Call for input

AI assurance

Publication date:	17 June 2026
Response deadline:	12 August 2026
Contact:	Jonathan Thurlwell
Lead:	Kerry Sheehan
Team:	Emerging Technologies
Email:	EmergingTechnologies@ofgem.gov.uk

Contents

1. Introduction

1.1 Ofgem is seeking views on the growing use of artificial intelligence (AI) across Britain's energy sector and how organisations are assuring the safe, secure, fair and effective operation of these tools and systems.

1.2 AI is increasingly being deployed in areas including:

- demand forecasting
- system balancing
- network planning
- asset maintenance
- trading
- pricing and market operations
- customer service and vulnerability support
- customer billing

1.3 For the purposes of this call for input, AI describes computer systems which can perform tasks usually requiring human intelligence (National Cyber Security Centre (NCSC)). This includes AI systems that generate outputs such as predictions, recommendations or decisions influencing operational or consumer outcomes.

1.4 As AI becomes more embedded in critical national infrastructure and energy services across the energy system, it is important that companies can demonstrate appropriate confidence in AI system performance, governance and, importantly, the outcomes they produce.

1.5 Stakeholders are increasingly focused on whether their organisations can demonstrate, through credible evidence, that their AI systems deliver safe, fair and effective outcomes in practice.

1.6 This call for input seeks evidence and views on whether and how AI assurance approaches could support energy sector participants (such as licensees, market participants and operators of essential services) in strengthening confidence, accountability and operational resilience in AI systems and their outcomes.

1.7 In particular, we are interested in views on what 'good' looks like in practice through an AI assurance lens. This may include, for example, the types of evidence, testing, audit or independent validation that could demonstrate that AI system risks are identified and effectively controlled prior to deployment; that performance is appropriately monitored and maintained once systems are in use; that customer outcomes remain fair and equitable; and that any failures are promptly detected, understood, and appropriately mitigated.

1.8 This is an exploratory exercise. It does not introduce new regulatory requirements.

1.9 Overall, the approach set out in this document seeks to balance effective risk management with enabling AI innovation, recognising the potential for AI to drive growth, improve energy system resilience and deliver better outcomes for consumers.

2. Objectives

2.1 This call for input seeks to understand:

- the current use of AI assurance across the energy sector
- maturity of existing AI governance and assurance practices
- challenges and gaps in assuring AI systems in operational environments
- understand the availability, maturity, and effectiveness of AI assurance tools, in-house capabilities, and external services, and whether there are opportunities for a sector-wide approach
- whether energy sector-specific good practice guidance on AI assurance would be useful

2.2 It also seeks views on how AI assurance approaches can remain proportionate, flexible, innovation-supporting and outcomes-focused, while strengthening confidence, accountability and operational resilience, including by providing assurance that AI systems deliver safe, fair and effective outcomes in practice.

2.3 It seeks views on the role, availability and maturity of tools and technical capabilities to support AI assurance in practice, including their effectiveness across activities such as testing, monitoring, explainability, auditability and governance, and whether there are gaps in current provision or opportunities for shared or sector-wide approaches.

2.4 Ofgem welcomes the provision of supporting evidence, including examples, case studies, good practice or practical experience where available.

Context

2.5 Ofgem has published AI guidance setting out principles and expectations for the ethical use of AI in the energy sector. This includes areas such as governance and accountability, risk management, explainability and transparency, capabilities, including human oversight, and organisational capability.

2.6 Energy sector participants are at different stages of AI maturity, and while governance and risk management frameworks are essential, they may not always provide sufficient confidence about how AI systems perform in practice or the outcomes they produce. AI assurance can play a role in addressing this gap by supporting organisations to test, evidence and demonstrate that governance and risk management measures are operating effectively in real-world settings.

2.7 This call for input builds on the foundations of existing Ofgem AI guidance. It explores how good practice governance expectations and risk management principles can be translated into practical AI assurance approaches that provide credible, proportionate evidence of performance and outcomes in practice.

2.8 It also aligns with the UK government's AI Roadmap, which sets out a national ambition to develop a trusted and effective AI assurance ecosystem across the economy.

2.9 The UK's Trusted Third Party AI Assurance Roadmap highlights the importance of fostering a mature and competitive AI assurance market, strengthening skills and professional capability, and supporting innovation in assurance approaches and methods. It also emphasises the role of AI assurance in enabling the trustworthy adoption of AI across sectors, including energy, and encouraging the use of both internal and independent third-party assurance.

2.10 Within this context, AI assurance can be understood as an emerging capability that supports organisations to build and demonstrate structured, credible confidence in AI systems and the outcomes they produce, including for consumers.

Relationship to existing guidance and policy

2.11 Ofgem is exploring how AI assurance could complement, not replace, existing good practice that is set out in our ethical AI guidance.

2.12 Ofgem's AI guidance sets out good practice for stakeholders to consider when evaluating opportunities to use AI. This is intended to supplement and support the existing energy regulatory regime. This guidance covers governance measures and policies to ensure effective oversight of AI, a risk approach to help stakeholders identify and manage risks associated with AI, and the competencies required for the ethical adoption of AI.

2.13 This call for input also reflects wider cross-sector and international work on AI governance and assurance, including

- the government's AI Opportunities Action Plan
- Information Commissioner's Office (ICO) AI guidance, including its AI auditing framework and related AI and data protection guidance
- practical approaches and research developed by the Alan Turing Institute on evidencing and demonstrating trustworthy AI in practice
- OECD's AI Principles

Together, these provide a foundation for the responsible development and use of AI, including accountability, risk management and implementation in practice.

2.14 Alongside these, relevant UK guidance on AI governance, data protection and cyber security is considered, including:

- ICO – AI and Data Protection Guidance: provides guidance on managing data protection risks in AI systems, including fairness, transparency, accountability and governance, with practical expectations for demonstrating compliance

- NCSC – Guidelines for Secure AI System Development: provides best practice guidance for building and deploying secure AI systems across the full lifecycle, including design, development, deployment and ongoing operation, with a focus on risk management, testing and monitoring
- NCSC – Machine Learning Security Principles: sets out practical principles to help organisations identify and mitigate security risks in AI and machine learning systems, emphasising secure-by-design approaches and lifecycle risk management
- UK government – AI Cyber Security Code of Practice: establishes baseline cyber security requirements for AI systems across the lifecycle, addressing risks such as data poisoning, model vulnerabilities and secure deployment

2.15 Relevant standards and frameworks are also emerging to support good practice AI governance and assurance, including ISO/IEC 42001 (AI management systems), which provides a structured and auditable framework for managing AI systems across their lifecycle, and ISO/IEC 23894 (AI risk management), which provides guidance on identifying, assessing and managing risks associated with AI. These standards may support organisations in demonstrating responsible AI practices.

3. Why AI assurance matters

3.1 AI assurance can support the responsible adoption of AI and help build stakeholder confidence and trust in both AI systems and the outcomes they produce.

3.2 In the energy sector, this requires not only defining intended outcomes, such as those set out in our ethical AI guidance, but also developing a shared understanding of the evidence and assurance approaches needed to demonstrate that those outcomes are being achieved in practice.

3.3 This should be proportionate to the level of risk and complexity associated with different AI use cases.

AI assurance is an emerging area, and there is not yet a single agreed definition. For the purposes of this call for input, we use a working description: AI assurance involves measuring, evaluating and communicating whether an AI system meets relevant criteria, such as regulatory requirements, standards, ethical guidelines and organisational values. It includes the processes used to generate and communicate evidence about how an AI system or process is performing in practice (DSIT, Introduction to AI Assurance; British Computer Society, What is AI assurance?).

3.4 Effective AI assurance can support:

- improved safety and resilience of AI-enabled systems
- continued innovation within an outcomes-based, non-prescriptive regulatory approach
- greater clarity across the sector on what constitutes good AI assurance in practice
- increased confidence that risks to consumers and the energy system are appropriately identified and managed

4. What is meant by AI assurance?

4.1 For the purposes of this call for input, AI assurance refers to the process, measures and evidence used to assess, monitor, test and evaluate, and communicate, whether AI systems are operating in line with intended objectives, legal obligations, organisational policies and consumer and stakeholder expectations. It can cover whether AI systems:

- operate safely and securely
- support reliable energy system functioning and resilience
- deliver fair and appropriate outcomes for consumers
- remain robust under changing operational conditions
- are appropriately governed throughout their lifecycle

4.2 Activities may include internal controls, technical testing, monitoring, documentation, human oversight and independent review. These activities support confidence and accountability, supporting to reduce risks and aiding trust in AI outcomes across the sector, and wider economy.

4.3 However, AI assurance terminology and approaches are emerging and evolving. As set out above, no single agreed definition currently exists, and approaches should be proportionate and context specific.

4.4 The emphasis is therefore not only on the presence of appropriate governance and controls, but also on whether systems demonstrably deliver intended outcomes in practice and whether risks are effectively identified and managed.

4.5 This includes establishing and maintaining credible, decision-useful evidence that AI systems are operating as intended, that risks and potential harms are appropriately mitigated, and that systems deliver safe, secure, fair and environmentally sustainable outcomes in practice.

4.6 AI assurance should apply across the full AI system lifecycle, from design and development through to deployment and ongoing operation.

4.7 The AI assurance lifecycle stages activities may include the following:

1. **Design:** defining objectives, risks, governance arrangements and intended outcomes
2. **Testing:** validating performance, robustness, safety and fairness prior to deployment
3. **Deployment:** implementing AI systems in operational environments with appropriate controls
4. **Monitoring:** ongoing tracking of performance, risks and outcomes in practice
5. **Review:** periodic evaluation of system performance, governance effectiveness and outcomes, including updates or decommissioning where needed

4.8 Organisations may adopt different approaches depending on the nature, risk and complexity of their AI systems.

4.9 The following examples are a range of possible AI assurance approaches. The list is not exhaustive, nor in order of importance. The choice of techniques should be proportionate to the level of risk, impact and complexity:

- documentation (e.g. model cards, risk assessments, decision logs)
- impact assessments (e.g. consumer, fairness, or system risk assessments)
- technical testing (e.g. performance, robustness, bias and stress testing)
- monitoring and performance evaluation in operational use
- red teaming and adversarial testing
- independent review or third-party audit
- incident management and reporting processes

5. Scope

5.1 This call for input covers the deployment of AI in the energy sector. It is aimed at all stakeholders involved with AI in the sector which includes, but not limited to, licensees, market, participants, operators of essential services, duty holders, technology companies, AI developers, consumer groups, other regulators and government.

5.2 It focuses on AI systems that may influence energy system reliability and resilience, operational decision-making, market functioning and pricing, consumer protection and vulnerability outcomes.

5.3 This includes consideration of how AI-related risks and impacts may propagate across interconnected systems within the energy system.

Energy system context

5.4 AI assurance approaches must reflect the characteristics of the energy system, including:

- the operation of safety-critical infrastructure, including electricity and gas networks
- the need for real-time or near real-time decision-making
- dependence on data from physical systems, including sensors and IoT infrastructure
- the potential for cascading impacts across interconnected systems

5.5 This means AI assurance should consider not only AI model performance, but also:

- system-level behaviour
- integration with operational controls
- performance under real-world conditions

5.6 The aims of AI assurance guidance is to:

- help companies build internal capabilities, improving confidence and oversight
- support proportionate risk management, encouraging good practice
- help companies communicate AI assurance to stakeholders, including to consumers
- support AI innovation and responsible AI adoption

Key challenges

5.7 Initial engagement suggests possible challenges across the energy sector, including:

- varying levels of maturity and inconsistent approaches to AI governance and assurance
- a lack of shared understanding of what constitutes sufficient evidence for outcomes-based AI assurance
- limited approaches to real-time monitoring of AI system performance
- variation in the maturity of data assurance practices
- challenges in integrating AI systems into existing safety and operational frameworks

Cross-cutting principles

5.8 Ofgem is considering whether any future energy sector-specific AI assurance guidance could reflect the following cross-cutting principles:

- proportionality to risk and impact
- accountability across the AI lifecycle, including appropriate human oversight
- system safety, security and resilience
- fairness and consumer protection, including appropriate outcomes for different consumer groups
- transparency proportionate to the use of AI, including in the context of critical national infrastructure
- alignment with existing energy, cyber, safety and consumer protection regulation
- focus on outcomes, including whether AI systems deliver safe, fair and effective results in practice

5.9 These principles are provided for discussion and do not represent formal requirements.

Key clarification

5.10 This call for input does not propose new legal or regulatory requirements. Any future AI assurance guidance would aim to provide context specific to AI use and therefore complement Ofgem's existing regulatory framework.

5.11 Energy sector participants remain responsible for complying with Ofgem's regulatory framework, as well as other areas of legislation that apply to the energy sector, including data protection, equality, human rights, and health and safety.

Questions

5.12 These questions are not exhaustive. Respondents are welcome to provide views on any other relevant issues/areas.

Question 1 Current AI assurance practices

a. How do organisations evidence that AI systems are operating as intended and delivering safe, fair and effective outcomes?

b. What AI assurance approaches are currently used or under development, including in-house and third-party?

c. What tools and technical capabilities are available to support AI assurance in practice, how mature and effective are they, and where are there gaps or opportunities for shared or sector-wide approaches?

d. How are AI governance frameworks translated into operational practice?

e. Which assurance or governance practices are most effective in supporting reliable outcomes?

f. What skills, expertise and resources are required for effective AI assurance, and where are the main capability gaps?

Question 2 Risks and challenges

a. What are the main barriers to implementing effective AI assurance?

b. What are the key risks associated with AI use in the energy system (including system reliability, market functioning and consumer outcomes)?

c. Which risks are most difficult to assess, evidence, or link to real-world outcomes?

d. Where are current AI assurance approaches most limited in practice?

Question 3 Critical infrastructure considerations

a. How should AI assurance reflect the criticality of energy systems as national infrastructure?

b. What level of rigour is appropriate for high-impact or safety-critical AI use cases?

Question 4 Consumer protection and fairness

a. How can AI assurance support fair treatment of consumers, including vulnerable groups?

b. What risks arise from AI-driven pricing, segmentation or prioritisation, e.g. fairness, transparency, consumer outcomes?

Question 5 Cyber security and resilience

a. How should AI assurance align with existing cyber and operational security frameworks, e.g. NIS Regulations?

b. How can AI assurance support system resilience, including identifying and mitigating cyber, operational and AI-specific risks?

Question 6 Proportionality

a. What does proportionate AI assurance look like across different use cases and risk levels?

b. How can assurance approaches be tailored while remaining effective and practical, including for smaller organisations?

Question 7 External assurance and standards

a. Are existing frameworks and standards sufficient, or is sector-specific AI assurance guidance needed?

b. What role should independent assurance (e.g. audits, certification) play?

c. What are the benefits and risks of external assurance approaches?

Question 8 Future guidance

a. What would be most useful in future AI assurance guidance for the energy sector?

b. What types of evidence are most useful in demonstrating outcomes in practice?

c. What examples or case studies would be valuable?

Question 9 Communication

a. How should organisations communicate AI assurance to different audiences?

b. What information is most useful for consumers, boards, senior management and affected groups?

6. How to respond

We want to hear from anyone interested in this call for input by 12 August 2026. Please send your response by email to EmergingTechnologies@ofgem.gov.uk with the subject line 'AI assurance call for input' before the response deadline.

Responses will inform our understanding of how AI assurance could support the potential development of guidance, and its relevance for the energy sector, consumers and wider society.

We have asked for your feedback in each of the questions throughout. You may respond to all, or selected areas, of the question areas outlined in this call for input. You are encouraged to include relevant case studies or examples.

Call for input stages

Stage 1 Call for input open: 17 June 2026

Stage 2 Call for input closes. Deadline for responses: 12 August 2026

Stage 3 Responses reviewed: autumn 2026

Stage 4 Call for input outcome (decision or policy statement): autumn 2026

Your response, data, and confidentiality

You can ask us to keep your response, or parts of your response, confidential. We will respect this, subject to obligations to disclose information. For example, under the Freedom of Information Act 2000, the Environmental Information Regulations 2004, statutory directions, court orders, government regulations, or where you give us explicit permission to disclose. If you do want us to keep your response confidential, please clearly mark this on your response and explain why.

If you wish us to keep part of your response confidential, please clearly mark those parts of your response that you do wish to be kept confidential and those that you do not wish to be kept confidential. Please put the confidential material in a separate appendix to your response. If necessary, we will contact you to discuss which parts of the information in your response should be kept confidential and which can be published. We might ask for reasons why.

If the information you give in your response contains personal data under the General Data Protection Regulation (Regulation (EU) 2016/679) as retained in domestic law following the United Kingdom's withdrawal from the European Union ("UK GDPR"), the Gas and Electricity Markets Authority will be the data controller for the purposes of GDPR. Ofgem uses the information in responses in performing its statutory functions and in accordance with section 105 of the Utilities Act 2000. Please refer to our Privacy Notice on consultations.

If you wish to respond confidentially, we will keep your response confidential, but we will publish the number, but not the names, of confidential responses we receive. We will not link responses to respondents if we publish a summary of responses, and we will evaluate each response on its own merits without undermining your right to confidentiality.

How to track the progress of a call for input

1. Find the web page for the call for input you would like to receive updates on.
2. Click 'Get emails about this page', enter your email address and click 'Submit'.
3. You will receive an email to notify you when it has changed status.

A call for input has two stages: 'Open' and 'Closed'.

Send us your feedback

We believe that consultation is at the heart of good policy development. We are keen to receive your comments about this call for input. We would also like to get your answers to these questions:

1. Do you have any comments about the quality of this document?
2. Do you have any comments about its tone and content?
3. Was it easy to read and understand? Or could it have been better written?
4. Are its conclusions balanced?
5. Did it make reasoned recommendations?
6. Do you have any further comments?

Please send your feedback to stakeholders@ofgem.gov.uk

7. Conclusions and next steps

7.1 Ofgem will review and analyse responses to this call for input in autumn 2026. Based on the evidence gathered, Ofgem will assess whether to proceed with AI assurance guidance.

7.2 This assessment will consider:

- stakeholder interest and needs, including demand for AI assurance approaches
- feasibility and resource implications
- alignment with Ofgem's statutory duties and regulatory objectives, including impacts on energy system resilience, market functioning and consumer outcomes

7.3 If the case for AI assurance guidance is strong, Ofgem intends to launch a formal consultation on the detailed design and publication on AI assurance guidance in early 2027.

7.4 Ofgem will also ensure that clear communication is embedded throughout the process to prevent any misconceptions about any pending AI assurance guidance scope or regulatory status.