

By email to: EmergingTechnologies@ofgem.gov.uk

12/08/2026

RECCo response to: Call for Input – AI assurance in the energy sector

We welcome the opportunity to respond to this consultation. Our non-confidential response represents the views of the Retail Energy Code Company Ltd (RECCo) and is based on our role as operator of the Retail Energy Code (REC).

RECCo is a not-for-profit corporate vehicle ensuring the proper, effective, and efficient implementation and ongoing management of the REC arrangements. We seek to promote trust, innovation and competition, while maintaining focus on positive consumer outcomes. We are committed to ensuring that RECCo is an 'intelligent customer', ensuring the efficacy and value for money of the services we procure and manage on behalf of REC Parties, including those which constitute the REC Code Manager.

We support the development of clear and proportionate guidance to promote the safe, responsible and effective adoption of AI, and welcome Ofgem's engagement with this important area. However, AI assurance is a cross-cutting and rapidly developing issue: its principal risks, standards and assurance techniques are not unique to energy, while many AI systems, providers and use cases operate across sectors and national borders. It is therefore not clear that Ofgem is best placed to lead on a standalone energy-specific framework. We consider that Ofgem can make the greatest contribution by bringing its sector expertise to a coordinated cross-government and cross-regulatory approach, and by providing targeted clarification where established cross-sector principles require interpretation in a particular energy context.

While the appendix addresses the consultation questions to the extent relevant to RECCo's role, we would highlight three overarching points:

- 1. AI assurance should principally be addressed through a coordinated cross-sector framework.**

The principal risks and assurance techniques are not unique to energy, while many use cases combine energy data with other sectors and rely on internationally supplied AI models. Separate sector frameworks could create duplication, inconsistency and complexity that could risk constraining innovation and growth.

- 2. Responsibility for outcomes must remain with the organisation using AI.**

AI does not excuse a breach of regulatory obligations. Ofgem should retain its outcomes-based approach, allowing organisations flexibility in how they assure AI while holding them

accountable for consumer, market and operational outcomes. Assurance should be proportionate to the risk and impact of the use case.

3. **Ofgem's sector-specific role should be targeted rather than comprehensive.**
Ofgem could explain how cross-sector standards apply in particular energy contexts, especially critical infrastructure, cyber resilience and materially consumer-affecting uses. It should avoid duplicating general guidance or prematurely prescribing particular external audit, certification or assurance methods.

We would be happy to discuss any of our comments further.

Yours faithfully,

Kathryn Coffin
Regulatory Policy & Strategy Manager

Appendix: Consultation question themes

This appendix sets out RECCo's responses to the nine consultation question themes, to the extent relevant to our role and experience. The responses should be read alongside the overarching points in the covering letter. As several questions address overlapping issues, we have used cross-references where appropriate to avoid repetition and have indicated where RECCo is not best placed to provide a substantive response.

Question 1: Current AI assurance practices

RECCo is not best placed to comment on the current use or maturity of AI assurance across the energy sector. Regarding our own activities, we use AI within the REC Portal in the production of public analytics and to help our stakeholders find REC information through our AI assistant ERIN. Separately, much of our current work is focused on enabling stakeholders' own use of AI by making REC data and information machine-readable – for example, through our 'digital REC' and by following Ofgem's Data Best Practice Guidance on metadata.

Our existing REC services do not interact directly with consumers, although our future Consumer Consent Solution (CCS) will. CCS is an example of how responsibility for AI assurance may span sectors and organisations: its identity-verification process for consumers may use AI and may be provided by a specialist organisation outside the energy industry. There is also potential for future cross-sector uses of CCS, such as supporting any cross-sector Priority Services Register for vulnerable consumers.

These activities do not provide a sufficient basis on which RECCo could assess the maturity of AI assurance across the energy sector more generally.

Question 2: Risks and challenges

As explained in response to Question 1, RECCo does not have a sufficient basis on which to generally assess the maturity of AI assurance across the energy sector. Our comments are therefore limited to identifying relevant risks and practical challenges.

Automation of tasks in the energy industry is not new, although we agree that the probabilistic and constantly evolving nature of AI creates new risks. Specific risks relating to critical infrastructure, cyber resilience and consumer outcomes are considered in our responses to Questions 3 to 5. We consider that a further risk, not specifically mentioned in the consultation, is that AI is used for coding in software development without appropriate human oversight.

While some stakeholders may build their own in-house AI systems, many organisations are likely to choose from prebuilt, pre-trained and ready-to-use AI models originating from outside the UK. The capabilities and adoption of these models have the potential to evolve faster than the methods and technologies available to assure them, with their 'black box' nature creating challenges for understanding, transparency and explainability. These factors

may make it particularly difficult to assess and evidence risks, or to link the operation of an AI system to real-world outcomes.

More generally, AI assurance remains an emerging capability without a single agreed definition. While we understand the UK government's ambition to create a recognised AI assurance profession, this will take time to develop and the use of such services is not currently a regulatory requirement.

The consultation asks how organisations evidence that AI systems are operating as intended and delivering safe, fair and effective outcomes. It is unclear whether this means evidencing internally for their own confidence, evidencing to consumers to build their trust, or evidencing to the regulator to demonstrate compliance. With AI likely to be embedded within wider processes and systems, isolating its contribution to an outcome may be difficult. This technology-specific level of monitoring may also be unnecessary and inappropriate for Ofgem's purpose of monitoring compliance with overall regulatory and consumer outcomes.

As discussed in our response to Question 8, separate approaches developed by individual sector regulators could create duplication, misalignment, complexity and confusion, especially for organisations operating across different sectors.

Question 3: Critical infrastructure considerations

RECCo is not an operator of Critical National Infrastructure and is therefore not best placed to comment substantively on the appropriate level of AI assurance for high-impact or safety-critical systems. Our relevant observations on AI-related cyber and operational resilience are set out in response to Question 5.

Question 4: Consumer protection and fairness

As noted in response to Q1, RECCo's existing services do not interact directly with consumers, and we are therefore not best placed to comment in detail on the use of AI-driven pricing, segmentation or prioritisation. We nevertheless consider that AI assurance should support fair treatment by focusing on actual consumer outcomes, including outcomes for vulnerable groups, rather than solely on whether an AI system is operating as technically intended.

Most importantly, Ofgem's existing guidance on Ethical AI Use in the Energy Sector clarifies that stakeholders retain responsibility for the legal and regulatory consequences of how they use AI, and that any breach arising from its use does not excuse or mitigate that breach. This is the most critical expectation for an outcomes-focused regulator to set. Where AI informs pricing, segmentation or prioritisation, organisations should remain accountable for demonstrating that the resulting outcomes are fair, transparent and consistent with their obligations, including that vulnerable consumers are not disadvantaged or prevented from accessing services or appropriate redress.

As noted in our response to Question 2, the 'black box' nature of some AI models can create challenges for understanding, transparency and explainability. Assurance should therefore consider evidence of real-world outcomes across relevant consumer groups and be proportionate to the risk and impact of the use case. Risks and mitigations around potential consumer harm, including from the use of AI in customer service, apply across multiple sectors and all essential services. A coordinated cross-sector approach would be clearer and more consistent, with Ofgem providing targeted clarification where established principles require interpretation in a particular energy context.

Question 5: Cyber security and resilience

We note the concerns about the use of AI in energy Critical National Infrastructure, particularly where it may be embedded in high-impact or safety-critical operational systems. Although there may be a case for specific assurance requirements in such contexts, many of the relevant risks apply across Critical National Infrastructure and are closely connected with cyber and operational resilience. The government's response on reshaping cyber regulation in downstream gas and electricity confirms that DESNZ will review the application of the Network and Information Systems Regulations and that Ofgem will develop baseline cyber-resilience requirements for all licensees, working with the National Cyber Security Centre and seeking to minimise duplication with existing regimes. AI-related cyber risks should therefore be addressed through, and coordinated with, that developing regulatory framework, rather than through a separate or duplicative body of public AI-assurance guidance.

Question 6: Proportionality

Ofgem's existing guidance on Ethical AI Use in the Energy Sector already contains outcome-based principles and a risk approach to help stakeholders identify and manage AI risks.¹ We consider that this provides an appropriate starting point for proportionate AI assurance. Assurance should focus on results rather than prescribing the actions used to achieve them, giving organisations flexibility while holding them accountable for the end result.² Its nature and extent should reflect the nature, scale, risk and potential impact of the use case, with more rigorous assurance applied to higher-impact uses.

Most importantly, Ofgem's existing guidance clarifies that stakeholders retain responsibility for the legal and regulatory consequences of how they use AI, and that a resulting breach does not excuse or mitigate that breach. Tailoring assurance requirements should not weaken that accountability.

Care should also be taken not to be overly prescriptive. Over-prescription or information overload could create unnecessary cost and complexity and risk constraining innovation and growth. Smaller organisations should not automatically be expected to adopt the same

¹ Ofgem, Ethical AI use in the energy sector (version 2): <https://www.ofgem.gov.uk/guidance/ethical-ai-use-energy-sector>.

² Ofgem, Consumer Outcomes Strategic Direction: <https://www.ofgem.gov.uk/policy/consumer-outcomes-strategic-direction>.

governance structures, documentation or external-assurance arrangements as organisations operating high-impact systems.

As discussed in our response to Question 7, independent assurance may be one useful means of evidencing outcomes but should not be prescribed as a default requirement.

Question 7: External assurance and standards

We note the substantial amount of cross-sector guidance that already exists around AI governance and assurance, both within the UK and internationally, as listed on pages 7–8 of the consultation. We also note the development of AI management standards and frameworks by the International Organization for Standardisation (ISO), and the establishment of an AI Assurance Stakeholder Consortium, chaired by BCS, the Chartered Institute for IT, to develop and professionalise the AI assurance industry.³

We consider that existing and emerging cross-sector frameworks and standards should provide the starting point for AI assurance in the energy sector. As the energy industry becomes increasingly interconnected with other sectors through digitalisation and Smart Data Schemes⁴, AI risks and assurance responsibilities need to be considered across organisational and sectoral boundaries. Separate sector frameworks could create duplication, misalignment, complexity and confusion, especially for organisations operating across different sectors. As explained in our response to Question 8, Ofgem could provide targeted clarification where the application of cross-sector standards in a particular energy context might otherwise be unclear, rather than developing a separate comprehensive framework.

Independent assurance may have a useful role where it is proportionate to the risk and impact of the use case. It may provide access to specialist expertise, independent challenge and additional confidence in the operation of higher-risk AI systems. However, responsibility for legal and regulatory outcomes must remain with the organisation using AI. The use of an external auditor, certification or other assurance service should neither transfer that responsibility nor excuse or mitigate a breach of the organisation's regulatory obligations.

While we understand the UK government's ambition to create a recognised AI assurance profession, this will take time to develop and the use of such services is not currently a regulatory requirement. Attempting to cover the third-party provision of AI assurance services in detail in Ofgem guidance could result in undue prescription for an outcomes-

³ BCS, AI Assurance: www.bcs.org/the-home-of-the-ai-professional/ai-assurance-leading-a-new-profession-responsibly/.

⁴ For example, a current Call for Evidence by what is now the Department for Business, Innovation, Science and Trade (BIST) is seeking evidence on how Smart Data governance should align with developments in areas such as artificial intelligence, digital verification services and data protection, including where greater join-up could support trusted, secure and interoperable data sharing. Its considerations on potential join-up are cross-sector and are international, not just UK-focused. www.gov.uk/government/calls-for-evidence/smart-data-multi-sector-call-for-evidence. DESNZ plans to consult on Smart Data in energy before the end of 2026.

focused regulator, particularly as the consultation acknowledges that AI assurance is an emerging capability without a single agreed definition. Prescribing particular external audit, certification or assurance methods could also add cost and complexity, create reliance on approaches that may not yet be mature, and risk constraining innovation.

We therefore consider that Ofgem should recognise independent assurance as one potentially useful means of evidencing outcomes, rather than prescribing it as a default requirement. Organisations should retain flexibility to select assurance arrangements that are appropriate to the nature, scale and risk of their AI use, while remaining accountable for the resulting consumer, market and operational outcomes.

Question 8: Future guidance

We believe there may be a case for expanding Ofgem's existing AI guidance to reflect the existence of cross-sector AI assurance principles or guidance, as these mature. Future guidance would be most useful where it provides targeted clarification of how those principles apply in a specific energy context, such as energy trading, where this might otherwise be unclear to stakeholders. Examples and case studies should similarly focus on circumstances in which interpretation in an energy-specific context would add value. By contrast, risks and mitigations around the potential consumer harm arising from the use of AI in customer service are applicable to multiple sectors, including all essential services.

Future guidance could also clarify the types of evidence that Ofgem expects and the purpose for which that evidence would be used. The consultation asks how organisations evidence that AI systems are operating as intended and delivering safe, fair and effective outcomes. It is unclear whether this means evidencing internally for their own confidence, evidencing to consumers to build their trust, or evidencing to the regulator to demonstrate compliance.

In our view, evidence provided for regulatory purposes should be proportionate to the risk and impact of the use case and should focus on actual consumer, market and operational outcomes. With AI likely to be embedded within wider processes and systems, technology-specific monitoring may be unnecessary and inappropriate for Ofgem's purpose of monitoring compliance with overall regulatory and consumer outcomes.

For the reasons above, care should be taken not to make future guidance overly prescriptive or to duplicate or conflict with approaches that are, or should be, established on a cross-sector basis, ideally within a single overarching UK governance framework for AI. Recent government changes have redistributed the responsibilities of the former Department for Science, Innovation and Technology across government, including transferring overall AI strategy to the Cabinet Office and appointing a Minister of State for Artificial Intelligence jointly in the Cabinet Office and the Department for Business, Innovation, Science and Trade (BIST). While these changes provide a potential focal point for national leadership, it remains unclear how responsibility for cross-sector AI governance and assurance will operate in practice across central government, BIST, the Department for Digital, Culture, Media and

Sport (DCMS) and sector-specific bodies such as DESNZ and Ofgem for energy. We therefore encourage Ofgem to work with government and other sector regulators to support a coherent national framework, while limiting its own guidance to targeted clarification where an energy-specific interpretation is genuinely required.⁵

Question 9: Communication

As noted in our response to Question 8, it is unclear whether assurance evidence is intended for organisations' internal confidence, consumers, or the regulator. The appropriate form and content of any communication will depend largely on the nature and purpose of the assurance, the use case and the audience to whom it applies.

Information should be proportionate and tailored to the audience, focusing on the outcomes and protections relevant to them. However, while AI assurance remains an emerging capability without a single agreed definition, it is difficult to prescribe more detailed communication requirements. A consistent cross-sector approach would ultimately be clearer in building consumer understanding and trust than multiple sector-specific approaches.

Consumers are themselves increasingly using off-the-shelf AI models for advice and help in their daily lives. This includes, for example, asking them for advice on product selection, money saving and debt. Recent research by the Financial Conduct Authority has found that less than half of consumers understand the difference in the protections they have when using consumer-facing AI chatbots within regulated organisations' apps or websites (where consumers have the right of redress for poor outcomes) compared with using general-purpose AI tools for advice outside of the 'regulatory perimeter' (where no right of redress exists). This is an area where cross-sector communication to consumers would be beneficial, whether by UK government and/or through joined-up communication by sector regulators.⁶

⁵ For example, the Financial Conduct Authority has recently recommended strengthening regulator coordination in the absence of a dedicated AI regulator or cross-sector AI regime. It recommends greater regulator coordination on areas such as AI-enabled impacts on consumer redress and complaints systems, data governance and privacy, market structure and platform power, and risks affecting vulnerable consumers, access to services, and outcomes that span unregulated and regulated platforms.
www.fca.org.uk/publications/corporate-documents/mills-review.

⁶ <https://www.fca.org.uk/publication/external-research/ai-consumer-research.pdf>.