GOV.UK

Department for Science, Innovation & Technology

Policy paper

Trusted third-party AI assurance roadmap

Published 3 September 2025

Contents

This publication is available at https://www.gov.uk/government/publications/trusted-third-party-ai-assurance-roadmap/trusted-third-party-ai-assurance-roadmap

Ministerial foreword

AI capabilities are advancing at an extraordinary pace, with new transformative developments in the field set to disrupt the global economy. Britain is home to pioneering AI firms and the third-largest AI market in the world. The technology is set to play an increasingly important role in driving forward this government's agenda to boost economic growth, provide jobs for the future and improve people's everyday lives.

To capitalise on the opportunities that AI presents and drive adoption, we must ensure it is developed and deployed responsibly, working as intended. As a means of demonstrating the trustworthiness of AI systems, AI assurance has a vital role to play in building confidence in AI systems, ensuring firms can confidently invest in new products and services, and helping to drive innovation and economic growth.

We believe the UK has a unique opportunity to be a world-leader in AI assurance services, building on its strengths in both the professional services and technology sectors. The UK's AI assurance market is nascent but growing, with over 524 companies operating in the market and an approximate value of £1.01 billion gross value added (GVA) in 2024. This market has the potential to drive innovation and economic growth, reaching over £18.8 billion GVA by 2035 if barriers to widespread AI adoption are addressed.

Third-party AI assurance firms have a vital role to play in enabling independent verification of the trustworthiness of AI systems and providing high-quality assurance services to firms who lack these capabilities in house. Despite this, these firms make up a relatively small portion of the UK's assurance market and they face numerous barriers to success.

This government has taken decisive action to support the UK's AI sector and address barriers to growth. In January 2025, we published the AI Opportunities Action Plan (https://www.gov.uk/government/publications/ai-opportunities-action-plan/ai-opportunities-action-plan), which set out our plans to ramp up AI adoption across the UK to boost economic growth, provide jobs for the future and improve people's everyday lives. Through the Industrial Strategy (https://www.gov.uk/government/publications/industrial-strategy) and Spending Review (https://www.gov.uk/government/publications/spending-review-2025-document) we committed to investing in key sectors, with this year's Compute Roadmap (https://www.gov.uk/government/publications/uk-compute-roadmap) establishing the infrastructure required for continued innovation. We are now turning our attention to addressing barriers that restrict the growth of the AI assurance market, a growing multi-billion-pound global industry

This roadmap to trusted third-party AI assurance sets out our ambitions for the third-party assurance market in the UK and the immediate actions that government will take to support this emerging sector.

By creating a world-leading AI assurance market, we believe we can increase confidence in AI, drive growth and make the UK the most attractive home for businesses seeking to adopt AI. However, this will require collaboration from all stakeholders across the ecosystem. This roadmap is intended as the next step to set us on this path to create a thriving UK AI assurance market and ensure the widespread adoption of safe and responsible AI across the UK.

Feryal Clark MP
Parliamentary Under-Secretary of State for AI and Digital Government

Introduction

AI assurance is crucial to ensure that AI systems are developed and deployed responsibly and in compliance with the law. By providing ways to measure, evaluate and communicate the trustworthiness of AI systems, assurance can increase confidence in AI systems, supporting AI adoption and economic growth.

Assurance can be conducted by multiple actors, including firms developing AI systems, firms deploying AI systems and third-party AI assurance providers. Third-party providers have a particularly important role to play in independently verifying the quality and trustworthiness of AI systems and providing bespoke, high-quality services to firms who may lack this capability inhouse. This is especially the case given that for the public the organisation assuring the AI product or service is as important as the process.

AI assurance services are a nascent but growing market in the UK. In November 2024, Department for Science, Innovation and Technology (DSIT) published its first analysis of the state of the UK's AI assurance market. We identified an estimated 161 UK-based assurance firms and found that the market for specialised AI assurance companies has grown significantly in recent years, with 80% of UK-based specialised firms in the assurance market showing growth signals.

The market's growth potential presents a unique position to be a global leader in AI assurance services. Relative to economic activity the UK's AI assurance market is greater than that of the US, Germany, and France.

Despite these strong foundations, third-party AI assurance providers currently face challenges related to identifying talent, skills-shortages, and keeping pace with accelerating capabilities in AI development. These challenges restrict the growth and quality of the UK's third-party assurance market.

This roadmap to trusted third-party AI assurance is a step towards addressing these challenges, stimulating collective action to drive the quality and growth of the UK's third-party AI assurance market. It draws on research conducted by DSIT, including:

- an economic analysis of the UK's AI assurance market;
- expert roundtables with participants from industry; regulators and the UK quality assurance infrastructure
- a roundtable with AI assurance providers on AI auditing skills requirements;
- expert research commissioned to explore potential interactions with the EU AI Act

The first section highlights the steps government will take now to support the third-party assurance market.

The next section highlights the key challenges the third-party assurance market currently faces, which these actions aim to address. These relate to quality, skills, information access and innovation.

The final section sets out the interventions we explored to address these challenges. This includes 3 potential quality assurance models for the third-party AI assurance market, as well as interventions to address skills challenges, information asymmetries and barriers to innovation.

Government actions

To ensure the UK's AI assurance market provides high-quality services and realises its growth potential, government must take targeted action to address the challenges the market is facing.

In the near term, we are prioritising areas where we can use our levers as government to have the greatest impact. Beyond the actions set out in this roadmap, DSIT will continue its work to support a growing, competitive and dynamic UK AI assurance ecosystem.

Professionalisation

Convening a UK consortium to work towards a future AI assurance profession

DSIT will support the establishment of an AI assurance profession. This could help firms to demonstrate the quality of the services they provide, ensure their employees have the requisite skills and qualifications, and increase confidence in the market.

To work towards this profession, DSIT will convene a **consortium of stakeholders**, led by a nominated partner and supported by government. Its membership will include organisations from the UK's quality infrastructure and existing professional bodies, and it will work closely with existing bodies like the international AIQI Consortium.

In the first year, the consortium will be tasked with developing the building blocks to support future professionalisation, including developing a voluntary **professional code of ethics for AI assurance**. This will help to embed criteria for professional practice, conduct and behaviour into this emerging industry.

The consortium will also support the development of a **skills and competencies framework for AI assurance and map information access**

requirements for AI assurance providers (see below).

Once these building blocks are established, the consortium can work towards developing a future professional certification or registration scheme for AI assurance. Given the breadth and nascency of the AI assurance market, AI auditing could be a useful starting point for professional certification, and one specialism within a wider assurance profession. Auditing has a particularly important role to play in independently verifying the trustworthiness of AI systems. As compared with other areas of the AI assurance market, auditing is also relatively mature.

Skills

Developing our understanding of AI assurance skills and competencies
To address the current lack of clarity surrounding the skills and competencies required for third-party AI assurance, DSIT will work with the consortium to develop a comprehensive skills and competencies framework for AI assurance.

This will inform the development of a future professional certification scheme for AI assurance. This scheme will need to consider existing standards, training courses and certification schemes in adjacent areas – including cybersecurity, data science, software development, internal auditing and privacy – and how these can support pathways into the AI assurance industry for existing professionals.

Once complete, DSIT will be able to assess the availability of training courses and qualifications to support this emerging sector and determine whether further investment in the area is necessary to create a skilled and diverse AI assurance workforce.

Information access

Mapping information requirements to inform best practice guidelines
To further our understanding of the information assurance providers require from their customers, the consortium will be tasked with working with UK assurance providers to **map information requirements** for different types of AI assurance services. This will inform the future development of **best practice guidelines for firms using assurance services** to help establish

expectations around information sharing up front. In the future, government will explore levers to implement these best practices.

Innovation

Establishing a new forum for multi-stakeholder collaboration
To ensure the UK is ready to respond to rapid developments in AI capabilities, DSIT is establishing the **AI Assurance Innovation Fund**. This initiative will issue £11 million funding to support the development of innovative and novel AI assurance mechanisms to help actors across the AI value chain to identify and address the risks posed by high-capability AI systems. The fund will capitalise on the UK's world-leading expertise in AI security and assurance to create a flourishing AI assurance market in the UK that is equipped to deal with the risks posed by advancing AI capabilities. The first round of the AI Assurance Innovation Fund will open for applications in Spring 2026. To drive AI adoption, we will also explore opportunities for the fund to support the work of the UK's AI Adoption Hubs by providing funding to pilot innovative assurance solutions alongside cutting-edge AI technologies.

Challenges for a trusted third-party assurance market

To support the quality and growth of the UK's third-party AI assurance market, this roadmap identifies 4 key market barriers that must be overcome.

Quality

The UK has a nascent but growing market for AI assurance worth over £1 billion. Despite this, the quality of the goods and services provided is currently unclear, and the quality infrastructure to ensure that assurance providers are supplying high-quality products and services is still developing.

There are existing certifications that can demonstrate competencies in AI assurance. However, it is difficult to ascertain their quality, and none are issued by UKAS-accredited organisations. In addition, not all assurance tools on the market are effective in mitigating risk; a recent World Privacy Forum report

suggests that as much as 38% of AI governance tools may utilise metrics that could result in harm.[footnote 1]

Technical standards provide the bedrock of any quality assurance ecosystem, but for AI systems and assurance they are still developing. This makes it unclear exactly what standards AI systems and those assuring them should be held to.

Skills

The AI Opportunities Action Plan (https://www.gov.uk/government/publications/ai-opportunities-action-plan/ai-opportunities-action-plan) recognised the importance of skills and training as an enabler of AI adoption and a driver of economic growth. The UK's AI assurance sector already employs an estimated 12,500 people and could provide many more jobs in the future.

Despite this, UK assurance providers have reported facing **difficulty in finding employees with the full range of skills** needed to assure AI systems. To provide effective third-party assurance services, employees will likely require a combination of knowledge and skills, including AI and machine learning, law, AI governance and standards, and more. Though training courses in some of these areas already exist, it is currently unclear exactly what combination of skills and competencies assurance professionals require.

Clearer pathways into the AI assurance sector could help bolster the market. However, the wider AI market suffers from a lack of diversity.[footnote 2] For AI assurance to effectively challenge the assumptions baked into AI systems and identify and mitigate the full range of risks associated with AI systems, encouraging diversity in the field is particularly important.

Information access

To effectively assure AI systems, assurance providers require access to information about these systems. This may include access to training data, models or information about AI systems, such as their management and governance.

Assurance service providers have identified **a lack of access to information about AI systems** as a barrier to effective AI assurance.[footnote 3] Firms being

audited may be unwilling to share the required information due to commercial confidentiality concerns, prioritisation of commercial delivery or lack of awareness of the risks their systems pose.[footnote 4] Without a clear understanding of the information that is required, they may also fear oversharing information and putting the security of their systems at risk.

Innovation

As AI continues to develop and new, transformative capabilities arise, innovative testing and evaluation methods, tools and services will be required to assure AI systems. Innovation in AI assurance is complex and will require inputs from diverse experts, including AI developers.

However, there are currently **limited forums for collaborative research and development on AI assurance** in the UK.

For the third-party assurance market to keep pace with AI development and ensure the UK is ready to respond to emerging AI capabilities, more collaborative research into assurance is required, as well as mechanisms to ensure this information is shared across the wider ecosystem as new models proliferate.

Exploring interventions to support a high-quality third-party AI assurance market

Pathways to quality assurance

Government action
Establishing a multi-stakeholder consortium to support the development of the AI assurance profession.

Ensuring the quality of the services provided on the UK's AI assurance market could help assurance firms to stand out from competitors, provide customers

with a shortcut to assess the credibility of an assurance firm's claims, and help increase confidence in the assurance market.

We considered 3 potential pathways to drive quality improvements in the UK's AI assurance market:

- Professionalisation of the AI assurance industry by providing professional certification and/or registration for individuals who demonstrate the necessary skills and qualifications required for effective AI assurance.
- Certification of assurance processes by issuing a quality mark for the processes used to assure an AI system.
- Accreditation of assurance firms who demonstrate they have the skills and competencies required to provide effective AI assurance services.

Certification of AI products is beyond the scope of this work. Our proposed approach to quality assurance would be a complement to this should a regime emerge.

Professionalisation

In the near term, we think professionalisation has the greatest potential in driving the quality and growth of the UK's AI assurance market. However, a professional certification or registration scheme for AI assurance professionals would need to be carefully designed and developed in partnership with existing professional bodies, as well as being supported by a high-quality training ecosystem.

What is professionalisation?
Professional certification provides an opportunity for an individual to develop their knowledge and expertise in a specific subject matter. To assure they are high quality, government can mandate that professional certification schemes are delivered by accredited trainers.

By contrast, professional registration providers assesses an individual's existing skills, knowledge and experience against professional standards, and is granted by a regulated industry authority. Adherence to professional standards is a requirement in regulated professions – including teaching, dentistry and law – as well as some chartered professions.

Professionalisation relies on an ecosystem of qualifications and training programmes to support and improve the skills of aspiring professionals.

The UK Cyber Security Council
The UK Cyber Security Council (CSC) was established to tackle barriers facing the cybersecurity profession, including the lack of universal professional standards, public awareness of professional opportunities and diversity in the industry.

The CSC has developed its own model for professionalisation of the cybersecurity sector. This includes the Standard of Professional Competence and Commitment (SPCC), which provides a framework to assess the skills and competencies of the cybersecurity workforce, as well as different cybersecurity specialisms to encourage further professional development. This model can help employers assess what a good professional looks like and identify who has the specialist skills they require.

Market readiness

Demand for professionalisation in the AI assurance sector is increasing. BCS, The Chartered Institute for IT has called for registration of AI assurance professionals.[footnote 5] The Alliance for Data Science Professionals (https://allianceforadatascienceprofessionals.com/) has also developed certifications for data science professionals.

Potential benefits and limitations

Professionalisation could enable assurance firms to demonstrate they hire employees with appropriate skills and qualifications, increasing consumer confidence in the assurance market and **attracting more business** for assurance providers with certified employees.

Government-backed professionalisation could also give aspiring professionals confidence that associated qualifications and training programmes are **high quality** and offer a **meaningful path into the assurance profession**, as well as providing **more employment opportunities**.

Despite this, professionalisation **relies upon a wider ecosystem** of qualifications, training and professional development programmes to support aspiring AI assurance practitioners.

In addition, as AI assurance is an emerging sector, determining the **scope** of a future profession – including how it interacts with existing training programmes and certification schemes in related areas like data science, cybersecurity and data privacy – may be challenging.

Given the nascency of the AI assurance market, seeking to immediately establish a regulated industry body and professional standard for AI assurance

professionals may be premature. The building blocks towards a future AI assurance profession – including skills – must be carefully considered beforehand.

Other pathways to quality assurance

Alongside professionalisation, we also considered the potential of conformity assessment activities – including process certification and accreditation – to drive quality improvements in the UK AI assurance market.

While process certification and accreditation provide promising pathways to drive quality improvements in the future, we believe the market is not yet mature enough to fully realise their potential benefits.

Process certification

What is process certification?
Process certification involves verifying the quality of specific assurance processes – such as risk assessment or bias audit – that an assurance provider may use. For example, if an assurance provider conducts a technical audit that involves testing the performance of a model, they could obtain a certification for performance testing to demonstrate the quality of their auditing service.

British Standards Institution's (BSI) AI Algorithm Auditing and Dataset Testing service
BSI's Algorithm Auditing and Dataset Testing (https://www.bsigroup.com/en-GB/products-and-services/standards/ai-algorithm-auditing-dataset-testing/) service (AA&DT) offers independent verification that an AI system is performing as intended by assessing its algorithms, models and datasets.

The AA&DT is underpinned by a series of technical standards to ensure the service's consistency and replicability. ISO / IEC 24027 (https://www.iso.org/standard/77607.html) is used to standardise measurement techniques and methods for assessing bias across an AI system's lifecycle.

Developing a certification against this standard in the future could help build trust by demonstrating that the audit processes assurance providers

are using are consistent and replicable.

Market readiness

Some measurement and process standards for AI already exist. These include standards for performance testing, bias audit, risk assessment and – most recently – AI cybersecurity, led by the UK government.[footnote 6] As many of these standards are relatively new and have not yet been widely adopted, efforts to certify AI assurance processes are few and far between. However, lessons from process certification in similar industries – such as cybersecurity – can shed light on the potential benefits and limitations of this model.

Potential benefits and limitations

In the UK, process certification could offer several benefits. Standardising assurance processes could improve the consistency of assurance services across providers. This could give customers greater clarity on what to expect when procuring services, building their confidence in the market. As process certification is underpinned by global technical standards, this model could also provide UK AI assurance firms with improved access to international markets.

Despite this, process certification can be lengthy and costly, preventing smaller firms with fewer resources from obtaining certification. A 2021 Qualtrics survey identified the lengthy approval process for certification of cybersecurity products, processes and systems under the Common Criteria for Information Technology Security Evaluation (the Common Criteria) as a significant barrier to demand for certification, with the process taking an average of 6 months to a year to complete, and many firms opted out due to prohibitive costs.[footnote 7]

Process certification would also be complex. The services assurance firms provide are often context-dependent and bespoke, meaning they may combine different assurance processes in complex and differing ways.

In addition, best practices for assuring AI systems – and the technical standards that encode them – are still emerging, and certification of assurance processes may risk inferring consensus where it does not exist. Certification is also a static process, which would make it more challenging for firms to update or modify their services as best practice evolves.

Accreditation

What is accreditation?

Accreditation involves the assessment of organisations to confirm they can competently, impartially, and consistently conduct conformity assessment activities such as certification, testing, and inspection. In the UK, accreditation is issued by UKAS, the UK's national accreditation service.

Market readiness

Given the nascency of the AI assurance market and the breadth of different services assurance providers offer, it would be challenging to develop generalisable requirements to certify organisations based on their organisational practices, skills and competencies. Accredited management system certification may therefore be the most feasible way of driving quality improvements among AI assurance firms in the near term. Accredited management system certification verifies that the management system operated by an organisation will deliver a consistent and quality service.

Some organisations have begun to obtain UKAS accreditation to conduct specific types of assurance and auditing services. For example, UKAS is currently piloting accreditation for organisations to provide certification of AI management systems against ISO/IEC 42001.[footnote 8] However, the scope of existing efforts is limited.

Potential benefits and limitations

Accreditation could provide AI assurance firms with a mark of **credibility and quality**. UKAS's CertCheck enables organisations to find accredited certification bodies, which could bolster **visibility and uptake** of assurance providers who obtain accreditation. As it is underpinned by global technical standards, this approach could also enable **global market access** for UK AI assurance providers.

However, standards that could underpin certification by accredited assurance providers are currently **limited in number and scope**. This will likely curb the impact of accreditation in driving quality improvements in the near term.

Skills

Government action

Working with the consortium to support the development of a skills and competencies framework for AI assurance.

To meet expected demand for AI, the UK must be prepared to train tens of thousands of AI professionals over the next 5 years. The government's response to the AI Opportunities Action Plan (https://www.gov.uk/government/publications/ai-opportunities-action-plan/ai-opportunities-action-plan) commits to strengthening our AI skills and talent base to ensure we are looking across the whole skills and education system, developing the top-tier talent the UK's AI sector needs to compete.

Assurance firms – particularly smaller businesses – have reported that they are struggling to attract and retain employees with the right skills to effectively assure AI systems. Finding candidates for these roles is particularly challenging without there being associated qualifications or certifications to equip individuals with these skills and competencies. As assurance services are complex and diverse, individuals will likely require proficiencies across a range of different subject areas, and these will differ for different roles within assurance firms.

To understand the challenges and opportunities in this space in greater depth, we worked with the Alan Turing Institute to conduct research exploring the skills and competencies required by AI auditors. We chose to focus on audit as an illustrative example of the depth and range of proficiencies that AI assurance professionals will likely need to effectively assure AI systems.

We found that:

- auditors must be able to evaluate the wider societal impacts of AI systems, not only their technical compliance
- knowledge of risks and mitigations, regulatory and ethical compliance, and specialist knowledge across different sectors are essential for all audit roles
- governance audit roles require greater emphasis on soft skills – such as leadership and strategy – whereas technical assessment roles require deeper technical knowledge of complex AI systems
- assurance providers rely on in-house training of AI auditors, due to a lack of training with practical utility for auditors and the high costs of relevant training
- the skills identified as important for AI audit are present within occupational standards, but they don't explicitly acknowledge AI assurance or audit or provide detail on the combination of competencies they require
- existing training and certification schemes – such as the IAPP's AI Governance certificate (https://iapp.org/certify/aigp/) and training programmes in cybersecurity, data science, internal audit and software engineering – may provide some of the relevant skills required for AI auditing, but there is no clear and accessible route into AI auditing for aspiring professionals[footnote 9]

Information access

Government action
Working with the consortium to map information access requirements for AI assurance providers and explore government levers to implement these best practices.

To effectively assure AI systems, third-party assurance providers will need access to information about different components of these systems.

To effectively assure AI systems, third-party assurance providers will need access to information about different components of these systems.

This includes:

- **requirements** that capture specific boundaries of the AI system's functionality and use
- **inputs** (for example, training data) and **outputs** (for example, the answers it provides to queries)
- the **algorithm** that is used to generate the model, and its **parameters**
- **oversight** and **change management mechanisms**, such as the monitoring of the AI system and steps taken to update, improve or repair it post-deployment
- **documentation** that describes the management and governance processes surrounding the AI system

Different AI assurance services will require different levels of access to information, ranging from full, white box access (that is, to the inner workings of an AI system) to minimal access (that is, to relevant documentation).

Assurance providers often struggle to access the information they need to conduct effective assurance of AI systems. Firms who are using assurance services may have concerns about sharing commercially confidential information – such as training data – with third-party providers. Conversely, these firms are also at risk of providing access to unnecessary information about their systems, potentially exposing them to security and privacy risks. They may also lack established practices to capture and store information about their AI systems and make this easily accessible to assurance providers.

There are a range of interventions that could help address these barriers and enable information access for third-party assurance providers.

These include:

1. **Technical solutions** to enable auditor access to AI systems within a secure, privacy-preserving environment. For example, the UK's AI Security Institute, Anthropic and OpenMined have piloted the creation of secure enclaves for AI evaluation.[footnote 10]

2. **Standards** for information access and transparency. IEEE 7001:2021, for example, requires that all government-funded AI systems adhere to appropriate transparency standards.

3. **Best practice guidelines** for information sharing. Government-backed guidelines could provide shared expectations between firms and assurance providers around best practices for information sharing.

Innovation

> **Government action**
> Establishing an AI Assurance Innovation Fund to develop novel and innovative assurance tools and services to address the risks posed by highly capable AI systems.

AI development is advancing rapidly. Transformative AI performing at human levels or above across most cognitive tasks looks increasingly likely to emerge in the near future. While offering unprecedented opportunities, transformative AI will also present novel and emerging risks. To prepare the UK for advancing AI capabilities and ensure these systems are trustworthy, continuous innovation in AI assurance is required.

However, third-party assurance firms often lack access and insight into the process of AI system development. This information asymmetry between developers and assurance providers risks limiting the ability of third-party providers to develop tools and services that can address the capabilities and risks of emerging AI systems.

Innovation in the assurance sector also requires funding, and market incentives for investment in this area are currently weak. Inputs from a diverse

pool of experts – including AI developers, deployers, and experts in AI governance, law and ethics – are required. At present, there are limited forums to support this kind of collaborative research and development on AI assurance in the UK.

In 2024, DSIT ran the Fairness Innovation Challenge (https://fairnessinnovationchallenge.co.uk/), a grant challenge that awarded over £500,000 to fund the development of novel approaches to auditing AI systems for bias. The Challenge sought to bridge the gap between technical approaches to and societal concepts of fairness by encouraging winners to adopt a socio-technical approach to fairness, and to collaborate with UK regulators, to develop effective bias audit solutions. DSIT funded 4 teams that developed innovative solutions spanning the healthcare, HR and recruitment, financial services and higher education sectors. The Challenge concluded in March 2025 and the solutions the winning teams developed are now publicly available.

The AI Security Institute also has a mission to equip governments with a scientific understanding of the risks posed by advanced AI, by conducting research and developing and testing mitigations. However, the scope of the Institute's work focuses specifically on security risks posed by advanced AI and evaluations conducted by developers, as opposed to assurance across the entire AI value chain.

Other countries have started to fund research and development in AI assurance. In February 2025, Singapore's AI Verify Foundation launched a Global AI Assurance Pilot (https://aiverifyfoundation.sg/ai-assurance-pilot/). This will help to codify emerging norms and practices around the technical testing of generative AI applications, promoting collaboration by pairing AI assurance providers with organisations deploying generative AI applications.

For the UK assurance market to ready the UK for increasingly capable AI, support widespread AI adoption, and continue growing, efforts are required to bring together the knowledge and expertise of different actors to encourage innovation in AI assurance and distribute this knowledge across the wider ecosystem.

Next steps

This roadmap has set out the first steps government will take to drive collective action to boost the quality and growth of the UK's third-party AI assurance market.

We are committed to ensuring this is an open and multi-stakeholder endeavour and want to engage across the assurance ecosystem to ensure that the actions we take are as informed and impactful as possible.

To get in touch, email us at ai-assurance@dsit.gov.uk.

---

1. Risky Analysis: Assessing and Improving AI Governance Tools (https://worldprivacyforum.org/wp-content/uploads/2023/12/WPF_Risky_Analysis_December_2023_fs.pdf)
2. Promoting diversity in AI (https://www.business-reporter.co.uk/ai--automation/promoting-diversity-in-ai)
3. Code and conduct: How to create third-party auditing regimes for AI systems (https://www.adalovelaceinstitute.org/report/code-conduct-ai/)
4. Ensuring Trustworthy AI: the Emerging AI Assurance Market (https://www.drcf.org.uk/publications/blogs/ensuring-trustworthy-ai-the-emerging-ai-assurance-market)
5. Helping AI grow up without pressing pause (https://www.bcs.org/articles-opinion-and-research/helping-ai-grow-up-without-pressing-pause/)
6. Securing Artificial Intelligence (SAI); Baseline Cyber Security Requirements for AI Models and Systems (https://www.etsi.org/deliver/etsi_ts/104200_104299/104223/01.01.01_60/ts_104223v010101p.pdf)
7. How Do Organizations Seek Cyber Assurance? Investigations on the Adoption of the Common Criteria and Beyond (https://researchoutput.csu.edu.au/ws/portalfiles/portal/518847329/518801408_Published_article.pdf)
8. Pilot accreditation update: certification of AI management systems (https://www.ukas.com/resources/latest-news/pilot-update-ai-ms/)
9. NCSC Assured Training (https://www.ncsc.gov.uk/information/certified-training), Alliance for Data Science Professionals (https://afdsp.co.uk/), Auditing Artificial Intelligence (AI): A Hands-On Course for Internal Auditors (https://www.theiia.org/en/products/learning-solutions/course/auditing-artificial-intelligence-ai-a-hands-on-course-for-internal-auditors/), BCS Foundation Certificate in the Ethical Build of AI (https://www.bcs.org/qualifications-and-certifications/online-it-professional-development-courses/bcs-foundation-certificate-in-the-ethical-build-of-ai/)
10. Secure Enclaves for AI Evaluation (https://openmined.org/blog/secure-enclaves-for-ai-evaluation/)