared and used in growing quantities – by governments, businesses and other organisations across all sectors. It is used to create new products, services, insights and analyses, enabling previously untapped economic activities that could create trillions of dollars worth of value.[1]

Jurisdictions around the world are increasingly acknowledging that access to data – and the data infrastructure that enables this access – is now a major determinant of economic growth. Mission 1 of the UK government's National Data Strategy (NDS) aims to 'unlock the value of data across the economy', while the European Union's European Data Strategy notes that access to data is 'essential for innovation and growth'.[2] [3]

Beyond the economic gains, data is rapidly becoming an essential component of government, business and community decision-making for social good. It can help us to tackle the biggest challenges we face as a society, such as managing the impacts of climate change, access to healthcare and reducing poverty. Coordinating our response to these cross-sectoral social goals requires data to be shared widely across sectors, organisations, societies and governments.[4]

We witnessed this first-hand during the Covid-19 pandemic. There were examples of rapid, efficient, and ethical sharing of vital information between governments, businesses, organisations and public services that helped save countless lives and helped prevent further economic damage. The UK government recognises this, pledging in the NDS to 'maintain the high watermark of data use set during the pandemic'.[5]

The importance of data will only grow further in the coming years and decades. The rapid development and increased adoption of technologies that use data, along with the availability of increased computing power, is resulting in ever-increasing data requirements and capabilities for predictive modelling, advanced data analytics and artificial intelligence (AI). Data is an essential component of government, business and community decision-making, and is an emerging class of infrastructure in its own right.

[1] Open Data Institute (2021). The economic impact of trust in data ecosystems – Frontier Economics for the ODI [report]
[2] Department for Digital, Culture, Media and Sport, gov.uk (2021), National Data Strategy Mission 1 Policy Framework: Unlocking the value of data across the economy
[3] European Commission (2022), European data strategy
[4] Global Partnership for Sustainable Development Data (2022) Global Partnership for Sustainable Development Data
[5] Department for Digital, Culture, Media and Sport, gov.uk (2020) National Data Strategy

Every organisation is a data organisation

This means that data is now everyone's business. In previous eras, data stewardship was primarily the concern of what we might call 'traditional' data institutions (such as national statistics offices, company registers and other large bureaucracies). Today, by contrast, nearly every organisation has some role in data collection, maintenance and sharing, from small businesses maintaining records of transaction data to large conglomerates publishing data on their environmental records. In other words, in the 21st century, every organisation is a data organisation.[6]

In this context, **data governance**, **data infrastructure** and **data practices** represent essential activities within an organisation. These cover the framework for the overall integrity, availability, usability and security of data within the organisation. The data infrastructure comprises data assets, standards, technologies and policies, including the processes by which the data is collected, shared, held and managed. Just as businesses in every sector are expected to adhere to best practice in financial management, or in the management of their people, we think that organisations should also adhere to trustworthy data practices.

Data skills are often considered to be part of a technical domain, centering on practices associated with data engineering and analysis. At the ODI, we think that data practice is more holistic than this, bridging the 'two cultures' of science and humanities described by CP Snow.[7] Our data skills framework illustrates how technical data skills must be balanced with skills that enable data innovation and data management across the data lifecycle, helping to unlock the full value of data.

Trust in data

While businesses, governments and other organisations – as well as the people and societies they serve – stand to benefit immensely from data, there remain legitimate concerns about how data is, or might, be used. Data collection, use and sharing brings with it risks to people, organisations, the economy and wider society. These risks can be difficult to predict, particularly when existing data is combined with new data, or analysed using new technologies or algorithms which may create sensitive insights. Organisations holding data and considering whether to share it may therefore have concerns about how that data will be used – and the consequent reputational, legal and financial costs that come with misuse.

Left unaddressed, these fears are likely to diminish data sharing and the use of data shared by other organisations. The result of this will be to damage the credibility of products, services and decisions derived from data, limiting the potential growth and innovation.

In other words, to effectively unlock the value of data, it is essential that the individuals and organisations collecting, maintaining, sharing and using data are **trusted**. Research carried out for the ODI by Frontier Economics in 2021 found

[6] Including in the UK government. Open Data Institute (2021), Mapping data in the UK government.
[7] Cambridge University Press (1959), The Reed Lecture 1959: The two cultures and the scientific revolution. Vol. 960

quantitative evidence that trust in data and data practices is a key determinant of data sharing.[8] Greater trust – in individual datasets, in the institutions stewarding them, and in the wider data ecosystems in which those institutions sit – results in higher levels of data sharing, and increased data availability. If there are higher levels of data sharing, and more data is available, then better decisions are made at all levels that affect people, communities, and organisations.

This research has since been corroborated by findings from further studies. Respondents to the Centre for Data Ethics and Innovation's (CDEI's) most recent tracker survey reported that their willingness to share data with an organisation was strongly related to the levels of trust they reported in that organisation.[9]

Professionalising data practices

There is strong evidence that individuals and businesses are more willing to share data, and to use data that is shared by a third party, when strong governance mechanisms are in place to assure them.[10]

Despite this, public trust in the data practices of many organisations across the public and private sectors is currently low, with only the NHS, pharmaceutical researchers and academic institutions trusted by more than half of respondents to the CDEI tracker survey.[11]

Data regulations, for example for data protection, such as the General Data Protection Regulation (GDPR), set the minimum standards that are acceptable in law when handling personal data. Organisations must abide by the law to avoid legal consequences. However, there are currently no laws that cover all types of data, with legal regulation often lagging behind technological developments, creating a gap between the law and the reality of work in a data-driven environment.

At the ODI, we believe there is a need to go beyond the current legal requirements as they are not sufficient across all areas. This is vital if we are to build trust in data and unlock the significant economic benefits of data sharing. We believe that data assurance will help those creating, using or sharing data to assess, build and demonstrate trustworthiness in data and data practices.

The UK's NDS also acknowledges the importance of data assurance. It notes its role in making data useful and usable – with standards, 'leading to greater consistency, integrity and interoperability, and enabling data to be used widely and effectively across government' – as well as trustworthy. Without assurance sitting alongside transparency and standards within a 'robust ethical framework' which 'builds and maintains public trust in the government's use of data', the transformation in data use envisaged by the strategy will not be possible or sustainable.[12]

Assurance of business practices has existed for years, allowing businesses to demonstrate trustworthiness to investors, consumers and regulators. Assurance

[8] Frontier Economics for the Open Data Institute (2021), The economic impact of trust in data ecosystems
[9] https://www.gov.uk/government/publications/public-attitudes-to-data-and-ai-tracker-survey-wave-2
[10] Frontier Economics; CDEI
[11] https://www.gov.uk/government/publications/public-attitudes-to-data-and-ai-tracker-survey-wave-2
[12] Department for Digital, Culture, Media and Sport, gov.uk (2020) National Data Strategy

practices – such as audit, certification and accreditation – play an important role in the professionalisation and growth of the business world, allowing the development of new industries.

We anticipate that as data, and technologies that use data, become more important to the way the economy operates, the assurance of data and data practices will grow in significance. Data assurance is a new class of professional service which aims to improve and professionalise individual and organisational data practices. In doing so, it helps ensure that organisations and individuals can trust data as it flows across institutions and sectors.

2. The solution: assuring data to build trust

We define data assurance as:

> 'the process, or set of processes, that **increase confidence that data will meet a specific need**, and that organisations collecting, accessing, using and sharing data are doing so in trustworthy ways.'

Data assurance activities

There are two important aspects when considering assurance – the organisation creating the data, and the data itself.

There are many ways that organisations can assess, build and demonstrate trustworthiness to provide assurance around data and data practices. These include adopting ethical codes of practice, ensuring equity in who has access to data, and effective data management practices.

For the data itself, assurance relates to several factors including its quality, supply and ethics. When it comes to supply, users need to be assured that the data can flow securely from where it is stored to where it is used, with no impact on the quality of the data. When considering ethics, users need to be assured that the data is appropriately collected, used and shared. All of these factors can affect the confidence that data is fit for purpose and will meet user requirements. That means considering data assurance across the whole data lifecycle, from collection, to use, sharing and deletion.

Figure 1: The Data Lifecycle[13]

By assuring data and data practices, we can reduce risks when the data is being used and reused. These practices allow us to maximise the value that comes from using and sharing data. Data assurance also helps to address concerns that sharing data could cause damage to an organisation's reputation. It can support legal compliance, help to protect a market position and prevent harm to society, the economy and the environment.

Data assurance tools and practices can help to provide confidence that the data is trustworthy throughout its lifecycle. Organisations can take some of these steps themselves, like monitoring activities, publishing data policies, or building communities of practice. Others can be carried out by external people or organisations to provide assurance, such as auditing and certification. All of this helps to demonstrate and ensure trustworthy data practices.

As detailed in Table 1, data assurance activities can be applied to both *data and datasets*, and to the *data practices of an organisation.*

[13] RDMkit, Data lifecycle diagram

Table 1: What data and data practices can be assured?
You can provide assurance for several aspects of data and data practices, for example:

Data and datasets	**to improve confidence that:**	**by performing activities such as:**
	data is of trustworthy *provenance*	checking data to verify the sources, including those from third parties
	data meets ethical expectations or requirements	reviewing a dataset to ensure it meets the ethical principles as set by the organisation
	data is of appropriate *quality*	checking the dataset conforms to the specification
Data practices of an organisation	**to ensure:**	**by performing activities such as:**
	data is relevant and applicable for the intended use	ensuring those involved in data practices have the necessary skills and knowledge to work with data
	data is shared with the right people	assessing the data to ensure it is shared responsibly, legally and in ways that will minimise harms and maximise benefits
	there are no harmful impacts on people, organisations and communities who the data is about, or who are affected by use of the data	reviewing the lifecycle of how data is collected, managed and shared to confirm that data is managed legally, securely and ethically

Formal and informal data assurance

Data assurance activities can be classified based on how formally they are defined and applied.

More formal data assurance activities could include processes such as audits, certification or accreditation schemes. These would have to be supported by well-defined standards and involve multiple layers of review and assessment; not just of the process itself, but the people and organisations involved.

Less formal data assurance activities include developing and applying norms and principles that might help to guide and reinforce trustworthy behaviours. In some cases, their application may only be loosely defined and the results may not be verifiable.

Data assurance, AI assurance and regulation

As discussed in the previous section, regulations on data such as GDPR set the minimum standards that are acceptable in law, in this case regarding personal data which organisations must abide by. We believe that data assurance activities can help support regulatory goals like data protection and security, but can also enable organisations to fill any gaps currently in regulation, allowing them to build trust in data and data practices. A good example of this is data ethics, where currently there is no regulatory requirement or legislation for organisations to follow, however many wish to identify and manage ethical issues within their data practices.

It would be a mistake to see assurance – either internal or provided on a business-to-business (B2B) basis – as a replacement for robust regulation. We see the two as complementary, and (as discussed in Section 4) believe that regulation and regulators have a role to play in encouraging the uptake of assurance activities in the private sector.

We should also distinguish data assurance from **AI assurance**.

AI assurance is related to, but distinct from, data assurance. AI assurance is defined by the CDEI as services that 'help people to gain confidence in AI systems by evaluating and communicating reliable evidence about their trustworthiness.'[14]

Trusted data is required to feed predictive analytics, modelling, machine learning (ML) and AI systems to enable the creation of more sophisticated analyses and insights from data.

Data assurance is therefore a necessary condition for AI assurance: data is used to train and be used within AI systems, so AI assurance requires confidence that the data supplied is trustworthy and collected ethically and equitably. Beyond the assurance of the training and input data, AI assurance involves other elements such as assurance of the AI models used and the instructions that human operators provide to these models.

[14] Centre for Data Ethics and Innovation (2021), The roadmap to an effective AI assurance ecosystem

3. The opportunity: leading the world in data assurance

At the ODI, we believe that the greater adoption of data assurance practices should reassure organisations who want to share or re-use data. This will become increasingly vital as data, and data governance, becomes ever more central to the operating models of businesses, governments and the wider public sector, and the third sector.

In the context of growing domestic and international demand, we see an opportunity for the UK to leverage its existing strengths in professional services and develop credibility in data ethics and governance, enabling the UK to lead globally in data assurance.

Developing a reputation as a global centre for excellence in these areas would support wider government aspirations to deliver economic growth and establish the UK as a global data and digital services hub, as set out in the Plan for Growth and the Integrated Review respectively.[15] [16]

Data assurance service providers

Data assurance service providers are found across different sectors of the economy, and they vary in size. There is already involvement from established professional services firms such as KPMG, EY, PwC and Deloitte (sometimes referred to as the Big Four). These large professional services firms have started responding to opportunities in data assurance, and are increasingly offering data assurance services. One recent blogpost by KPMG argues that data assurance would be a 'game changer' for the professional services sector.[17]

Despite the activities of these large companies, the field is characterised by the presence of a high number of startups and challenger organisations demonstrating the nascency of the sector as a whole. In the UK, the majority of firms currently providing data assurance services were incorporated in the last 10 years and employ fewer than 10 people each. In addition to private sector firms, public bodies such as regulators will play a market-shaping role.

Research carried out for the ODI by Frontier Economics and glass.ai in 2021 found a nascent but buoyant market of UK business-to-business data assurance firms and services, with around 900 firms offering data assurance products and services in the

[15] HM Treasury (2021), Build Back Better: our plan for growth

[16] Cabinet Office (2021), Global Britain in a Competitive Age: the Integrated Review of Security, Defence, Development and Foreign Policy

[17] KPMG (2022), ESG Assurance will be a game changer

UK. More than half of these firms were incorporated in the previous 10 years, and new ones are currently being created at a rate of nearly 12% each year.[18] We expect this growth to continue as demand continues to rise both in the UK and globally.[19]

Data assurance users

It is likely that different types of data assurance will be relevant for different types of data assurance users. These end users include data holders, who hold and share data, and may require data assurance services to signal the trustworthiness of that data for its intended purposes, both internally and externally. It also includes data users, who may not hold data themselves but use third-party data and may require data assurance services to ensure the data is trustworthy.

Significant diversity will exist within each category of client. For example, data assurance for data holders formally publishing data on a one-to-many basis (for example, a government department publishing open data on its activities) might look quite different to those who are sharing data through bilateral channels (such as organisations with commercial agreements to share data with one another).

Different assurance practices are needed for different situations. Organisations coordinating data exchange among federated subsidiaries (such as a large conglomerate that wants to enable its component businesses to share data with each other) may need one method. Institutions sharing data with defined groups of data users (such as an academic institution aiming to provide data access to particular groups of affiliated researchers) may need a different method.

According to research commissioned by the ODI, confidence in data assurance products and services is strong. A majority (55%) of data holders and users believe data assurance can improve data quality and minimise risks associated with sharing data, and nearly all (94%) of surveyed organisations using data assurance products or services believed that their organisation's trustworthiness benefited as a result.[20]

Despite this, the adoption of data assurance is uneven and remains low. The sectors in which uptake of data assurance products or services is highest include the information technology sector (in which 18% of companies report using data assurance products or services); the manufacturing, engineering and construction sectors (8–11% and the finance sector (9%).[21]

A growing global sector

According to research carried out for the ODI, the data assurance market for external data flows is projected to grow from £1.86bn in 2021 to £7.31bn by 2025. We

[18] Frontier Economics (2021) Review of the UK business to business data assurance market

[19] ibid.

[20] Additional research for the ODI, Metia (2022)

[21] ibid.

anticipate growth across three sectors in particular: financial services and insurance; pharmaceuticals and healthcare; and energy and climate change.[22]

We also expect the sector to diversify and change alongside evolving legal, regulatory and technical requirements. Two-thirds of data holders and users say that the existing landscape of data assurance products and services doesn't meet their needs, and significant numbers regard currently-available solutions as too rigid and one-size-fits-all.

ODI research suggests that the current gaps in the market are services aimed at assuring data quality and supporting data management and governance, as well as compliance with major regulations like GDPR.[23] Cultivating new services in these areas could offer a growth opportunity for UK companies, although we anticipate that the UK's planned divergence from the GDPR could harm the positioning of UK companies in this regard.

[22] ibid.

[23] ibid.

4. The challenge: considerations for policymakers

While prospects for the data assurance sector seem strong, we believe that downstream barriers and market failures might prevent the UK from capturing the full benefits of a booming data assurance sector. If this is the case, then government or regulatory intervention might be necessary to unlock the considerable economic opportunities associated with the growth of data assurance.

We think that policymakers ought to consider measures falling into three categories:

- Supporting the wider data assurance ecosystem
- Driving and directing the growth of the data assurance sector
- Leading by example in adopting and carrying out data assurance activities

Supporting the wider ecosystem

The UK's wider data assurance ecosystem extends to actors beyond data holders, data users and data assurance providers. This wider ecosystem includes the following:

- **Government and regulators** who are responsible for producing policies, legislative frameworks, guidance and tools that shape how data is accessed, used and shared
- **Standards development organisations, including open standards** such as the British Standards Institution, Office for Product Safety and Standards, National Physical Laboratory, the Open Standards Board, the Open Geospatial Consortium and the United Kingdom Accreditation Service, which is responsible for developing and maintaining standards, including:
    - standards that describe how a product or service should operate (core standards)
    - the standard processes by which a data-enabled product or service might be certified against that standard
    - standard training and assessments that are used to accredit organisations to complete these certifications.
- **Researchers and advocacy organisations** who can help to spot emerging trends and support dialogue between industry, government and other stakeholders.

The government and regulators should support the development of this wider ecosystem, helping to convene and support organisations where appropriate and ensuring the right skills are present in the UK to support standards development and the delivery of assurance services.

Driving and directing growth

While demand for data assurance remains buoyant, the growth of the sector is unlikely to follow a smooth and consistent trajectory in the medium to long term. There might be a need to stimulate demand, which could take the form of mandating specific formal types of assurance (for example certification against agreed standards).

This is likely to be particularly true for particular sub-sectors and use cases. In most sectors, companies will often have a direct interest in ensuring that the data they use is appropriate and trustworthy. Using poor quality or unreliable data could impact the effectiveness of company decision-making, harming profitability. In some cases, the incentives will work the other way: for instance, if the data in question is used to support judgements on company performance. In these cases, there may be an incentive to downplay or minimise the extent of such activities. Demand, and therefore growth, might be lower for data assurance services provided to these sectors.

Driving growth could also mean addressing the associated costs. A report by the Climate Risk Disclosure Lab at Duke University published in 2021 found that most companies expected audit and assurance services to be the main cost driver associated with the introduction of new environmental disclosure requirements. Reducing the cost of assurance – whether by subsidising it or by ensuring the required skills are readily available – could help to further drive the development of the sector.

Leading by example

Government bodies and regulators can lead by example, both through the adoption and delivery of data assurance activities. Governments and regulators collect and hold significant quantities of data, and so by procuring data assurance services they can signal confidence in those services and support the process of mainstreaming them.

Government and regulators can also facilitate the setting of best practices and publication of guidance (which parts of government, such as the Central Digital and Data Office, Data Standards Authority and Government Data Quality Hub, are already doing), or the integration of data assurance into their existing compliance and regulatory activities. To drive adherence to these best practices, regulators could collaborate with industry or professional bodies to offer certification schemes or to accredit other organisations to do so.

The UK's leading role in international standard setting on data

Global Britain in a Competitive Age, the UK government's 'Integrated Review' which sets out its foreign policy vision, highlights the importance of 'regulatory diplomacy' in pursuing the UK's national interest. This involves shaping standards, norms and regulations in areas that will underpin the global economy – especially in areas like emerging technologies, cyber and data. A 2022 report by the House of Commons Foreign Affairs Committee considered that technology standards 'have become a tool for geopolitical competition'.

The UK has a long track record of leadership in this area. The select committee calls the UK's influence over rule-making and standard-setting one of its 'main global strengths'. The UK was a founding member of longstanding international standards organisations like the International Organisation for Standardization and International Electrotechnical Commission). But it has also been at the forefront of setting standards in emerging areas, such as AI: the UK was a founding member of the Global Partnership for AI, helped shape the Organisation for Economic Co-operation and Development's principles on AI (adopted by the G20 and forming the basis for UNESCO's principles) and actively engages with crucial initiatives like the UN Secretary-General's High-Level Panel on Digital Cooperation.

Activity in areas such as AI builds on the UK's existing reputation in data and statistics. The Office for National Statistics, for instance, is one of the world's most respected statistics agencies and supports countries around the globe in its work.

Next steps

The ODI knows that data can help unlock huge value for the economy, society, and the environment by improving public services and increasing efficiency and effectiveness in business, and that data needs to be trusted and trustworthy to support growth and innovation.

To tackle some of the biggest challenges of our time, like climate change, data must flow across organisations, sectors and countries. By failing to share and re-use data we are missing opportunities to capitalise on the social, economic and environmental value that could be gained through greater trust in data, data flows and organisations.

We believe that data assurance will help organisations and individuals creating, using or sharing data to assess, build and demonstrate trustworthiness in data and data practices. We continue to work with partners, stakeholders and collaborators to explore this important and rapidly developing area in managing global data infrastructure.

The ODI's future work will include the following:

- Continuing with research to assess the need for data assurance, and working on public policy advice and initiatives to enable as many people as possible to benefit from the value of data sharing
- Creating a code of conduct and tools, to support those that are working to assure both data and the organisations sharing and using it
- Developing guidance for data assurance. In time, the ODI will enable the development of certification and accreditation services to support data assurance codes of conduct and standards
- Convening a steering board across government, regulators, not-for-profit organisations and industry to support the strategic direction of this work, specifically to determine which sectors and use cases will deliver the greatest benefit from the development and adoption of standards to support the trusted flow of data across the ecosystem. Our initial research suggests these would include healthcare, energy and finance (in addition to environmental performance)

Through its current work on data assurance, the ODI aims to provide support and direction for informal data assurance activities, including proposing norms and principles that help guide and reinforce trustworthy behaviours. This is filling the current gap in providing guidance and direction for organisations to build trust in their data practices and datasets.

As this work develops, we at the ODI are interested in working with key stakeholders to develop more formal data assurance processes, including the development of well-defined data assurance standards and certification processes to build a trustworthy data ecosystem.

You can get in touch with us by emailing the ODI's Policy team at policy@theodi.org

Annexe: further resources

Our work around data assurance to date has included:

- Introducing the topics of data assurance and trust through a series of blogposts, explainers and videos
    - Building trust through data assurance (video explainer)
    - How does data assurance increase confidence in data?
    - Assurance, trust, confidence – what does it all mean for data?
    - Trust in data is about more than ethics
    - Regulators, industry bodies and professional bodies: their role in data assurance
    - Demonstrating and assessing trustworthiness when sharing data (report)
- Work around greenwashing and the need for confidence in environmental performance data:
    - Tackling greenwashing through data assurance project and report
    - Data and the climate crisis (video explainer)
    - Our partnership with London Stock Exchange Group (LSEG) to develop a sustainable ecosystem of ESG data
- Working with clients and developing open tools that are at the start of the journey in providing data assurance across sectors and use cases
    - Open Data Certificates
    - Data Ethics Canvas
    - Data Skills Framework
    - Data Ethics Maturity Model
    - Trustworthy Data Stewardship Guidebook
    - Data Landscape Playbook
    - Data Ecosystem Mapping tool
    - Open Data Maturity Model
    - Mapping data ecosystems: methodology
- Sharing tools and guidance for business leaders to making building trust with data is part of both strategic planning and everyday data operations
    - ODI Inside Business: Build a brand that is trusted with data – a checklist for leaders
    - Why leaders should care how their organisation collects, accesses, uses and shares data
    - How leaders can develop a data strategy that addresses global challenges
    - Practical tools and techniques for building a brand that is trusted with data (webinar)
- Creating sector-specific guidance on data assurance
    - Health data governance: a playbook for non-technical leaders
- Commissioning a report on the economic value of trust in data ecosystems
    - The economic impact of trust in data ecosystems – Frontier Economics for the ODI (report)

- Developing case studies that demonstrate the importance of data assurance to businesses
    - TomTom – Data assurance is 'critical for us, and it's so difficult to do'
    - Helping Barclays build trust through data ethics
- Hosting events, panels, podcasts and discussions where we've explored data assurance and trust
    - ODI Canalside Chat: Data sharing and the need for new business models (video)
    - ODI Canalside Chat: Why embedding ethical data practices could make or break your bottom line (video)
    - Data Decade: Responsible use of data (podcast)
    - Data Decade: Trust and misinformation (podcast)
    - Data Decade: Data and public policy (podcast)
    - ODI Inside Business: The role of data literacy in building a trusted brand (podcast)
    - ODI Inside Business: Why poor data governance could be a director's undoing (podcast)
    - ODI Summit 2021: Our world transformed: Who's looking after the data? (video)
    - ODI Summit 2021: Will data ethics ever be part of an organisation's DNA?
- Engaging with government consultations related to data assurance
    - Update to Green Finance Strategy: call for evidence
    - The ODI submits evidence to the parliamentary inquiry on public sector health data practices
    - The ODI responds to the UK government's consultation on proposed reforms to artificial intelligence and intellectual property
    - The ODI responds to the UK government's consultation on proposed reforms to data protection
    - The ODI responds to the UK government's restoring trust in audit and corporate governance consultation

You can find out more about the ODI's data assurance work: Data assurance: Building trust in data

Glossary

Assurance: the process, or set of processes, that show evidence that something is reliable or trustworthy.

AI assurance: the process, or set of processes, that increase confidence that AI systems work as they are supposed to work, and that they are effective, trustworthy and legal.

Data assurance: the process, or set of processes, that increase confidence that data will meet a specific need, and that organisations collecting, accessing, using and sharing data are doing so in trustworthy ways.

Data assurance activity: a specific activity to create trust in data, such as conducting an audit, validating a dataset, or carrying out training.

Data assurance scheme: a specific project that works by applying one or more data assurance activities and may involve multiple actors.

Data ecosystem: the people, communities, and organisations that are stewarding data, creating things from it, deciding what to do based on it, influencing any of those activities, or are affected by any of those activities.

Data governance: a framework for ensuring the overall integrity, availability, usability, and security of data in an organisation

Data infrastructure: is made up of data assets, standards, technologies, policies and the organisations that steward and contribute to them

Data practices: the processes by which data is collected, shared, held and/or managed.

Disclosure: the action of publishing information about a company's activities, financial performance, exposure to risks and other aspects relevant to its operations and current and future performance.

Quality infrastructure: formal mechanisms of assurance such as standardisation, conformity assessment, measurement or accreditation.

Standards: documented, reusable agreements that solve a specific set of problems or meet clearly defined needs. Data standards are often used to help define or support a data assurance activity.

Trustworthy data ecosystem: an environment in which individuals and organisations across the public, private and third sector trust that data is flowing in ways that will maximise benefits whilst minimising harms.