Chartered Institute of Internal Auditors

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

Chartered Institute of Internal Auditors – Reshaping Cyber Regulation in Downstream Gas and Electricity Consultation – DESNZ/Ofgem – Consultation Response

Question 1 — Is there a need to expand the scope of our cyber oversight and assurance to cover more DGE operators?

The Chartered Institute of Internal Auditors (Chartered IIA) agrees there is a clear need to expand the scope of cyber oversight and assurance across the Downstream Gas and Electricity (DGE) sector. However, the current proposals need to go further by explicitly recognising and embedding the important role of internal audit within the cyber regulatory framework for DGE operators. An appropriately positioned and resourced internal audit function provides boards and senior management with independent assurance that the controls managing cyber risk are operating effectively. For large wholesale operators forming part of the UK's critical national infrastructure, this is not a disproportionate requirement; internal audit should already be in place, and as the scope expands, the framework should formalise the role of internal audit. This position is consistent with the DSIT and NCSC Cyber Governance Code of Practice, which explicitly recognises internal audit's role in providing boards with independent assurance over cyber risks. Formalising this expectation within the DGE regulatory framework would bring it into line with established government guidance on cyber governance.

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 assurance to boards (typically via the audit committee) and senior management that governance, risk management and internal controls — including those relating to cyber security — are working effectively to help protect organisations from threats and deliver long-term resilience.

As the consultation rightly identifies, the energy system has become more distributed and digitalised since the Network and Information Systems (NIS) Regulations came into force in 2018, and the cyber threat to UK critical national infrastructure has continued to grow. The recent attack on the Polish energy system, which targeted around 30 distributed renewable assets with the potential to impact over 500,000 customers, demonstrates the scale and ambition of cyber attacks targeting national infrastructure. The threat is also growing here in the UK, with the NCSC handling a record 204 nationally significant cyber incidents last year, up from 89 the year before, with nearly half relating to national infrastructure.

The Chartered IIA's Risk in Focus 2026 research, our annual flagship survey of nearly 900 Chief Internal Auditors across the UK and Europe, similarly found that cybersecurity is the biggest risk facing organisations going into 2026. The survey also found that cybersecurity is the risk area in which internal audit spends the most time and effort auditing. As the UK's reliance on a secure and resilient energy system increases, the consequences of security breaches causing widespread disruption are rising.

The Chartered IIA's research into the internal audit capabilities of retail energy suppliers, though conducted in a different part of the energy sector than wholesale DGE, highlights a directly relevant governance risk. We found that of the 30 or so retail energy suppliers that collapsed since 2021, including Bulb, the UK's seventh largest, none had an internal audit function. Following this, we engaged with

Chartered Institute of Internal Auditors

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

Ofgem on strengthening the Financial Responsibility Principle, which now requires retail energy suppliers to explain their internal audit capability or justify its absence. Despite this, our most recent research found that among the top 28 retail energy suppliers, 11 appear not to have an internal audit function, including the largest supplier outside the Big Six energy providers. We continue to raise this issue with Ofgem.

While this research concerns retail rather than wholesale energy, the governance lesson is directly applicable — and the stakes in wholesale DGE are considerably higher. DGE wholesale operators are a part of critical national infrastructure, potentially exposed to state-sponsored cyber threats from hostile actors. If retail suppliers without internal audit have proven vulnerable to financial and operational failure, the consequences of equivalent governance gaps in wholesale DGE would be far more serious for energy security and for consumers.

Expanding the scope of cyber oversight and assurance across the DGE sector is therefore the right step, and explicitly embedding internal audit within the framework is essential to ensuring the expanded requirements deliver the resilience they are designed to achieve.

Question 2 — Views on the proposal to expand scope by (a) reviewing NIS applicability and (b) introducing baseline cyber resilience requirements for all Ofgem licensees.

The Chartered IIA supports both elements of the proposal. As the proposals are taken forward, we strongly recommend that DESNZ and Ofgem explicitly recognise within the proposals the role internal audit can play in supporting licensees to adhere to the new requirements and in giving boards and senior management independent assurance that the controls put in place to meet those cyber resilience requirements are operating effectively. This is particularly valuable for licensees newly brought within scope, where cyber governance arrangements may be less developed and where internal audit can help ensure new requirements are embedded effectively from the outset.

Setting a clear expectation that licensees consider their internal audit capability as part of their cyber governance arrangements would help ensure that the proposed requirements deliver the stronger oversight, assurance and resilience improvements DESNZ and Ofgem are seeking. We expand on how this could be done in our response to Question 3.

Question 3 — Are there alternative approaches we should consider on how to expand the scope of cyber oversight and assurance and build resilience across the sector?

The Chartered IIA recommends that the cyber regulatory framework for DGE clearly and explicitly recognise the role of internal audit in supporting boards and senior management to oversee cyber risk, and the critical role that internal audit can play in strengthening cyber oversight and assurance.

Internal audit provides independent and objective assurance to the board (typically via the audit committee) and senior management that the organisation's governance, risk management and internal controls are operating effectively. For cyber security, this includes assurance over how cyber risks are identified and managed, how internal controls are designed and applied, how cyber attacks are prepared for, responded to and learned from, and how supply chain and third-party risks are governed.

Chartered Institute of Internal Auditors

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

Recognising the role of internal audit is well established across regulated sectors. Ofgem's own Financial Responsibility Principle already requires domestic energy suppliers to explain their internal audit capability or justify its absence. In financial services, the FCA Internal Controls Handbook and the PRA Rulebook embed internal audit within governance expectations. The DSIT & NCSC Cyber Governance Code of Practice explicitly references internal audit's role in providing boards with assurance over cyber risks. Recognising internal audit within the DGE cyber regulatory framework would bring the sector into line with this approach and reinforce the consistency of government guidance on cyber governance.

For large DGE wholesale operators who are a fundamental part of critical national infrastructure, requiring an appropriately positioned and resourced internal audit function is proportionate, appropriate, and consistent with expectations across other regulated sectors. These are large organisations, many potentially exposed to state-sponsored cyber threats from hostile actors, for whom independent assurance over cyber governance, risk management and internal controls is essential. The framework should formalise this expectation explicitly rather than leaving it to individual operators to determine what level of independent assurance is necessary.

The Chartered IIA calls on DESNZ and Ofgem to embed this requirement within the regulatory framework and would welcome the opportunity to work with both departments and NCSC to develop the details of how this is achieved in the framework.

Question 9 — What are your views on the proposed principles for baseline requirements?

The Chartered IIA supports the proposed principles, which together set a sensible foundation for the baseline. We particularly welcome the principle that baseline requirements should be independently assured to verify their effectiveness. Internal audit can play a critical role in providing this assurance, giving boards and senior management confidence that the controls in place to manage cyber risk are operating effectively. We therefore recommend that the baseline requirements explicitly recognise internal audit as a means through which the principle of independent assurance can be delivered.

The Cyber Essentials scheme, which the consultation proposes as the basis for the baseline, focuses on technical controls and, as the consultation itself recognises, does not extend to the wider areas where mature cyber resilience needs to be embedded, including governance, training, supply chain, and response and recovery. These are exactly the areas where internal audit provides independent assurance to boards. Internal audit provides ongoing assurance that the wider controls relating to cyber risk are robust and working as intended, and supports licensees in demonstrating the effectiveness of the practices they already have in place.

We recommend that, in developing the baseline requirements, DESNZ and Ofgem explicitly recognise internal audit as a means through which the principle of independent assurance can be delivered. This would strengthen the principle further by ensuring that licensees have access to ongoing, independent assurance on their cyber resilience, alongside any other arrangements that form part of the final scheme. We would welcome the opportunity to engage further with DESNZ, Ofgem and NCSC as the baseline requirements are developed.