UK Government

Energy Sector Cyber Security Strategy

Building resilience through partnership

DESNZ, NCSC, Ofgem & NESO (2026)

Authors

- Department for Energy Security and Net Zero (DESNZ)
- National Cyber Security Centre (NCSC)
- Office of Gas and Electricity Markets (Ofgem)
- National Energy System Operator (NESO)

Contents

Ministerial foreword

I am pleased to present the Energy Sector Cyber Security Strategy, which sets out an ambitious vision and four-year roadmap of activities for the UK's energy sector as it transitions to deliver Clean Power 2030. This vision cannot be achieved by any organisation in isolation, so I am delighted that the strategy has been developed jointly with Office of Gas and Electricity Markets, the National Cyber Security Centre, and the National Energy System Operator. I look forward to working together with them to strengthen the cyber security of the UK's energy sector.

Energy touches the heart of everyone's lives in this country. It heats our homes, powers our businesses, fuels our economy and underpins the services we rely on every day. A secure, reliable energy system is not only essential to our economic prosperity, but fundamental to our national security. The UK continues to navigate a changing global landscape, increasing cyber threat and transformation to its energy system for the future. Ensuring that our energy remains affordable, resilient and secure is critical to protecting households, supporting growth, and safeguarding the country's interests.

Great Britain starts from a position of strength. We have a resilient and reliable energy system, supported by world-class expertise across government, regulators and industry. But parts of our infrastructure were not designed for today's highly digital, interconnected and decentralised system. As we build new networks, deploy renewable technologies, and bring new actors into the market, we must ensure cyber security is built in from the start – not added as an afterthought.

The Energy Sector Cyber Security Strategy sets out what the government will do to protect the energy system and its consumers, and how we will partner with industry to mitigate cyber risks. Securing our energy system is a shared responsibility. I expect boards, executives and leaders across the energy sector to treat cyber risk with the same seriousness as safety, reliability and operational resilience. By working in partnership, we can secure the energy system we rely on today, while building a clean, digital and resilient energy system fit for the future – delivering Clean Power 2030, Net Zero, and long-term energy security.

Rt Hon Michael Shanks MP,
Minister for Energy, Department of Energy Security and Net Zero

1. Introduction

Secure, clean, and affordable energy underpins our economy. It is vital that our energy system is secure and resilient to those who wish to do us harm. Amplified by geopolitical risks from global conflicts, we have seen an increasing use of cyber attacks and a growing number of actors prepared to employ them, with aspirations to disrupt western Critical National Infrastructure (CNI).[1] Maintaining secure energy supplies is a government and sector priority, and a cyber secure and resilient energy system now, and in the future, is central to this.

The National Cyber Security Centre (NCSC) has noted a stark increase in the threat to our CNI systems, as our adversaries seek to compromise these systems to achieve a range of outcomes, from financial gain and economic advantage, to pre-positioning, espionage and disruptive and destructive attacks.[2] In recent years we have seen how cyber-attacks can have far reaching impacts, including on essential services. In the increasingly unstable geopolitical landscape and considering the attractiveness of energy as a target by high capability state actors, it is now, more than ever, that robust and coordinated cross-sector action is required to enhance sector security and resilience.

Great Britain (GB) boasts a reliable, resilient energy system. However, our energy infrastructure was never designed with rapid digitalisation and decentralisation in mind. We need to ensure that our infrastructure remains resilient to the growing cyber threat.

The UK government's Clean Power 2030 (CP2030) report sets out an ambitious plan to deliver its Net Zero targets, ensure a secure and affordable energy supply, foster new industries and investments, and protect the environment from climate change.[3] As we deliver this ambition, the energy sector will undergo transformation at a scale never experienced before. New energy resources will enter the market, renewable technologies will be rapidly deployed, infrastructure will be significantly upgraded and expanded, and digital solutions from new market participants will revolutionise how the energy sector meets consumer demand.

The transition to a clean power system, driven by the adoption of new energy technologies, will fundamentally reshape the environment in which threat actors operate. If security is not embedded throughout the transformation of the energy sector, adversaries are likely to exploit emerging vulnerabilities and gaps. This was highlighted by the cyber attack in Poland in December 2025, where threat actors attempted to disrupt energy systems by targeting distributed energy resources.[4]

[1] Critical National Infrastructure is defined as those critical elements of infrastructure, the loss or compromise of which could result in:
a) Major detrimental impact on the availability, integrity or delivery of essential services and/or
b) Significant impact on national security, national defence, or the functioning of the state.
[2] NCSC (2025) 'It's time to act - NCSC Annual Review 2025' (viewed 12 March 2026)
[3] DESNZ (2024) 'Clean Power 2030 Action Plan - GOV.UK' (viewed 12 March 2026)
[4] CERT Polska (2026) 'Energy Sector Incident Report - 29 December 2025' (viewed 12 March 2026)

However, we recognise that, in developing the cyber resilience of the energy sector, there are structural challenges that need to be overcome. The UK faces a significant shortage of professionals that have the required combination of cyber and engineering skills, with an insufficient number of security-cleared industry staff. Additionally, there is a need to continue to raise awareness at pace about the critical nature of cyber security.

Since the introduction of the Network and Information Systems (NIS) Regulations in 2018 there has been a significant shift in culture.[5] However, the NIS Regulations are relatively recent, and their coverage is limited. It is imperative for us to prioritise engagement with companies, boards, and employees to shift cyber security attitudes, particularly for the most critical parts of the energy system. Furthermore, the integration of legacy infrastructure with new technologies presents a complex challenge, requiring careful management to ensure seamless and secure operations. Addressing these issues is crucial to successfully navigating the path to Net Zero while safeguarding our energy sector against evolving cyber threats.

This strategy sets out a four-year plan from 2026 - 2030 ensuring that:

- cyber security risks to the energy sector are identified, assessed, understood and managed
- cyber security and resilience is increased at pace across the sector, appropriate to the risks faced
- response and recovery plans are in place and tested for cyber incidents, including sophisticated attacks from capable actors
- cyber requirements are expanded in scope and depth, proportionate to the risk faced and keep pace with the evolving threat and system landscape

We will deliver the above by focusing on the following strategic outcomes:

- **Enhancing our understanding of threat, vulnerability, and risk**: Develop and maintain a comprehensive understanding of the whole energy system and its component parts (including critical suppliers) - highlighting dependencies, high impact points of failure and areas of risk concentration. Carry out risk assessments to understand the impact of security threats to the system, identifying the key security risks and most critical components.
- **Prevention through enhanced and accelerated resilience:** Enable a secure Net Zero transition by addressing the evolving structure and future demands of the energy system, ensuring new assets are designed with security and resilience. Where appropriate expanding cyber oversight, targets and monitoring across a broader range of energy players – proportionate to the risk they pose. Ensure that the highest-impact operators have appropriate and proportionate levels of cyber resilience, utilising regulatory oversight to establish and monitor maturity targets.

[5] DSIT and DCMS (2022) '[Second Post-Implementation Review of the Network and Information Systems Regulations 2018]' (viewed 12 March 2026)

- **Strengthening preparedness, response and recovery:** Facilitate improved detection capability across the sector to defend against the most sophisticated, high capability cyber actors. Ensure that comprehensive, cross-cutting plans are in place to respond and recover to the threats faced and that plans are regularly tested and exercised with a focus on continuous improvement.
- **Effective monitoring, regulation and enforcement:** The Office of Gas and Electricity Markets (Ofgem) and the Department for Energy Security and Net Zero (DESNZ) will ensure operators in scope of regulation are under appropriate oversight. The National Energy System Operator (NESO) and NCSC will assess resilience and provide recommendations to strengthen cyber assurance across the energy system.
- **Fostering partnership, culture and skills:** Working with government partners, private organisations, academia, and international partners to manage cyber risk effectively. Cultivate a robust, risk driven cyber security posture within industry, expanding access to clearances and information sharing, and investing in the skills needed to secure our energy future.

1.1 Cyber threat

The cyber threat has increasingly focused on CNI systems, as hacktivist groups and high capability state actors strive to compromise these systems for political effect and propaganda victories. Ransomware attacks continue to pose the most immediate and disruptive threat to UK CNI, with some state-linked cyber groups now targeting the industrial control systems that infrastructure relies on.[6]

In February 2024, the NCSC and international partners co-signed an advisory on observed compromises of US CNI by a China state-sponsored threat actor.[7] The targeting of energy, transportation and water sectors could be laying the groundwork for future disruptive and destructive cyber attacks, and is a clear warning about China's intent to threaten essential networks. On top of a more complex picture of actors, the overall cyber threat is amplified by geopolitical risks from global conflicts. In 2024, NCSC repeatedly saw heightened use of cyber activity in areas of wider competing influence around conflict zones.

During direct conflict, Russia has routinely deployed wiper malware to delete data from inside Ukrainian government and CNI to hinder their operation. Russia is routinely seeking to compromise the systems of North Atlantic Treaty Organisation (NATO) states and aiming to shape the information space globally around Ukraine as it erroneously sees itself in conflict with NATO. In January 2026, CERT Polska (one of the Polish Cyber Security Incident Response Teams) attributed an attack on key renewable infrastructure in Poland to Russian actors.[8] This attack affected both Information Technology (IT) systems and physical industrial equipment.

[6] NCSC (2025) 'It's time to act - NCSC Annual Review 2025' (viewed 12 March 2026)
[7] NCSC (2024) 'NCSC and partners issue warning about state-sponsored cyber attackers hiding on critical infrastructure networks' (viewed 12 March 2026)
[8] CERT Polska (2026) 'Energy Sector Incident Report - 29 December 2025' (viewed 12 March 2026)

Iran-based threat actors remain aggressive in cyberspace and continue to achieve their objectives through less sophisticated cyber techniques and have been seen targeting industrial control systems. Following conflict in the Middle East, in March 2026 the NCSC released a Cyber Alert which highlighted heightened risk of indirect cyber threat for organisations and entities who have a presence, or supply chains, in the Middle East.[9]

We must take immediate action to address this escalating threat.

1.2 Current regulatory landscape

The main regulatory lever related to cyber resilience in the energy sector is the NIS Regulations. The NIS Regulations were introduced in 2018 to enhance the security and resilience of network and information systems that are critical for essential services. They are intended to only apply to the most critical operators and therefore do not provide holistic coverage of the energy system. For GB, Downstream Gas and Electricity (DGE), DESNZ and Ofgem are a joint Regulator under NIS, while DESNZ is also the NIS Regulator for Oil and Upstream Gas (OUG).

The NIS Regulations have driven significant improvements in cyber security and resilience. However, they need to evolve to keep pace with the threat, technology and digital transformation landscape. In November 2025, the government introduced to Parliament the Cyber Security and Resilience (Network and Information Systems) Bill (CSRB), to increase UK defences against cyber-attacks.[10] The CSRB will protect more essential and digital services from cyber attacks, enable cyber regulators to be more effective, and provide the government with the flexibility to respond to new threats in the cyber landscape.

The government has proposed new powers in the Bill that, subject to Royal Assent, could be leveraged to drive resilience in the energy sector, where it is necessary to safeguard public services, the economy or national security. However, legislation is not the only tool available and to ensure that the transformation of the whole sector is secure we must also look at improving resilience through license conditions, international standards, collaboration and sharing of best practice and actionable, relevant guidance for companies from government and regulators on cyber security.

1.3 Sector transformation

CP2030 will tackle three major challenges: the need for a secure and affordable energy supply, the creation of essential energy industries, supported by skilled workers, and the need to reduce greenhouse gas emissions and limit our contribution to the damaging effects of climate change.[11]

[9] NCSC (2026) '[Alert: NCSC advises UK organisations to take action following conflict in the Middle East]' (viewed 12 March 2026)
[10] Government Bill introduced by DSIT (2025) '[Cyber Security and Resilience Bill]' (viewed 12 March 2026)
[11] DESNZ '[Clean Power 2030 Action Plan]' (viewed 12 March 2026)

Clean power will require doing things differently.[12] It will only be achieved with bold action and sustained momentum, across every area and every step of the way between now and 2030. A huge uplift in wind, solar, and storage technologies and supporting infrastructure are driving our CP2030 goals. We must contract as much offshore wind capacity in the coming one to two years as in the last six combined, with GB's offshore wind capacity expected to rise by 30GW by 2030. We must deliver first-of-a-kind clean dispatchable technologies, such as carbon capture and storage and hydrogen to power. We must build twice as much transmission network in the next five years as was built in total over the last decade. And that is only a small subset of the elements that must deliver at the limit of what is feasible to achieve our ambitions.

In addition to new technologies and growing subsectors such as wind generation, the energy sector is evolving through increased digitalisation and seeing the phase out of longstanding fossil fuel generation with coal-burning generation plants decommissioned.

A key challenge will be making sure all elements deliver simultaneously, in full, and at maximum pace, without compromising security to achieve speed. The diversity and transformation of the GB energy system will bring with it new risks. These risks will not always rest on the largest of infrastructure operators, we therefore need to look at all parts of the energy system to drive security and resilience.

[12] NESO (2024) 'Our Clean Power 2030 advice to Government' (viewed 12 March 2026)

2. Call to action

It is vital that we increase the cyber resilience of the UK's energy sector and we need to act with urgency and coordination. As the scale and capability of cyber actors proliferates, the relationship between state and non-state actors becomes more obfuscated, and the potential security debt of new clean infrastructure compounds the security gap. Therefore, private organisations and government need to work even more effectively together to secure the energy sector and will need to make the most of all the resources at our disposal to protect our national security and way of life. Cyber security should be a board level priority, recognising that cyber security is a critical enabler of public trust, resilience and competitive advantage.[13] Together, our collective cyber capabilities can deliver a secure Net Zero transition and enable us to keep pace with the evolving risks.

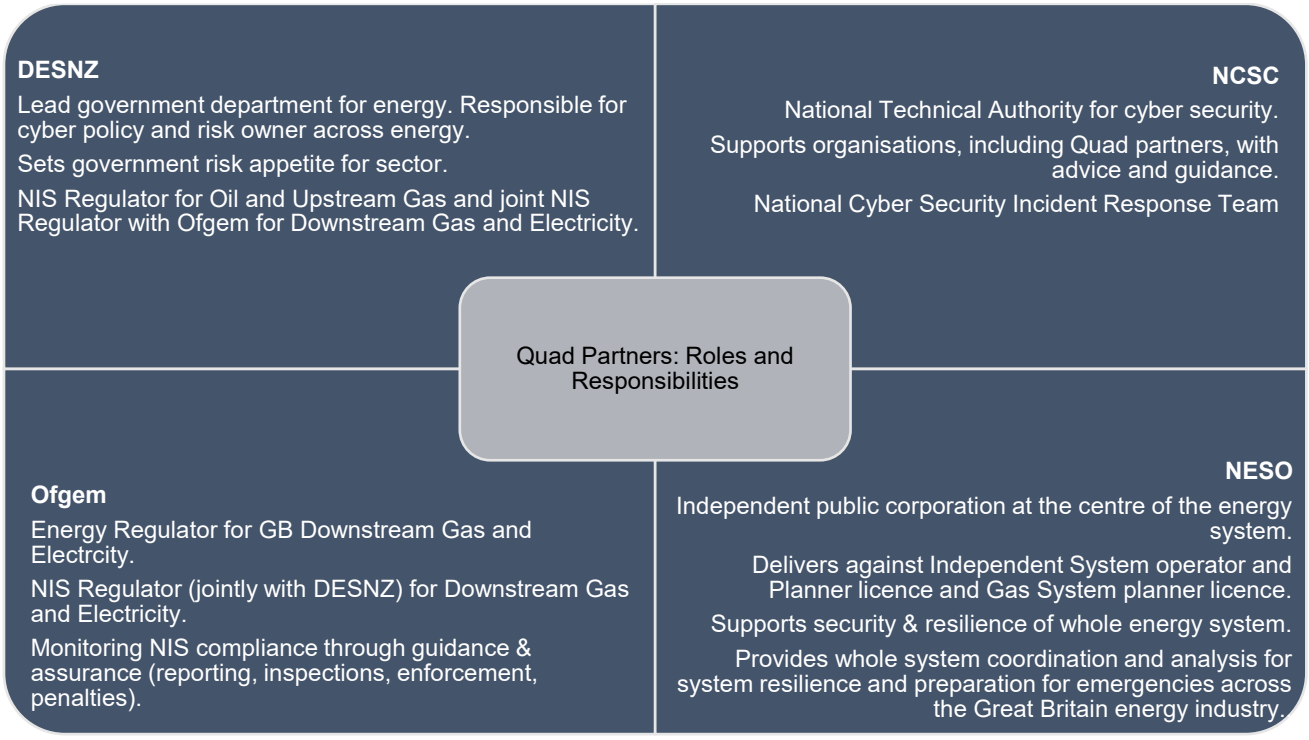
DESNZ, Ofgem, NESO, and the NCSC, the 'Quad partners', each play a crucial role working with energy organisations to improve the cyber security and resilience of the sector. Recognising the scale of the challenge, we need to work together to drive cyber security and resilience across the energy system.

In response to the escalating cyber threat, sector transformation, and evolving regulatory landscape, the Quad partners believe a coordinated approach is essential to enhance cybersecurity and resilience across the energy sector. Consequently, the Quad partners have decided to advance this together through a joint cyber strategy and activities to be delivered working hand in hand with industry.

The Quad partners will remain as independent organisations with clear roles and responsibilities but will leverage our collective resources to focus on the most impactful initiatives and work together to deliver these strategic outcomes to deliver significant improvements in cyber security and resilience across the energy sector.

[13] Rt Hon Liz Kendall MP and others 'Ministerial letter on cyber security' (viewed 12 March 2026)

Figure 1: Quad partner roles and responsibilities[14]



[14] NESO is a regulated entity under the NIS Regulations, but is invited to the Quad partnership for its broader system-wide responsibilities established under their licence conditions, which are distinct from its regulatory obligations as an Operator of Essential Services.

3. Strategic objectives

3.1 Understanding Threat, Vulnerability and Risk

The energy sector is undertaking a rapid transformation to meet our CP2030 ambition, marked by unprecedented infrastructure development, a significant increase in renewable generation, and extensive digitalisation. The sector is also supported by a highly interconnected and complex supply chain, which is becoming increasingly critical to its security and resilience.

To navigate this evolving landscape, it is essential to understand how these changes impact critical elements of the system. We must assess how the interconnected nature of the new energy network, combined with existing and emerging cyber threats, shapes the risks we face. This assessment will inform the actions needed to bridge the gap between our current state and our desired future state.

It is vital that we work hand in hand with industry and its supply chain to understand relationships and interconnections across the system. We also need to assess the risks they pose and what needs to be done to bridge the gap between where we are and where we need to be. As part of this scoping work, we will consider baseline cyber hygiene measures such as Cyber Essentials (CE) as a core factor, ensuring alignment with wider government expectations while maintaining a high-level principle-based approach.[15] If we do not fully understand the complexities of our increasingly diverse, complex, interconnected, and digital, energy and supply chain system, we will not be able to mitigate against the vulnerabilities these complexities introduce.

- By the end of **2026** we will have increased our **understanding of cyber security risks** across the most critical parts of the energy system and ensured we have robust processes to **identify and prioritise operators** across the sector.
- By the end of **2026** we will have developed **preliminary supply chain security principles to support operators and suppliers meet our expectations and manage supply chain risks effectively**.
- By the end of **2027** we will have **built our capability** to engage with and assess the energy supply chain, **supported existing Operators of Essential Services (OES)** with managing their supply chains, and influenced legislation that will enable us to directly regulate critical suppliers.
- By the end of **2030** we will have **designated critical suppliers** and scoped appropriate **maturity targets** for them.

[15] NCSC '[Cyber Essentials]' (viewed 26 March 2026)

3.2 Prevention through enhanced resilience

The threat landscape has evolved rapidly. The heightened risk to CNI and the increased targeting of the technologies that underpin the energy system are being repeatedly highlighted. NCSC reporting and recent global events have shown that the energy sector is a particularly attractive target for attacks of increasing sophistication – including advanced capability and state threat actors. We must work with industry to accelerate the baseline resilience of the energy sector.

Increasing pace

Ministerial deadlines for cyber resilience targets have driven a significant uplift in the energy sector's resilience.[16] However, the current assessment of the threat landscape in the UK energy sector necessitates a further increase in cyber resilience pace. The Quad partners expect operators to prioritise acceleration of plans for the assets they deem most critical and deliver against them as soon as possible. Wherever possible, we encourage operators to do this ahead of ministerial deadlines.

Increasing scope

To achieve the government's CP2030 ambitions, the energy sector is transitioning at pace and taking vital steps to unlock necessary flexibility to deliver Net Zero, making the network increasingly interconnected and digitised. As new entrants join the market there is a risk that organisations and sectors crucial to the transforming energy system lack proportionate cyber resilience requirements or aren't developed to be secure by design.

Therefore, the Quad partners aim to increase resilience across the whole energy system through evidence-based prioritisation, legislative reforms, and consideration of appropriate regulatory tools ranging from guidance and engagement to licensing or other suitable vehicles. These measures will ensure that services and operators, even the ones that are not under the scope of the NIS regulations, have a baseline level of cyber resilience that they can build on based on their individual risk context. Early engagement in new energy infrastructure is essential to ensure that key assets are secure by design, considering both system impacts (e.g. grid stability) and consumer impacts (e.g. price, consumer confidence). Leveraging new legislative powers through the proposed CSRB if necessary, the Quad partners will ensure that the scope of the NIS Regulations keeps pace with the energy sector transition.

Increasing standards

For NIS operators, especially those most critical to the resilience of the entire energy sector, the Quad partners will consider what an appropriate cyber resilience roadmap should be to ensure the protection of the energy system's 'crown jewels' against the advanced threats they face.

[16] Cabinet Office and Rt Hon Oliver Dowden (former Chancellor to the Duchy of Lancaster (2023) 'CyberUK Speech' (viewed 26 March 2026)

- By the end of **2027**, we will assess the NIS Regulatory thresholds, including whether new critical sub-sectors are captured, revising via secondary legislation if necessary (subject to CSRB Royal Assent and consultation), to keep pace with the rapidly evolving energy system.
- By the end of **2027** for DGE and 2028 for OUG we will have **supported NIS OES to prioritise accelerated maturity for their most critical systems** and considered appropriate cyber maturity roadmaps to protect these assets from advanced threats.
- By the end of **2027** we will have **engaged with the industry to promote security by design** in new infrastructure, we will have consulted on **re-shaping cyber regulation** in DGE, and we will have shaped proposals for introducing **baseline cyber resilience requirements** for all Ofgem licensees, with an initial proposal – subject to consultation – for these to use Cyber Essentials as the starting point.
- By the end of **2030** we will have ensured that **cyber resilience is raised across the whole DGE system** by introducing a baseline level of cyber resilience to all involved parts.

3.3 Preparedness, response and recovery

Our adversaries are growing increasingly sophisticated in their capabilities. No matter how high we raise our defences, a sufficiently determined and capable actor will be able to find a way through them. We need to strike the right balance of preventing adversaries from getting access to our systems, while at the same time ensuring that if they do, we can detect them as soon as possible and take swift action. We will encourage more reporting of cyber incidents below NIS thresholds and clarify reporting expectations of companies that experience cyber incidents. We must be prepared to detect, respond to and recover from sophisticated cyber-attacks or systemic incidents to avoid catastrophic impacts to the UK if such incidents were to occur.

Therefore, the Quad partners will drive improved threat detection capabilities within the sector through advanced monitoring and comprehensive testing of security measures and the exercising of cross-cutting incident response plans. We will also investigate how to enhance government and industry's ability to prevent, detect, respond and recover from sophisticated cyber-attacks and safeguard our energy system.

- By the end of **2026** we will have **delivered a cross industry and government exercise** to test collective capabilities and processes in responding to a sophisticated cyber attack on the GB energy system.
- By the end of **2026** we will have scoped a capability to raise the sectors' **ability to detect adversaries** so that, even when our defences fail, we are aware as soon as possible and can act promptly. A pilot will be delivered in **2027** and by **2028** we will deliver this capability in full.
- By the end of **2030** the sector will have access to a capability that allows for **advanced capability testing schemes** to prove their defences. We recommend that

this is to be based on established schemes such as the Cyber Adversary Simulation (CyAS) Scheme.[17]

3.4 Monitoring, regulation and enforcement

Whilst NIS Regulations have driven considerable improvement across the energy sector, further steps are required to close regulatory gaps and ensure operators in scope of NIS are under effective oversight.

NIS operators must achieve full compliance with the NIS Regulations and existing ministerial targets. The CSRB will enable cyber regulators to be more effective, with expanded and more timely incident reporting of harmful cyber attacks, a stronger mechanism for government to set priority outcomes for them to work to, and a fuller toolkit for sharing information, recovering costs and enforcement. In conjunction, the Quad partners will increase regulator capability and capacity. This will be supported through new frameworks that will recommend deeper assurance approaches, such as CyAS, and the use of recognised industry providers, such as Cyber Resilience Audit (CRA) providers.[18]

- By the end of **2026** we will have **strengthened regulatory capacity** through access to assured industry providers (CRA), to support stronger cyber assurance processes.
- By the end of **2027** we will have ensured **all relevant operators**, as permitted by current regulatory levers**, are designated under NIS.**
- By the end of **2026** for DGE and **2027** for OUG we will have developed new assurance frameworks to provide deeper and proportionate cyber oversight.

3.5 Partnership, culture and skills

The Quad partners will leverage our respective expertise and collective resource to accelerate the resilience of the sector. The Quad partners consider that a regulatory compliance approach only goes so far and will not drive the shift in culture required to secure our energy system. Therefore, we will work with industry to help them better understand moderate and advanced cyber threat capabilities, increase the pool of skilled, security-cleared cyber professionals, collaborate with academia, and drive a risk-rather than compliance-driven culture in organisations and at board level. We will work with industry to drive cyber security up their board's agenda and engage CEOs directly on cyber risk, encouraging the adoption of the government's Cyber Governance Code of Practice to support risk owners in managing cyber risk effectively.

The cyber threat is acute and globally pervasive. No nation can address this threat in isolation. It is addressed through robust international collaboration – sharing intelligence, harmonising standards, and building mutual resilience. The Quad partners remain committed to working with international partners to understand and manage risk effectively. It will work with partners

[17] NCSC, 'Cyber Adversary Simulation (CyAS)' (viewed 19 March 2026)
[18] NCSC, 'Cyber Resilience Audit (CRA)' (viewed 25 March 2026)

to minimise regulatory burdens on industry and develop common languages for talking about cyber security.

- We will maintain a cross-industry **Energy Security and Resilience Taskforce**, comprised of energy sector CEOs and chaired by the Minister for Energy, to drive accountability at CEO level.
- By the end of **2027** we will have **fostered a cyber and security culture** centred around risk, collaboration, capability (specifically related to bridging the gap between OT engineering and cyber), and intelligence to accelerate resilience.
- By the end of **2028** we will have delivered a **CEO tabletop exercise** to ensure practical understanding of cyber risks.

4. Next steps

This strategy is intended as a clear statement of intent across the four organisations, driving our approach to cyber security and resilience. The delivery of its ambition will rely on continued collaboration across the organisations, with industry leaders, and international partners. We will regularly review our progress against our outcomes and ensure they are driving the change required to ensure the energy sector is resilient to the threats we face now, and in the future.

This publication is available from: www.gov.uk/desnz

If you need a version of this document in a more accessible format, please email alt.formats@energysecurity.gov.uk. Please tell us what format you need. It will help us if you say what assistive technology you use.