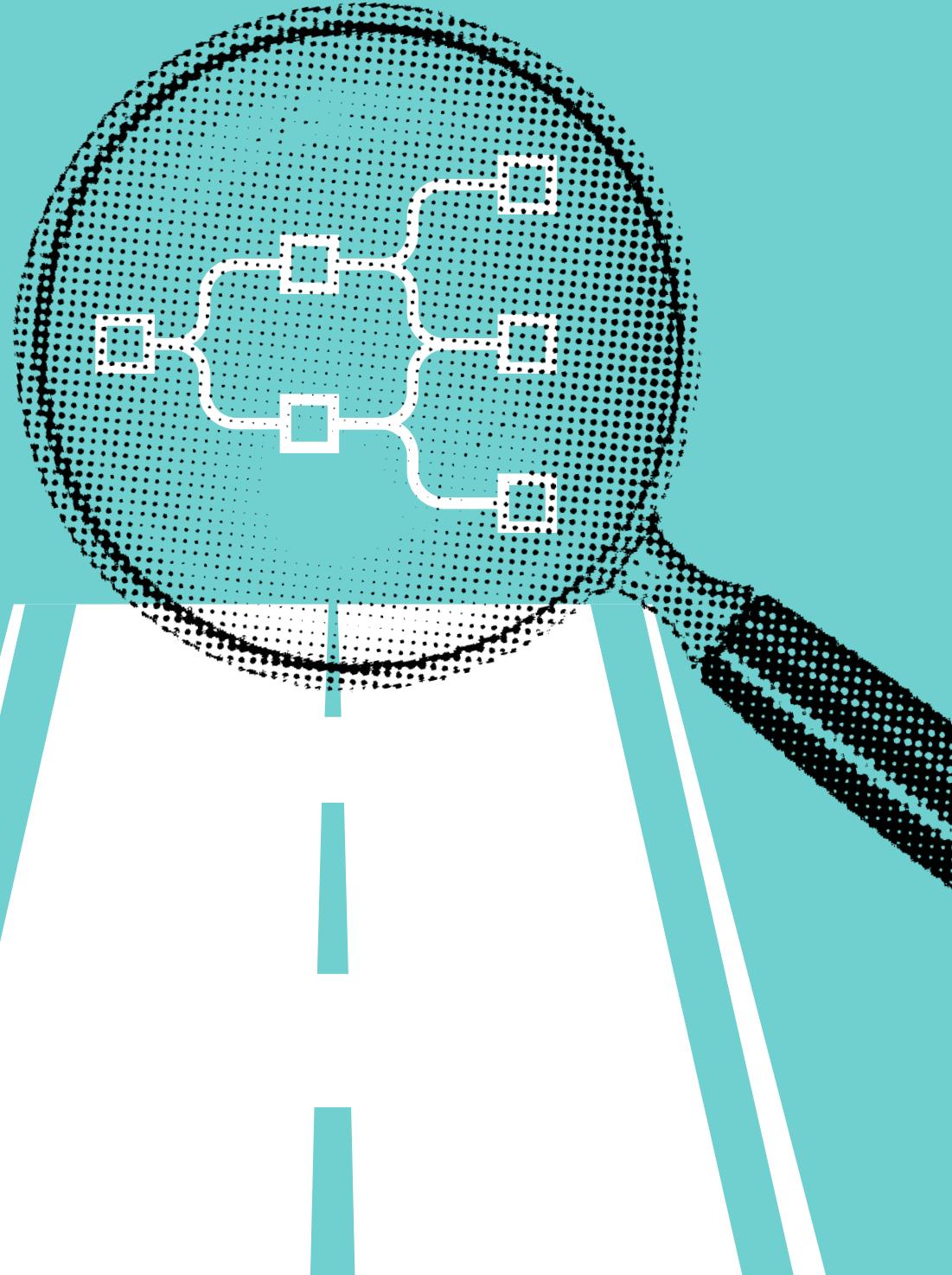


# The roadmap to an effective AI assurance ecosystem

December 2021



# Ministerial foreword



Chris Philp MP

**Artificial intelligence (AI) is one of the game-changing developments of this century. From powering innovative businesses of all sizes across the length and breadth of the UK, to enabling trailblazing research into some of the greatest societal challenges of our time, AI offers a world of transformative potential. As AI becomes an ever more important driver of economic and social progress, we need our governance approaches to keep up. Getting governance right will create the trust that will drive AI adoption and unlock its full potential. As we announced in the National AI Strategy, the UK intends to establish 'the most trusted and pro-innovation system for AI governance in the world'.**

**AI assurance will become a significant economic activity in its own right, with the potential for the UK to be a global leader in a new multi-billion pound industry.**

Our Plan for Digital Regulation sets out how well-designed regulation can drive growth and shape a thriving digital economy and society, whereas poorly-designed or restrictive regulation can dampen innovation. We will also need those building, deploying and using AI to have the information and means to ensure these technologies are used in ways that are effective, safe and fair, as a market-based complement to more formal regulation.

A critical building block of our approach will be the promotion of a strong ecosystem of tools and services to assure that AI systems work as they are supposed to. A similar approach to auditing or 'kitemarking' in other sectors will be needed to enable businesses, consumers and regulators to know whether the AI systems are effective, trustworthy and legal. As a first step towards this goal, the National AI Strategy committed to the publication of the Centre for Data Ethics and Innovation's (CDEI) AI assurance ecosystem roadmap.

This roadmap will help the UK to grow this ecosystem. The first publication of its kind, the roadmap sets out the steps needed to grow a mature, world-class AI assurance industry. AI assurance services will become a key part of the toolkit available to ensure effective, pro-innovation governance of AI. The forthcoming White Paper on the governance and regulation of AI will highlight

the role of assurance both as a market-based means of managing AI risks, and as a complement to regulation. This will empower industry to ensure that AI systems meet their regulatory obligations.

Building on the UK's strengths in the professional services and technology sectors, AI assurance will also become a significant economic activity in its own right, with the potential for the UK to be a global leader in a new multi-billion pound industry. A flourishing AI assurance ecosystem will also support a proportionate, pro-innovation AI governance regime, cementing the UK's place on the world stage and enabling us to develop a competitive advantage over other jurisdictions on AI.

The roadmap sets out the vision for what the whole UK AI ecosystem must do to give companies the confidence to invest and earn the justified trust of society. The opportunities are there - now we must seize them.

A handwritten signature in black ink, appearing to read "Chris Philp MP".

**Chris Philp MP,  
Minister for Tech and the Digital Economy**

# The roadmap to an effective AI assurance ecosystem

**Artificial intelligence (AI) offers transformative opportunities for the economy and society, but these benefits will only be realised if organisations, users and citizens can trust AI systems and how they are used.**

AI has the potential to bring substantial benefits to society and the economy. PwC estimates that AI will add 10.3% to UK GDP over 2017 to 2030.<sup>1</sup> While this aggregate figure doesn't account for the distributional or downstream impacts of AI adoption, it is clear that AI presents significant opportunities. AI has already been harnessed to achieve scientific breakthroughs<sup>2</sup> and holds promise in other sectors too, for example, operating an efficient and resilient green energy grid<sup>3</sup> and tackling misinformation<sup>4</sup> on social media platforms.

However, to unlock these benefits, trust in AI systems, and how they are used, is vital. Without this trust, organisations can be reluctant to invest in AI, because of concerns over whether these systems will work as intended (i.e. whether they are effective, accurate, reliable, or safe). Or alternatively, if organisations adopt AI systems without understanding whether they are in fact trustworthy, they risk causing real-world harm. In the CDEI's recent business innovation survey, over a fifth of organisations who are currently non-users of AI, but plan to introduce it, flagged uncertainty about regulation and legal responsibility as a barrier to adoption.<sup>5</sup>

Without trust, consumers and citizens will also be reluctant to accept AI and data-driven products and services, or to share the data that is needed to build them. Research commissioned by the Open Data Institute (ODI) demonstrated how improved public trust is associated with increased data sharing.<sup>6</sup> Without consumer trust, organisations are even more reluctant to adopt AI for fear of public or consumer backlash.

Recognising the importance of trust in the responsible adoption of AI, in its recent National AI Strategy, the UK government set out its ambition to be "the most trusted and pro-innovation system for AI governance in the world."<sup>7</sup>

To realise this ambition, a range of actors, including regulators, developers, executives, and frontline users, need to understand and communicate whether AI systems are trustworthy and compliant with regulation. AI assurance services which address this need will play a critical role in building and maintaining trust as AI becomes increasingly adopted across the economy.

AI assurance will be crucial to building an agile, world-leading approach to AI governance in the UK. AI assurance provides a toolbox of mechanisms to monitor and demonstrate regulatory compliance, as well as support organisations to innovate responsibly, in line with emerging best practices and consensus-based standards.

1 'The economic impact of artificial intelligence on the UK economy', PwC, June 2017; <https://www.pwc.co.uk/economic-services/assets/ai-uk-report-v2.pdf>

2 'AlphaFold: a solution to a 50-year grand challenge in biology', DeepMind, November 2020; <https://deepmind.com/blog/article/alphafold-a-solution-to-a-50-year-old-grand-challenge-in-biology>

3 'Why artificial intelligence is key to renewable energy grid resilience', World Economic Forum, March 2021; <https://www.weforum.org/agenda/2021/03/artificial-intelligence-is-key-to-grid-resilience/>

4 'The role of AI in addressing misinformation on social media platforms', Centre for Data Ethics and Innovation, August 2021; <https://www.gov.uk/government/publications/the-role-of-ai-in-addressing-misinformation-on-social-media-platforms>

5 'CDEI 2021 Business Innovation Survey Exploratory Analysis', Centre for Data Ethics and Innovation, Forthcoming

6 'Economic Impact of Trust In Data Ecosystems - Report prepared for the ODI', Frontier Economics, February 2021; <https://theodi.org/article/the-economic-impact-of-trust-in-data-ecosystems-frontier-economics-for-the-odi-report/>

7 'National AI Strategy', Office for Artificial Intelligence (OAI), September 2021; <https://www.gov.uk/government/publications/national-ai-strategy/national-ai-strategy-html-version>

## The vision for AI assurance



Our vision is that the UK will have a thriving and effective AI assurance ecosystem within the next 5 years. Strong, existing professional services firms, alongside innovative start-ups and scale ups, will provide a range of services to build justified trust in AI.



These services, along with public sector assurance bodies, will independently verify the trustworthiness of AI systems - whether they do what they claim, in the way they claim. This new growing industry could be worth multiple billions to the UK economy if it follows the progress of the UK cyber security industry.



By providing reliable information about the trustworthiness of AI systems, the AI assurance industry will also support adoption of AI and enable its full potential to be realised across the economy.

## AI assurance provides the tools to build trust and ensure trustworthy adoption

Assurance is about building confidence or trust in something, for example a system or process, documentation, a product or an organisation.

Assurance services help people to gain confidence in AI systems by evaluating and communicating reliable evidence about their trustworthiness.

Similar challenges occur in other domains, including financial reporting, product safety, quality management and cyber security. In those areas, ecosystems of independent assurance providers offering services such as audits, impact assessments and certification have emerged to address these challenges, supported by standards, regulation and accreditation of assurance providers.

These assurance services provide the basis for consumers to trust that the products they buy are safe, and the confidence for industry to invest in new products and services. In the food industry, safety and nutrition standards and product labelling ensure that consumers can purchase food in the supermarket, secure in the knowledge that it's safe to eat. In technologically complex industries, such as medical technology and aviation, quality assurance throughout the supply chain prevents accidents which could have fatal consequences. This ensures people are confident to adopt these technologies, to perform important surgeries and fly on aeroplanes.



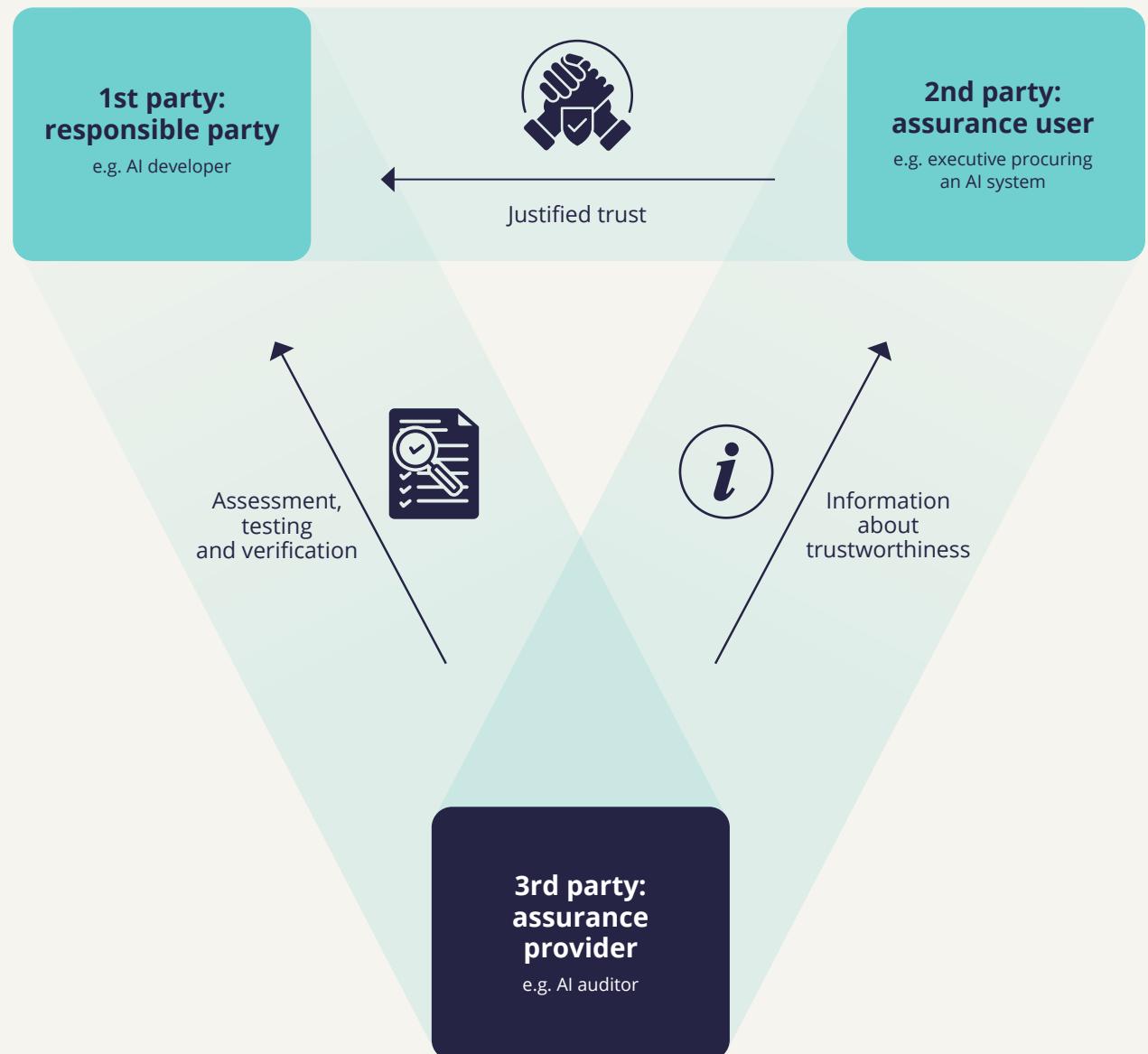
## To provide meaningful and reliable assurance for AI, organisations need to overcome:

- **An information problem:** reliably evaluate evidence to assess whether an AI system is trustworthy.
- **A communication problem:** communicate the evidence at the right level, to inform assurance users' views on whether to trust an AI system.

Assurance helps to overcome both of these problems to enable trust and trustworthiness.<sup>8</sup>

By performing this function, assurance services can help to justify the level of trust people have in AI systems, as shown right.

## The role of assurance in building justified trust in AI systems



<sup>8</sup> 'A Question of Trust - The BBC Reith Lectures, Onora O'Neill, June 2002; <https://www.cambridge.org/gb/academic/subjects/philosophy/political-philosophy/question-trust-bbc-reith-lectures-2002?format=PB&isbn=9780521529969>

## The UK is well placed to play a leading role in AI assurance

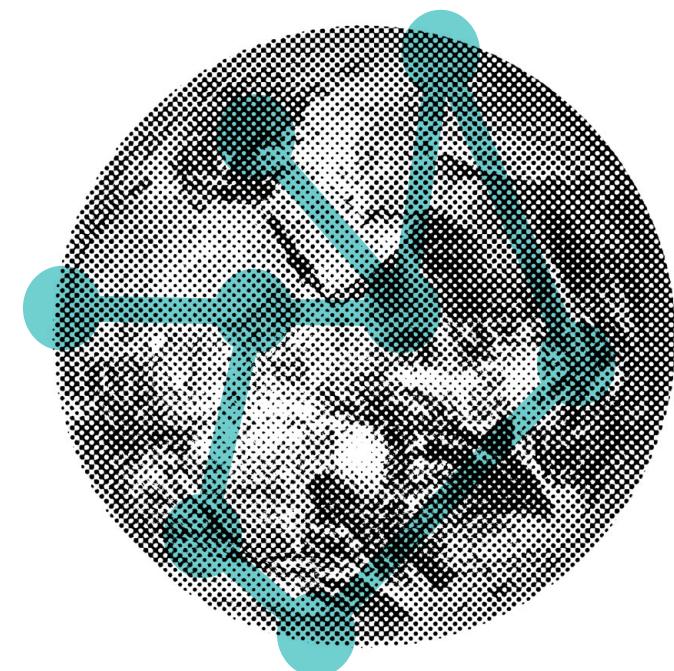
There is an opportunity for the UK to lead by example and influence the development of AI assurance internationally. Assurance techniques and best practices developed for the UK market can be exported to support trustworthy innovation in growing international markets, facilitating trade and industry cooperation. The UK has played similar leading roles in the development of other assurance ecosystems, including cyber security and risk management, where the current International Organisation for Standardisation (ISO)/International Electrotechnical Commission (IEC) 27001 cyber security standards<sup>9</sup> and ISO 9001 quality management standards were developed from originally British standards.<sup>10</sup>

This leadership has also led to the creation of new industries and professions. The UK's cyber security industry, which is an example of a mature assurance ecosystem, employed 43,000 full-time workers in 2019, and contributed nearly £4 billion to the UK economy.<sup>11</sup> As the use of AI systems proliferates across the economy, there is an opportunity to develop an AI assurance ecosystem which will address risks, unlock growth and create new job opportunities in a similar way.

UK regulators also have a strong track record of pioneering regulation to enable responsible innovation, putting them in a strong position to facilitate the development and adoption of AI across the economy. For example, the Financial Conduct Authority (FCA) has helped to foster a new ecosystem of fintech start-ups in the Open Banking ecosystem,<sup>12</sup> and the Medicines and Healthcare Products Regulatory Agency (MHRA) has enabled the development and use of emerging technologies in healthcare, through their medical device regulation.<sup>13</sup>

Building an effective AI assurance ecosystem is a critical part of addressing the ethical and governance challenges of AI and enabling responsible adoption. Organisations developing and deploying AI will increasingly rely on a market of independent assurance providers to assess and manage AI risks, and to demonstrate and monitor regulatory compliance. Playing this crucial enabling role, AI assurance is set to become a significant economic activity in its own right and is an area in which the UK is well positioned to excel, drawing on strengths in legal and professional services.

The market for AI assurance is already starting to grow in the UK and worldwide, with a range of actors beginning to offer assurance services. However, it is still early days, and action is needed to shape this ecosystem into one that brings together the right mix of interdisciplinary skills and technical approaches, and provides the right incentives to enable organisations to manage AI risks effectively.



9 'ISO/IEC27001 Information Security Management', International Organisation for Standardisation / International Electrotechnical Commission (ISO/IEC), 2005 (revised 2013); <https://www.iso.org/isoiec-27001-information-security.html>

10 'ISO9001 Quality Management Systems - Requirements', International Organisation for Standardisation (ISO), 1987 (revised 2015); <https://www.iso.org/standard/62085.html>

11 'UK Cyber Security Sectoral Analysis 2020 - Report for DCMS', Ipsos Mori, Perspective Economics, Centre for Secure Information Technologies, January 2020; [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/957960/UK\\_Cyber\\_Sectoral\\_Analysis\\_2020\\_Report\\_V2.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/957960/UK_Cyber_Sectoral_Analysis_2020_Report_V2.pdf)

12 'What Is Open Banking?', Open Banking; <https://www.openbanking.org.uk/what-is-open-banking/>

13 'The Medical Devices Regulation 2002', Medicines and Healthcare Products Regulatory Agency, 2002; <https://www.legislation.gov.uk/uksi/2002/618/contents/made>

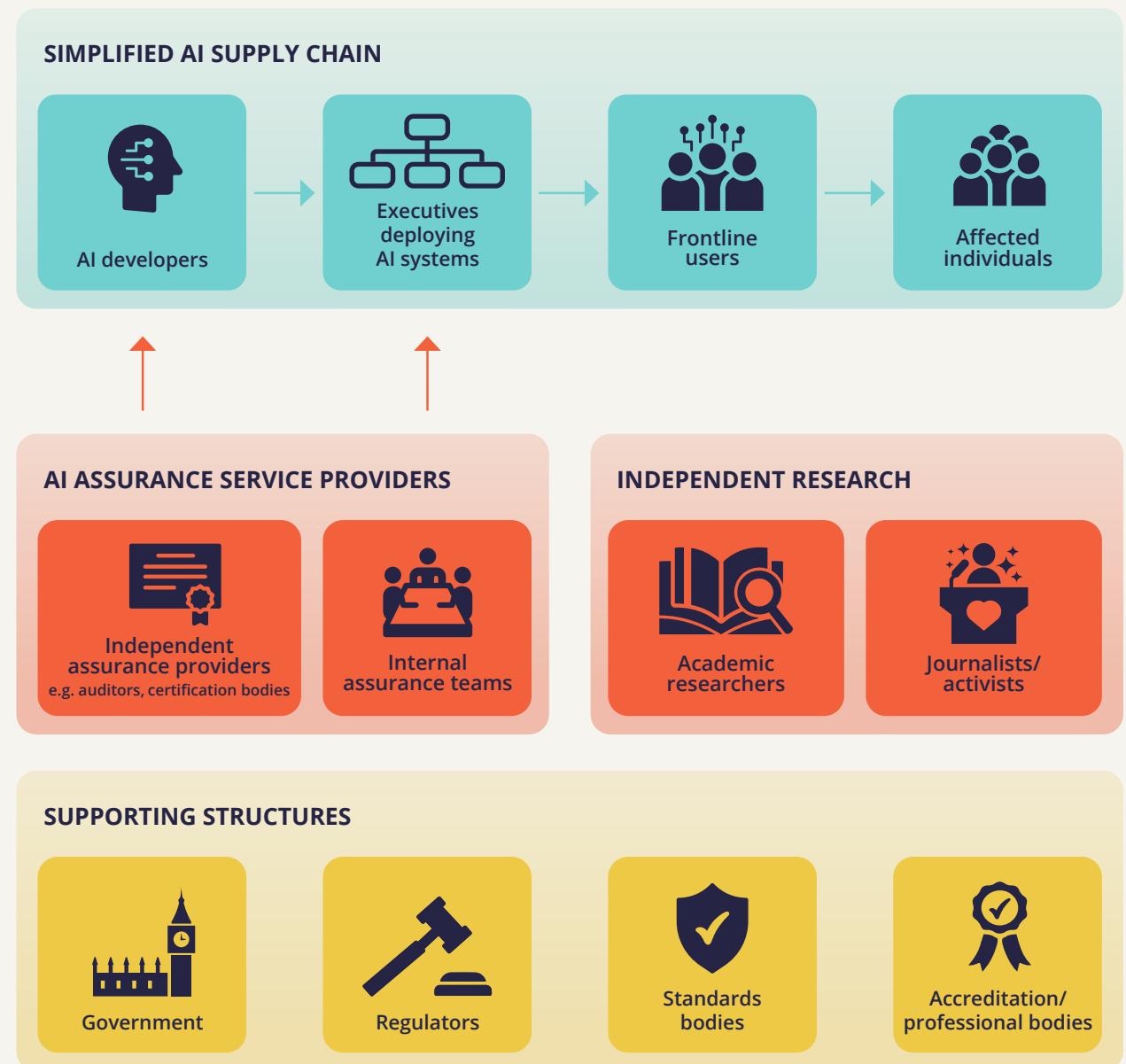
This roadmap aims to make a significant, early contribution to shaping and bringing coherence to this ecosystem. It sets out the roles that different groups will need to play, and the steps they will need to take, to move to a more mature ecosystem.

## Towards an effective and mature AI assurance ecosystem

While the right ingredients to develop an effective AI assurance ecosystem are available, current efforts are fragmented. For the ecosystem to mature effectively, in a way that supports innovation whilst mitigating risks and societal harms, a coordinated effort is required between different actors in the ecosystem. The diagram right highlights four important groups of actors who will need to play a role in the AI assurance ecosystem.

This simplified diagram highlights the main roles of these four important groups of actors in the AI assurance ecosystem. However, while the primary goal of the ‘supporting structures’ is to set out the requirements for trustworthy AI through regulation, standards or guidance, these actors can also provide assurance services via advisory, audit and certification functions e.g. the Information Commissioner’s Office’s (ICO) investigation and assurance teams assess the compliance of organisations using AI.<sup>14</sup>

## Key actors in the AI assurance ecosystem



14 ‘Assurance’, The Information Commissioner’s Office (ICO); <https://ico.org.uk/about-the-ico/jobs/departments/good-practice-audit/>

Drawing on desk-research, pilot projects and expert engagement, the CDEI have identified six priority areas for developing an effective, mature AI assurance ecosystem:

**1. Demand for AI assurance:** The AI supply chain will need to demand, and receive, reliable evidence about the risks of these technologies, so they can make responsible adoption decisions.

There are a range of issues that need to be considered by those who build, deploy or use AI systems, to ensure that they are trustworthy. For example, is an AI system robust? Is it compliant with relevant regulations? Is it accurate and free from unacceptable bias? What are the privacy and

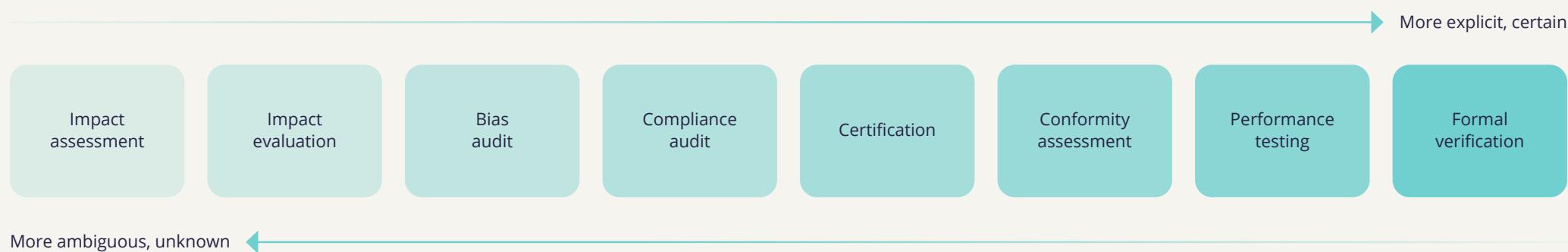
security risks? What governance and risk management processes are in place? Is a third party needed to perform specialist testing, or independent validation?

Demand for AI assurance services is starting to emerge. Public concern about the potential risks of AI deployment has driven organisations to consider the reputational risks of using AI. To ensure their use of AI systems is trustworthy, organisations need to recognise this concern and respond by proactively addressing and managing AI risks. Achieving trustworthiness will require actors in the AI supply chain to develop a clear understanding of relevant AI risks and their accountabilities for mitigating these risks.

**2. An AI assurance market:** A competitive, dynamic, market of service providers is needed to provide the tools and services to create this reliable evidence in an efficient and effective way.

There is no silver bullet to AI assurance, the trustworthiness of an AI system will need to be evaluated and communicated in very different ways depending on the type of risk and specific application. To assure AI systems effectively, a toolbox of different products, services and standards is required, suited to assessing these different aspects. Our AI assurance guide, published alongside this roadmap, examines different assurance mechanisms and sets out how they can be effectively applied in practice.<sup>15</sup>

### The spectrum of mechanisms for assuring AI systems



<sup>15</sup> 'The CDEI's AI assurance guide', Centre for Data Ethics and Innovation, December 2021; forthcoming

A market is already emerging to respond to demand for AI assurance, with established large companies and specialist start-ups beginning to offer AI assurance services around topics including algorithmic bias, robustness and data protection. A trustworthy market of assurance providers is needed to provide specialist skills for AI assurance and independent oversight to ensure incentives for responsible innovation are aligned appropriately in the AI supply chain.

This market is supported by a range of toolkits and techniques for assuring AI. However, this market is currently fragmented, with little common understanding about what topics AI systems need to be assured for, and what standards they need to be assured against. There is an exciting opportunity to accelerate growth to the ecosystem and in turn facilitate increased adoption of responsible AI by building common understanding, ensuring the development of the full range of assurance tools and incentivising value-adding assurance practices.

**3. Standards:** Different kinds of standards are needed to build common language and scalable assessment techniques.

Standards have an important role to play. In most mature assurance ecosystems, a mix of industry-led (technical) and regulatory standards define the agreed basis for assurance, allowing actors throughout the supply chain to understand what has been assured. There are many ongoing standardisation efforts for AI, which is positive, however a degree of consolidation and focus is needed. The UK's National AI strategy set out the government's existing work on global digital technical standards in this area, and plans to expand the UK's international engagement and thought leadership.<sup>16</sup>

The highest priority areas for AI standards to support AI assurance are AI management system and risk management standards which establish good practices that organisations can be certified against, and a range of measurement standards, which will build consensus and common understanding about measuring AI risk and performance.

**4. Professionalisation:** The governance and incentives for assurance service providers need to be trusted.

Customers of assurance services often need a means to determine the quality of an assurance service. Building a trusted and trustworthy ecosystem of assurance providers will therefore rely on the professionalisation of AI assurance.

Accreditation comes in a number of forms, from accrediting assurance service providers or individual assurance practitioners to recognise expertise, integrity and good practice, to accrediting specific services such as certification schemes. Accreditation schemes build trust in the ecosystem by 'checking the checkers' to ensure those providing assurance services are competent to do so.

In other contexts, models such as accreditation and chartered professions deliver this trust. It is too early to tell which of these models is right for AI assurance, but initial steps will need to be taken to build an AI assurance profession.

16 'National AI Strategy', Office for Artificial Intelligence (OAI), September 2021; <https://www.gov.uk/government/publications/national-ai-strategy/national-ai-strategy-html-version>

**5. Regulation:** Beyond auditing and inspecting AI as part of their enforcement activity, regulators will play an important role in supporting the development of the broader AI assurance ecosystem. Regulation can help to enable assurance, by setting assurable requirements that enable organisations to manage their regulatory obligations. Assurance also helps regulators to achieve their objectives by empowering users of AI to achieve compliance and manage risk.

UK regulators have the opportunity to drive demand for assurance and shape the development of AI assurance techniques and processes within their remits. Indeed some UK regulators are already setting a leading example in addressing AI risks via assurance methods.

Regulation can help to enable assurance, by setting assurable requirements that enable organisations to manage their regulatory obligations.



## Example regulatory initiatives for AI assurance



The ICO is currently developing an AI Auditing Framework (AIAF), which has three distinct outputs.<sup>17</sup> The first is a set of tools and procedures for their assurance and investigation teams to use when assessing the compliance of organisations using AI. The second is detailed guidance on AI and data protection for organisations.<sup>18</sup> The third is an AI and data protection toolkit designed to provide further practical support to organisations auditing the compliance of their own AI systems.<sup>19</sup>



The ICO has also published guidance with The Alan Turing Institute on explaining decisions made with AI, which gives practical advice to help organisations explain the processes, services and decisions delivered or assisted by AI, to the individuals affected by them.<sup>20</sup>



The MHRA has developed an extensive work programme to update regulations applying to software and AI as a medical device. The reforms offer guidance for assurance processes and on how to interpret regulatory requirements to demonstrate conformity.<sup>21</sup>

The AI assurance landscape is also influenced by international trade. International trade of AI technologies will be a significant benefit to the UK economy, and therefore, ensuring regulatory compliance and interoperability across borders will be crucial to enabling trade.

As an example, in 2021 the European Commission published its draft Artificial Intelligence Act which sets out a risk based framework for regulating AI systems.<sup>22</sup> Ensuring cross-border trade in AI will require a well-developed ecosystem of AI assurance approaches and tools to ensure

that UK AI services can also demonstrate risk management and compliance in ways that are understood by trading partners.

**6. Independent research:** In addition to specialised assurance providers, standards, regulatory, industry and professional bodies, other independent actors can offer important services to the assurance ecosystem.

Independent researchers are already playing a significant role in the development of assurance techniques and measurements.<sup>23</sup>

However, organisations developing and deploying AI systems could more directly partner with external researchers to both identify and mitigate AI risks. This will involve incentivising both researchers and organisations to provide access to the relevant systems. The CDEI hopes to see the approach here building on the lessons learnt in cyber security, where clear good practice has emerged for organisations dealing responsibly with independent security researchers, with clear mechanisms for responsible disclosure of security flaws and even bug bounties.<sup>24 25</sup>

<sup>17</sup> 'The CDEI's AI assurance guide', Centre for Data Ethics and Innovation, December 2021; <https://cdeiu.github.io/ai-assurance-guide/>

<sup>18</sup> 'Guidance on the AI auditing framework - Draft guidance for consultation', Information Commissioner's Office (ICO), February 2020; <https://ico.org.uk/media/2617219/guidance-on-the-ai-auditing-framework-draft-for-consultation.pdf>

<sup>19</sup> 'AI and Data Protection Risk Toolkit', Information Commissioner's Office, July 2021; <https://ico.org.uk/about-the-ico/news-and-events/blog-new-toolkit-launched-to-help-organisations-using-ai/>

<sup>20</sup> 'Explaining decisions made with AI', Information Commissioner's Office (ICO), The Alan Turing Institute, May 2020; <https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/explaining-decisions-made-with-ai/>

<sup>21</sup> 'Transforming the regulation of software and artificial intelligence as a medical device', The Medicines and Healthcare Products Regulatory Agency, September 2021; <https://www.gov.uk/government/news/transforming-the-regulation-of-software-and-artificial-intelligence-as-a-medical-device>

<sup>22</sup> 'EU Artificial Intelligence (AI) Act', European Commission, April 2021; <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206>

<sup>23</sup> 'Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification', Joy Buolamwini, Timnit Gebru, February 2018; <https://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf>

<sup>24</sup> 'Microsoft Bug Bounty Program', Microsoft, 2021; <https://www.microsoft.com/en-us/msrc/bounty>

<sup>25</sup> 'Introducing Twitter's first Algorithmic Bias Bounty Challenge', Rumman Chowdhury, Jutta Williams, July 2021; [https://blog.twitter.com/engineering/en\\_us/topics/insights/2021/algorithmic-bias-bounty-challenge](https://blog.twitter.com/engineering/en_us/topics/insights/2021/algorithmic-bias-bounty-challenge)

## Summary: The roadmap to an effective AI assurance ecosystem

 Vision	 Current challenge	 What needs to happen?
Demand for reliable and effective assurance across the AI supply chain, and across the range of AI risks	Limited demand, primarily focused on the topics attracting reputational risk	Actors in the AI supply chain have a clearer understanding of AI risks and of their corresponding accountabilities for addressing these risks via assurance services
Dynamic, competitive AI assurance market providing a range of effective, efficient, and fit-for-purpose services and tools	Nascent, fragmented market that is mostly focused on the needs of developers	Government, regulators and private sector organisations shape an effective market for AI assurance services to fill skills gaps and lack of incentives to provide effective assurance in the AI supply chain
Standards provide a common language for AI assurance, including common measurement thresholds where appropriate	Multiple AI standardisation efforts, but crowded and often not the sorts of measurement and management standards that support assurance	Standards bodies deliver common measurement standards for AI risks and management system standards
An accountable AI assurance profession providing reliable assurance services	No clear direction for which professionalisation model or models are best suited to build trust in AI assurance services	Collaboration between existing professional and accreditation bodies to build routes to professionalisation
Regulation enables trustworthy AI innovation by setting out assurable guidelines to ensure systems meet regulatory requirements	Some promising efforts by individual regulators (e.g. ICO) to make their regulatory concerns assurable and by others (FCA, MHRA) to adapt existing assurance mechanisms to AI, but this will need to become more widespread across regulated areas	Regulators make active efforts to translate their concerns with AI into assurable guidelines for the AI supply chain
Independent researchers play an important role developing assurance techniques and identifying AI risks	Links between industry and independent researchers are currently underdeveloped, preventing effective collaboration	Industry opens up space for independent researchers to provide solution-focused research to address AI risks and contribute to the development of AI assurance techniques

## The CDEI is committed to making its vision a reality

The CDEI intends this roadmap to be a first step towards building an effective AI assurance ecosystem. Going forward, actors from across the ecosystem will need to play their part to enable it to mature. To support development of this ecosystem, AI assurance is a core theme of the CDEI's 2021/22 work programme, which includes:

### Enabling trustworthy assurance practices:

**Publishing an AI assurance guide:** The CDEI will publish an AI assurance guide to accompany this roadmap as an immediate follow up to this work. The guide focuses in more detail on the delivery of AI assurance and aims to support practitioners and others using or providing AI assurance.

**Embedding assurance into public sector innovation:** The CDEI will embed assurance thinking into existing partnership projects with defence-focused organisations, police forces and local authorities.

### Advising and influencing the critical supporting roles in the assurance ecosystem:

**AI standard setting:** The CDEI will support the Department for Digital, Culture, Media and Sport (DCMS) Digital Standards team and the Office for Artificial Intelligence (OAI) as they establish an AI Standards Hub, focused on global digital technical standards. The CDEI will also partner with and support professional bodies and regulators in the UK to set out assurable standards and requirements for AI systems.

**Supporting effective regulation, policy and guidance:** The CDEI will work in partnership with government policy teams and regulators, as well as with industry and professional bodies, as they respond to the emergence of AI across the economy. The CDEI is already partnering with the Centre for Connected and Autonomous Vehicles (CCAV) to embed ethical due diligence in the future regulatory framework for self-driving vehicles, and has worked with the Recruitment and Employment Confederation (REC) to develop guidance on the use of data-driven tools in recruitment. Additionally, the CDEI is supporting the OAI as it develops a White Paper on the governance of AI systems, and working with DCMS as it considers potential options for reform of the UK's data protection regime.

### Convening to build consensus and ensure effective coordination between stakeholders:

**Building consensus around the need for assurance:** Taking the roadmap as a starting point for discussion, an initial series of events will focus on building a more detailed cross-stakeholder strategy and corresponding accountabilities to deliver an effective AI assurance ecosystem.

**Accreditation and professionalisation:** The CDEI will convene an AI assurance accreditation forum to bring together professional and accreditation bodies who will need to play a role in the professionalisation of AI assurance.

### Future partnerships:

The CDEI is actively looking to partner with organisations who are looking to help build an effective AI assurance ecosystem. If you are interested in exploring opportunities to partner with CDEI on AI assurance related projects, please get in touch at [ai.assurance@cdei.gov.uk](mailto:ai.assurance@cdei.gov.uk).

To support development of this ecosystem,  
AI assurance is a core theme of the CDEI's  
2021/22 work programme.

## The CDEI's work programme on AI assurance

 <b>Vision</b>	 <b>What needs to happen?</b>	 <b>The CDEI's role in making this happen</b>
<p>Demand for reliable and effective assurance across the AI supply chain, and across the range of AI risks</p>	<p>Actors in the AI supply chain have clearer understanding of AI risks and demand assurance based on their corresponding accountabilities for these risks</p>	<ul style="list-style-type: none"> <li>Enable assurance in our ongoing work with public sector partners</li> <li>Convene cross-stakeholder workshops to develop a shared action plan</li> <li>Influence demand for effective AI assurance with the AI assurance guide, clarifying how a range of assurance mechanisms can address different AI risks</li> </ul>
<p>Dynamic, competitive AI assurance market providing a range of effective, efficient, and fit-for-purpose services and tools</p>	<p>Government, regulators and private sector shape an effective market for AI assurance services to fill skills gaps and lack of incentives to provide effective assurance in the AI supply chain</p>	<ul style="list-style-type: none"> <li>Enable an effective assurance market, using the AI assurance guide to build common understanding around the full range of AI assurance tools</li> <li>Convene assurance practitioners to develop a full range of assurance solutions</li> </ul>
<p>Standards provide a common language for AI assurance, including common measurement thresholds where appropriate</p>	<p>Standards bodies focus on common measurement standards for bias and management system standards</p>	<ul style="list-style-type: none"> <li>Advise the DCMS Digital Standards Team and the OAI as they pilot an AI Standards Hub</li> <li>Influence professional bodies to develop sector-specific standards that support AI assurance</li> </ul>
<p>An accountable AI assurance profession providing reliable assurance services</p>	<p>Collaboration between existing professional and accreditation bodies to build routes to professionalisation</p>	<ul style="list-style-type: none"> <li>Convene forums and explore pilots with existing accreditation (UKAS) and professional bodies (BCS, ICAEW) to assess the most promising routes to professionalising AI assurance</li> </ul>

 <b>Vision</b>	 <b>What needs to happen?</b>	 <b>The CDEI's role in making this happen</b>
<p>Regulation enables trustworthy AI innovation by setting out assurable guidelines to ensure systems meet regulatory requirements</p>	<p>Regulators make active efforts to translate their concerns with AI into assurable guidelines for the AI supply chain</p>	<ul style="list-style-type: none"> <li>Advise the OAI on the development of the AI governance White Paper, including on the role of assurance in addressing AI governance</li> <li>Advise the DCMS Data Protection team on potential reforms to the UK's data protection regime and data protection's role in wider AI governance</li> <li>Advise regulators and policy teams to ensure that approaches to AI regulation support, and are supported by, a thriving AI assurance ecosystem</li> </ul>
<p>Independent researchers support AI assurance by identifying emerging AI risks and developing assurance techniques</p>	<p>Industry open up space for independent researchers to contribute to solution-focused research to address AI risks and develop AI assurance techniques</p>	<ul style="list-style-type: none"> <li>Enable increased coordination between researchers and industry, using the AI assurance roadmap and guide to highlight where coordination is vital to address risks and build an effective assurance ecosystem for AI</li> <li>Convene stakeholders from industry and academia to facilitate collaboration</li> </ul>

1 Horse Guards Avenue  
London  
SW1A 2HU

cdei@cdei.gov.uk  
[www.gov.uk/cdei](http://www.gov.uk/cdei)

**Centre for  
Data Ethics  
and Innovation**