Chartered Institute of Internal Auditors

Chartered IIA
Office 202
Alliance House
12 Caxton Street
London SW1H 0QS

Chartered Institute of Internal Auditors – Ofgem AI Assurance Call for Input – Consultation Response

Ofgem
Emerging Technologies Team
10 South Colonnade
Canary Wharf
London
E14 4PU

Submitted by email to: **EmergingTechnologies@ofgem.gov.uk**

Dear Emerging Technologies Team,

The Chartered Institute of Internal Auditors (Chartered IIA) welcomes the opportunity to respond to Ofgem's call for input on AI assurance in the energy sector.

The Chartered IIA is the professional body for internal auditors in the UK and Ireland, representing over 10,000 members working across all sectors, including the energy sector. Internal audit provides independent, objective and risk-based assurance and advice to boards, audit committees and senior management on whether governance, risk management and internal controls are designed and operating effectively.

Our central recommendation is that any future Ofgem guidance, framework or regulatory approach to AI assurance in the energy sector should explicitly recognise internal audit as a key source of independent assurance within a broader AI assurance ecosystem that includes governance, risk management, controls, monitoring, human oversight and specialist assurance where appropriate.

This is particularly important in the energy sector. Ofgem's call for input rightly recognises that AI is increasingly being deployed across a wide range of activities, including demand forecasting, system balancing, network planning, asset maintenance, trading, pricing and market operations. AI is also being used in customer-facing activities, including customer service, vulnerability support and billing. It also recognises that AI assurance should help organisations demonstrate that AI systems are safe, secure, fair and effective in practice. As AI adoption accelerates, there is a risk that governance, risk management and control arrangements fail to keep pace. Effective AI assurance can help organisations identify where this gap is emerging and provide boards with independent insight into whether AI-related risks are being understood and managed appropriately.

To help inform our response to this consultation, the Chartered IIA convened a roundtable on AI assurance with internal audit leaders and audit committee members from the energy sector. The roundtable identified or reinforced the following key Chartered IIA points, which are expanded on further in our full consultation response:

- AI assurance maturity is still developing - with organisations taking different approaches to AI governance and assurance.
- There are challenges around maintaining visibility over AI use, particularly where AI is embedded within existing business processes or third-party systems.

Chartered Institute of Internal Auditors

Chartered IIA
Office 202
Alliance House
12 Caxton Street
London SW1H 0QS

- There is a need for practical, proportionate and risk-based guidance for boards, audit committees and assurance functions.
- Internal audit should not be treated as an afterthought in AI assurance; it is already experienced in providing independent assurance and advice over complex and fast-moving risks, including cyber security, data, technology, operational resilience, third-party risk and regulatory compliance.
- AI should be recognised as another significant risk area, one where internal audit has a critical role to play.
- Ofgem should encourage organisations to maintain visibility of where AI is being used, including AI being embedded in third-party tools and business processes.
- Ofgem guidance should emphasise the importance of clear accountability, human oversight, traceability of outputs, evidence of control effectiveness and independent assurance over the most significant AI risks.
- Given the criticality of many energy sector use cases, Ofgem guidance should also recognise that assurance arrangements may need to evolve as AI systems, risks and operating environments change over time.

We would welcome the opportunity to continue engaging with Ofgem as this work develops. We are happy for our response to be published.

Yours sincerely,

Mo Warsame

Senior Policy and Public Affairs Executive

Chartered Institute of Internal Auditors

Question 1 – Current AI assurance practices

The Chartered IIA believes that AI assurance practices in the energy sector are developing rapidly, but remain varied across organisations. As a result, there is currently no common approach to demonstrating that AI systems are operating safely, effectively and as intended.

From an internal audit perspective, effective AI assurance should extend beyond technical testing and assess whether governance arrangements, risk management processes (including horizon scanning) and controls are operating effectively in practice. Internal audit provides independent assurance and advice to boards, audit committees and senior management in these areas. In the context of AI, this includes assessing whether organisations understand where AI is being used, whether the associated risks are being managed appropriately, whether there is sufficient oversight of AI-enabled processes and whether boards receive meaningful information about AI-related risks and outcomes. Internal audit can also challenge boards to ensure that they have sufficient forward-looking information and leading risk indicators to respond quickly to emerging opportunities and threats. This is consistent with the Chartered IIA's Internal Audit Code of Practice, which explicitly includes technology, cyber, digital and data risks, including the use of emerging technologies such as artificial intelligence, within the scope of internal audit.

Chartered Institute of Internal Auditors

Chartered IIA
Office 202
Alliance House
12 Caxton Street
London SW1H 0QS

Senior internal audit leaders in the energy sector highlighted significant variation in current practices. Some organisations described developing AI governance arrangements, including AI policies, governance committees, risk assessments and AI registers. Others reported that they are still trying to understand where AI is being used across the organisation and how it should be incorporated into audit planning. A common challenge is maintaining visibility of AI use, including "shadow AI" operating outside established governance processes.

To address these risks, some organisations have introduced AI governance committees, monitoring activities, control testing, output validation and independent assurance by internal audit. Some organisations are also exploring technology-enabled assurance approaches, including process mining, data analytics and continuous monitoring. However, there remains significant variation in maturity and no shared understanding of what good AI assurance looks like in practice in the energy sector.

A recurring theme raised by internal auditors was the importance of visibility, traceability and human oversight. Organisations face challenges in validating AI outputs, understanding how outputs are generated and obtaining sufficient evidence that systems are operating as intended. Concerns also arise around explainability, data lineage and identifying where AI is embedded within business processes. These challenges are particularly important where organisations rely on AI outputs for operational decision-making, regulatory reporting or customer-facing activities. This reinforces the importance of maintaining effective human oversight.

The Chartered IIA's recent white paper, **Artificial Intelligence and Internal Audit: Opportunities, Risks and Future Directions**, identified a dual role for internal audit: using AI within the internal audit function and providing assurance over AI deployment across the organisation. While AI introduces new considerations around areas such as model risk, explainability and data governance, internal auditors already have extensive experience providing assurance over technology, cyber security, data, operational resilience and other complex risk areas. As organisations increase their use of AI, internal audit functions are continuing to build capability through professional guidance, knowledge-sharing and specialist expertise where appropriate, enabling them to provide increasingly effective assurance over AI-related risks. The Chartered IIA and The Institute of Internal Auditors Global are also supporting the profession through guidance, resources, the AI Auditing Framework and practitioner forums that help internal auditors build capability and share emerging good practice in relation to AI-related risks and assurance.

We recommend that any future AI assurance framework or regulatory approach explicitly recognises internal audit as a critical source of independent assurance and advice over AI governance, risk management and controls. Any accompanying guidance should make clear that effective AI assurance extends beyond technical testing to include governance, monitoring, accountability, human oversight and independent assurance. It should also provide practical examples of assurance activities and evidence organisations can use to demonstrate that AI systems are delivering safe, fair and effective outcomes.

Question 2 – Risks and challenges

The Chartered IIA believes that the main barriers to effective AI assurance are not solely technical. They are also governance, control and accountability challenges. Organisations may struggle to provide effective assurance where they lack visibility of AI use, where accountability is unclear, or where AI is embedded within third-party systems that limit transparency and access to information.

Chartered Institute of Internal Auditors

Chartered IIA
Office 202
Alliance House
12 Caxton Street
London SW1H 0QS

Key risks associated with AI use include poor data quality, limited explainability, over-reliance on AI outputs, weak human oversight, third-party dependency, cyber security vulnerabilities, inaccurate or unreliable outputs, bias, ineffective escalation and uncertainty over whether controls remain effective as AI-enabled systems evolve. These risks are particularly significant in the energy sector where AI supports operational decision-making, regulatory reporting, customer service, vulnerability support, pricing, billing or asset management. At the same time, organisations that are slow to adopt AI may face their own risks, including missed opportunities to improve efficiency, resilience and service delivery. Effective AI assurance should therefore help organisations adopt AI with confidence, while ensuring that risks are appropriately understood and managed.

From an internal audit perspective, many AI-related risks are not entirely new. Internal audit already provides assurance over areas such as cyber security, technology risk, data governance, third-party risk, operational resilience and regulatory compliance. However, AI can amplify these risks and create new challenges around explainability, traceability, monitoring and accountability, making it more difficult to demonstrate that risks are effectively managed.

A recurring concern was that organisations may adopt AI faster than governance, risk management and assurance arrangements can keep pace. A significant challenge is identifying where AI is being used, particularly where AI is embedded within business processes, third-party tools or existing technology platforms. In some cases, organisations may rely on decisions, outputs or controls without realising that AI has influenced them, making effective assurance more difficult.

Even where organisations are aware of AI use, they may face challenges in understanding how AI-generated outputs are produced and determining whether they can be relied upon for decision-making. This creates a broader assurance challenge around explainability, traceability and evidencing how AI-supported decisions, recommendations and outcomes have been reached.

Where internal audit has appropriate visibility of AI use and access to relevant information, it can help organisations in the energy sector manage these risks by providing independent assurance over whether AI-related risks have been identified and assessed appropriately; whether governance, oversight and controls are operating effectively; whether boards receive reliable information on AI-related risks; and whether monitoring, escalation and accountability arrangements continue to operate as AI systems evolve.

We therefore recommend that Ofgem should encourage organisations to maintain visibility of where AI is being used, including AI embedded in third-party tools and business processes. Guidance should emphasise the importance of clear accountability, human oversight, traceability of outputs, evidence of control effectiveness and independent assurance over the most significant AI risks. Given the criticality of many energy sector use cases, guidance should also recognise that assurance arrangements may need to evolve as AI systems, risks and operating environments change over time.

Question 3 – Critical infrastructure considerations

The Chartered IIA believes that AI assurance should reflect the importance of the energy sector as critical national infrastructure. Where AI is used in operationally significant, safety-critical or infrastructure-related activities, the level of assurance should be more rigorous than for lower-risk administrative or back-office uses. Assurance approaches should be proportionate to the potential impact of the AI use case and the consequences of failure.

Chartered Institute of Internal Auditors

Chartered IIA
Office 202
Alliance House
12 Caxton Street
London SW1H 0QS

Ofgem's consultation rightly recognises that AI assurance approaches must reflect the characteristics of the energy system. This is because AI failures in the energy sector may have consequences beyond financial loss or operational inconvenience. Depending on the use case, failures may affect system reliability, service continuity, operational resilience and the safe operation of critical national infrastructure. In some circumstances, failures could contribute to service disruption or power outages, with potentially significant consequences for consumers, businesses and essential services. The Chartered IIA also recognises the importance of highlighting the unique characteristics of the energy sector when considering AI assurance.

Failures within energy infrastructure can have direct consequences for public safety, environmental protection and the continuity of essential services. AI also presents significant opportunities in these environments, including helping organisations identify risks, improve resilience and help prevent incidents before they occur. However, where AI is deployed in operationally significant or safety-critical settings, assurance arrangements must be capable of providing confidence that systems are operating as intended and that risks are appropriately controlled.

AI should not be treated as a single, uniform technology. Different AI models and use cases create different risks and therefore require different controls, testing and assurance approaches. The Chartered IIA believes that risk-based assurance should remain central. AI should be assessed in the context of the business process it supports. Higher-risk AI deployments will generally require stronger governance, more robust controls, greater transparency, more frequent monitoring and enhanced independent challenge than lower-risk uses.

Internal audit can contribute by ensuring that AI risks are considered within risk-based audit planning and by assessing whether higher-risk uses of AI receive an appropriate level of scrutiny. The role of internal audit is not to duplicate technical model validation, but to provide independent assurance that governance arrangements, controls, monitoring activities and escalation processes are proportionate to the level of risk and are operating effectively in practice.

We therefore recommend that Ofgem adopts a risk-based AI assurance framework for critical infrastructure. Assurance expectations should increase in line with the potential impact of the AI use case, with more rigorous requirements applying where AI supports operationally significant, safety-critical or resilience-critical activities. Future approaches should also recognise that different AI technologies and applications may require different assurance approaches.

Question 4 – Consumer protection and fairness

The Chartered IIA believes that AI assurance can support fair consumer outcomes by providing confidence that appropriate governance, controls and oversight arrangements are in place. Internal audit can play an important role in providing independent assurance that organisations have processes to monitor outcomes, identify unintended consequences and respond appropriately where issues arise.

Effective AI assurance should include human oversight, validation of AI outputs and effective escalation processes. Where errors are not identified and addressed appropriately, AI systems may create ethical concerns, bias or unintended consequences. These risks may be particularly relevant where AI influences customer interactions, billing processes, vulnerability assessments and support, complaints handling or other decisions that have a direct impact on consumers.

Chartered Institute of Internal Auditors

Chartered IIA
Office 202
Alliance House
12 Caxton Street
London SW1H 0QS

Internal audit can support organisations by providing assurance that governance arrangements are operating effectively, that fairness and bias risks have been considered and that significant AI-enabled decisions are subject to appropriate oversight and challenge. This includes providing assurance that products, services and supporting processes continue to operate in customers' interests and do not result in poor customer treatment. This aligns with the Chartered IIA's Internal Audit Code of Practice, which highlights the role of internal audit in evaluating conduct risk, customer outcomes and whether products, services and supporting processes are designed and controlled appropriately.

We therefore encourage Ofgem to ensure that future AI assurance approaches include assessment of consumer outcomes, monitoring for bias, consideration of vulnerable consumers and processes for identifying and responding to unintended consequences.

Question 5 – Cyber security and resilience

The Chartered IIA believes that AI assurance should be aligned with existing cyber security, technology risk and operational resilience frameworks.

From an internal audit perspective, many AI-related risks intersect with established risk areas that organisations already manage, including cyber security, data governance, technology controls, third-party risk, business continuity and operational resilience. However, AI can also introduce additional risks, including cyber security vulnerabilities, unreliable outputs, over-reliance on automated decisions, reduced transparency and vulnerabilities associated with third-party AI tools.

The Chartered IIA emphasises the importance of aligning AI assurance with existing risk and control frameworks. Internal audit leaders in the energy sector highlighted the need for human oversight, ongoing monitoring, error reporting and escalation processes, particularly where AI outputs may influence operational, regulatory or business-critical activity. There were also concerns about visibility of AI use, the challenges of assuring AI embedded within third-party systems and the need to ensure that governance and controls keep pace with the rapid adoption of AI technologies.

These considerations are particularly important within the energy sector, where operational resilience and cyber security are fundamental to the safe delivery of critical national infrastructure. AI assurance should therefore support organisations in identifying, monitoring and responding to both traditional cyber risks and AI-specific risks, while ensuring that resilience arrangements remain effective as technologies and threat landscapes evolve. This is consistent with wider government thinking on cyber governance, including the NCSC Cyber Governance Code of Practice, which explicitly recognises internal audit’s role in providing boards with independent assurance over cyber risks.

Internal audit can support resilience by providing independent assurance over whether AI-related cyber, operational and third-party risks have been identified appropriately, whether controls are designed and operating effectively, whether incidents are escalated and learned from appropriately and whether boards receive reliable information on the risks associated with AI adoption.

We therefore recommend that Ofgem's future guidance encourages organisations to align AI assurance with existing cyber security, operational resilience and technology risk frameworks. Guidance should recognise that effective assurance requires ongoing monitoring, human oversight and clear accountability, and that internal audit can provide independent assurance over whether AI-related risks and controls are being managed effectively in practice.

Chartered Institute of Internal Auditors

Chartered IIA
Office 202
Alliance House
12 Caxton Street
London SW1H 0QS

Question 6 – Proportionality

The Chartered IIA strongly supports a proportionate, risk-based approach to AI assurance. A one-size-fits-all approach would be inappropriate. It could overburden lower-risk uses of AI while failing to provide sufficient assurance over higher-risk or operationally significant use cases.

Proportionate AI assurance should take account of the purpose of the AI use, the risks associated with the use case, the quality and sensitivity of the data involved, the degree of human oversight, the reliance placed on AI outputs, the involvement of third parties and the potential consequences if the AI produces inaccurate or unreliable outputs. The level of assurance should reflect both the likelihood of risks occurring and the potential impact of those risks on consumers, operational resilience, regulatory compliance or critical services.

The Chartered IIA believes that maintaining a risk-based approach to assurance is essential. AI should be considered in the context of the business process it supports, and the presence of AI does not automatically make an activity high-risk. However, AI may change the nature of the risk and the type of assurance required. Different forms of AI may require different assurance approaches depending on the technologies involved, the use case and the risks presented. Assurance should not focus solely on implementation. Automated controls can degrade over time, and organisations need ongoing monitoring and review to ensure that controls remain effective as AI-enabled systems evolve.

Internal audit is well placed to apply this type of risk-based judgement. Internal audit planning is based on risk rather than applying the same level of scrutiny to every activity. This approach should also apply to AI assurance. Lower-risk uses may require basic governance, acceptable use controls and data handling safeguards. Higher-risk uses may require deeper testing, more frequent monitoring, stronger evidence, specialist input and reporting to boards or audit committees.

We therefore recommend that Ofgem's guidance should support proportionate assurance by setting out principles and practical examples rather than detailed prescriptive requirements. Guidance should help organisations distinguish between lower-risk AI use and higher-risk use that requires stronger oversight, monitoring and independent assurance, while recognising that different AI technologies and use cases may require different assurance approaches.

Question 7 – External assurance and standards

The Chartered IIA supports the development of practical, energy sector-specific guidance on AI assurance. Existing frameworks and standards provide useful foundations, but they do not remove the need for clear sector-specific guidance that reflects the risks, operational environment and public interest role of the energy sector.

The Chartered IIA is concerned that AI assurance may be viewed primarily through the lens of external assurance. External assurance may be valuable in some circumstances, particularly where specialist technical expertise is required, but it should not be seen as the only or primary route for AI assurance. Internal audit provides independent assurance to boards and audit committees on whether governance, risk management and internal controls are operating effectively.

Chartered Institute of Internal Auditors

Chartered IIA
Office 202
Alliance House
12 Caxton Street
London SW1H 0QS

Internal audit has decades of experience providing assurance across complex risks, including cyber security, data, technology, safety, operational resilience, third-party risk and regulatory compliance. It is therefore important that any future AI assurance approach recognises internal audit from the outset, rather than treating it as secondary to external assurance.

Internal audit's role should sit at the heart of organisational assurance arrangements, working alongside management, risk, compliance and specialist assurance providers. Where specialist technical expertise is required, internal audit may draw on subject matter experts, external support or specialist assurance providers. However, boards and audit committees still need an integrated view of whether AI risks are being governed and controlled effectively across the organisation, and internal audit is well placed to provide that independent perspective.

We therefore recommend that Ofgem explicitly recognises internal audit in any future AI assurance framework, guidance or regulatory approach. It should make clear that independent assurance may be delivered through internal audit, external review or specialist assurance depending on the risk, context and available expertise. It should avoid implying that external assurance is the default or only credible assurance route and instead recognise the complementary role that internal audit can play within a broader AI assurance framework.

Question 8 – Future guidance

The Chartered IIA believes that future AI assurance guidance would be most useful if it is practical, proportionate and focused on helping organisations understand what good practice looks like. The guidance should not be overly prescriptive. It should recognise that organisations in the energy sector are at different stages of AI maturity and that AI use cases vary significantly in risk, complexity and impact.

The guidance should cover the areas where boards, audit committees and assurance functions need the greatest clarity, including governance and accountability, risk assessment, data quality, human oversight, third-party dependencies, testing and validation, monitoring, incident reporting, escalation and board reporting. Clear articulation of responsibilities across management, risk and compliance functions, and internal audit would help organisations understand how AI-related risks should be managed, overseen and independently assured.

Senior internal audit leaders in the energy sector highlighted a strong appetite for practical guidance rather than high-level principles alone. There is a need for guidance on third-party AI risk, particularly where organisations have limited visibility of AI embedded within supplier systems. There is also a need for practical examples, case studies and sector-specific expectations that help organisations understand what evidence is sufficient in practice and what effective assurance looks like at different levels of AI maturity.

Organisations, boards, audit committees and assurance providers would benefit from guidance that helps establish a common understanding of what should be assured, what evidence is useful and how AI-related risks should be reported and escalated. This would support greater consistency while avoiding the creation of a rigid or overly prescriptive assurance model.

Chartered Institute of Internal Auditors

Chartered IIA
Office 202
Alliance House
12 Caxton Street
London SW1H 0QS

We therefore recommend that Ofgem's future guidance should include practical examples, case studies and proportionate expectations for assurance across the AI lifecycle – from design and testing through to deployment, monitoring and review. It should be designed for boards, audit committees, internal audit, risk, compliance, technology and operational teams, rather than solely for AI specialists, and should help organisations apply assurance approaches that are proportionate to the risks presented by different AI use cases.

Question 9 – Communication

The Chartered IIA believes that effective communication around AI assurance is particularly important for boards, audit committees and senior management, given their oversight of governance, risk management and internal controls. Reporting should be clear, concise and focused on the most significant AI-related risks and issues.

Boards and audit committees need meaningful information on AI use, higher-risk use cases, controls, assurance activity, identified issues and management actions. Reporting should support effective challenge and decision-making while remaining accessible to non-specialists.

Senior internal audit leaders in the sector highlighted that board understanding of AI risk is still developing. They also stressed the importance of board education, regular updates and clear summary reporting. Boards and audit committees need to understand the opportunities presented by AI, the limitations of AI outputs, the risks of over-reliance and any assurance gaps. This reflects the evolving nature of AI risk and the need for ongoing board engagement.

Internal audit can support effective communication by providing independent reporting on AI-related risks, assurance coverage, control weaknesses, emerging issues and whether AI governance arrangements are functioning effectively.

We therefore recommend that communication and reporting are treated as core components of effective AI assurance. Future guidance should help organisations communicate AI risks, controls, incidents and assurance outcomes clearly to boards, audit committees and senior management in a way that supports effective oversight and informed decision-making.