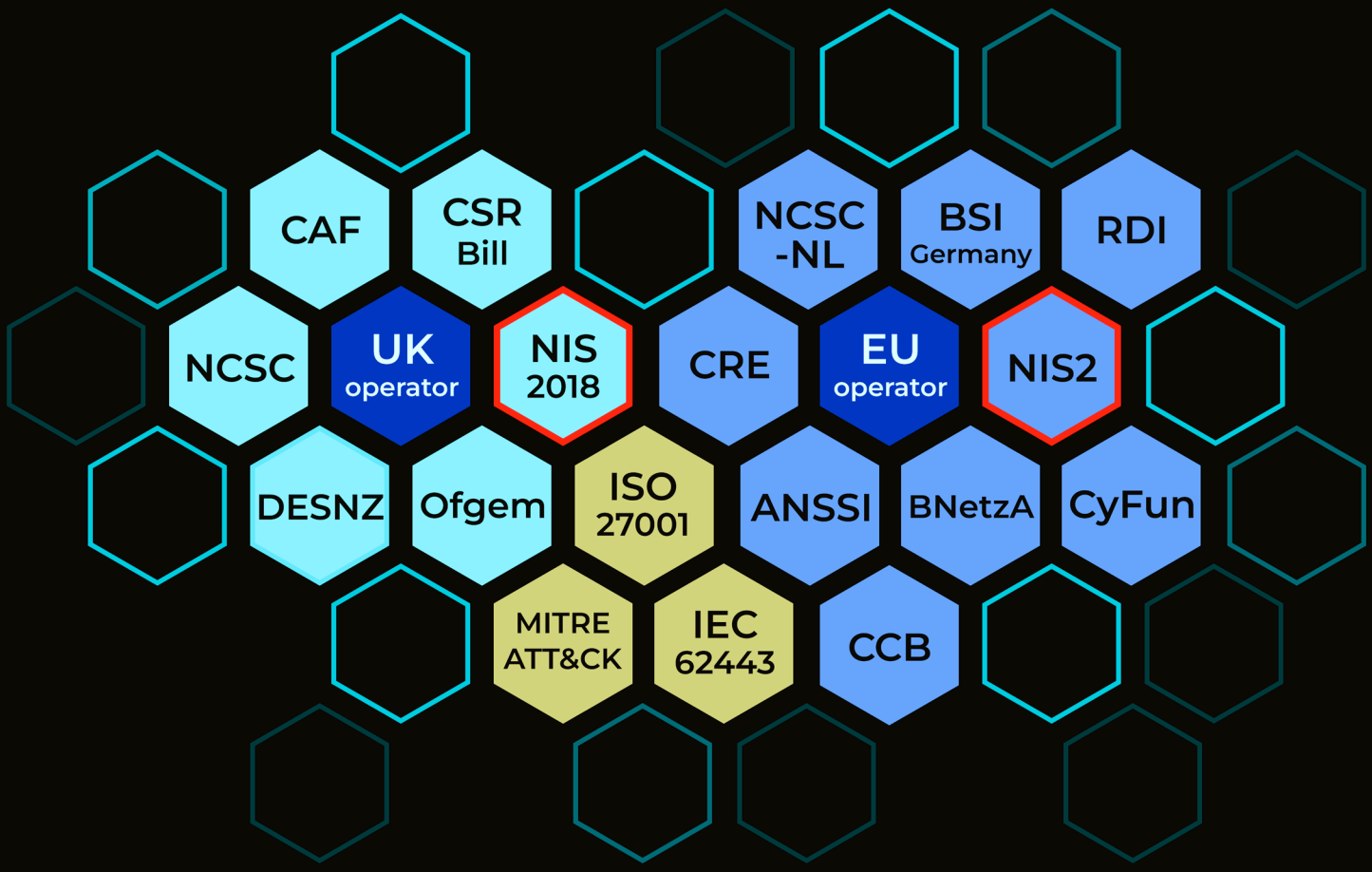

The half of cybersecurity that pays you back

Words: Carl Ketteringham, Founder and Director, Offshore Digital Engineering Limited (ODiGE)

Cyber governance is often treated as a compliance burden, but maintaining a clear, evidence-based position can improve operational discipline, procurement readiness and commercial credibility as regulation tightens across the energy sector.

Ask five people in an energy business what the cybersecurity regulations currently require of them and you will get five different answers. Ask what they need to do about it from a governance, risk and compliance perspective, and you may not get an answer at all.

That is not a criticism of the five people. It is a fair reflection of what they are being asked to navigate.

A British operator is navigating more than one set of requirements: regulations already in force, proposed amendments, assessment frameworks, international standards and catalogues of known attack techniques. Behind all of these sits a practical requirement: being able to demonstrate compliance to the relevant competent authority. For operators working across Europe, NIS2 adds further cybersecurity risk-management and reporting obligations.

None of that is cyber defence, and the distinction matters more than it gets credit for. Defence tends to attract more attention: penetration testing, red teaming, threat hunting, AI-driven anomaly detection. It is where much of the budget goes, and the sector has become considerably better at it.

Governance, risk and compliance pose a different problem: establishing what you are accountable for, deciding what is proportionate and being able to demonstrate the position you have taken. Most organisations are considerably further along with the first than the second.

Where the rules begin

The confusion begins earlier than most people expect, with whether the rules apply to you at all.

Under the UK Network and Information Systems Regulations 2018, designation works two ways. If you provide a listed essential service, rely on network and information systems and meet the threshold, you are designated by operation of law. Nobody writes to tell you. Working out your own status, and notifying the competent authority, is your responsibility. Separately, the authority may designate you below the threshold if it judges that disruption to your service would have a significant effect, and in that case you are told in writing.

The thresholds themselves are worth a careful read, and they are not fixed. In Great Britain the tests for electricity supply turn on supply to more than 250,000 final customers, or on supply combined with generation above a set capacity, cumulated across affiliated undertakings. Several categories of generation are excluded from that second test.

Read against the way renewable generation is structured, this leaves many standalone wind, solar and battery projects outside automatic designation, and dependent instead on the regulator's discretion to designate below the threshold. Offshore is the exception worth checking. Offshore transmission owners are caught by their own test, which cumulates the generation capacity connected across a licence holder and its affiliated undertakings, so a portfolio can cross the threshold where no single link does.

That is today's position. Ofgem and the Department for Energy Security and Net Zero (DESNZ) have consulted on whether the services in scope and their thresholds remain fit for purpose, and in August 2026 confirmed they intend to review who counts as critical in downstream gas and electricity. The Cyber Security and Resilience Bill, which is progressing through Parliament, adds large load controllers as a new category, brings data centre services in as a new essential service and gives the Secretary of State powers to amend the regime through secondary legislation. The boundary that currently excludes you can therefore move without another Act of Parliament.

Europe asks a different question entirely. NIS2 ignores capacity and asks which annex your sector sits in and how large your group is, with roughly 160,000 entities estimated to be in scope across the EU, an order of magnitude more than under the original directive.

It is also unevenly applied: in July 2026 the Commission referred four member states to the Court of Justice for still not having fully transposed it, nearly two years after the deadline. Size is assessed across the group, so a majority-owned company is consolidated in full and a holding between 25% and 50% counts pro rata.

Our sector builds through joint venture project companies with very few direct employees. On its own books a project company looks small. Counted through its parents, it is not.

Same asset, two jurisdictions, two unrelated tests and the answers do not correlate.

When regulation reaches the supply chain

Then there is the supply chain, which is where this stops being an operator problem.

Most suppliers will never be regulated directly. They will feel this through their customers instead. An operator's obligations travel down the chain as contract clauses, security questionnaires and evidence requests, and NIS2 already requires in-scope entities to address the security of their relationships with direct suppliers. You do not have to be designated to be affected.

Some suppliers will be regulated directly. The Bill creates a new category, the designated critical supplier. A regulator will be able to designate a business that supplies goods or services directly to an operator of essential services, relevant digital service provider or relevant managed service provider that the same regulator already oversees, where the supplier relies on network and information systems to make that supply, where an incident affecting those systems could disrupt the service, and where that disruption would be likely to have a significant impact on the UK economy or the day-to-day functioning of society.

Managed service providers come into scope in their own right. What a designated supplier will actually have to do is not yet settled. Those duties follow in secondary legislation, and the government has said they will not be more stringent than the requirements already placed on operators of essential services and relevant digital and managed service providers.

Commentators have already flagged an unintended consequence: some suppliers may become reluctant to provide technical services to operators for fear of later designation.

One change in the Bill reaches operators directly rather than through the chain. Initial incident notification moves to a light-touch report within 24 hours, with a fuller report at 72 hours. More significant than the clock is what becomes reportable.

An incident is currently reportable when it disrupts the service. Under the Bill it is reportable when it has adversely affected the operation or security of the systems the service relies on, whether or not anything has stopped working. Ransomware and pre-positioning become reportable at the point of access rather than the point of failure.

What the standards actually do

It is worth being clear about what these standards and frameworks are doing. IEC

62443 is designed for industrial automation and control systems, with concepts such as zones, conduits and defined security levels. ISO 27001 provides a certifiable information security management system. The National Cyber Security Centre Cyber Assessment Framework (CAF) takes a different approach: it is an outcome-based framework built around four objectives, 14 principles and 41 contributing outcomes. It was developed to support effective cyber regulation in the UK and is used by regulators and other cyber oversight bodies where they choose to apply it.

Attack catalogues serve another purpose, describing adversary behaviours and techniques that can be used to test whether security controls are capable of addressing realistic threats. None of these standards or frameworks is the regulation itself. Rather, they provide ways to structure, assess and demonstrate how an organisation is achieving the security outcomes that regulation requires.

For anyone supplying into this sector, the relevant parts of IEC 62443 are specific. Part 4-1 covers the secure product development lifecycle: how a component is built, shipped and maintained. Part 4-2 covers the component itself and the technical requirements at a claimed security level.

The two are linked. In certification schemes such as ISASecure, 4-2 is assessed alongside the supplier's secure development processes under 4-1, so meeting the technical requirements alone is not enough. Part 2-4 covers service providers rather than product suppliers.

This is how the obligation travels down the chain. Ofgem's guidance names an IEC 62443 conformance certificate as acceptable evidence towards an operator's target profile, including hardware and software security levels.

A supplier certificate can therefore become evidence in an operator's submission to its regulator. That gives the operator a documented reason to ask for it and gives the supplier who holds it a commercial advantage. In our experience of regulated UK procurement, buyers increasingly ask about 4-1 development practices directly rather than waiting for a certificate.

Assurance is moving beyond self-assessment

For operators already designated in Britain, the bar has moved as well. In April 2025 Ofgem, as joint competent authority with DESNZ, issued assurance guidance moving away from taking self-assessment at face value. Operators now submit an Assurance Programme Plan alongside the annual return, covering the scope, schedule and goals of assurance activities and remediation plans. Guidance and templates were updated in January 2026.

Activities fall into three categories: audit, operational exercising and technical testing. High-level findings or the final report go to the regulator within eight weeks. Broader and deeper assurance reduces intervention, while thin assurance invites inspection.

One footnote in that guidance deserves attention. The regulator observes that not all members of the accredited assurance schemes are skilled in operational technology and industrial control networks, and that further clarification may be needed to meet an operator's actual requirements. The competent authority is acknowledging a competence gap in the assurance market itself.

Why OT governance is different

Operational technology (OT) is the technology used to monitor and control physical equipment and industrial processes. In an energy environment, that can include the systems controlling generation, substations and other critical plant.

The governance challenge is that OT inverts some of the priorities information security was built around. In IT, confidentiality often leads. In OT, availability, reliability and safety can take priority because the plant has to keep running.

Patching illustrates the difference plainly. In an enterprise environment, you might patch on a scheduled cycle and reboot overnight. On plant, an unplanned restart of a control system can mean lost production, potentially a safety event, and quite often a warranty conversation.

The governance question is therefore not simply why a system is unpatched, but what compensating measures are in place, who assessed them and when that decision was last reviewed.

There is a second complication peculiar to how our sector procures. A large part of the OT estate is not the operator's to change. Turbine controllers, converters, inverters and their embedded software sit inside supply and service agreements with the manufacturer.

The operator holds regulatory accountability for an asset base whose configuration somebody else controls. That is a governance problem before it is a technical one, resolved through contracts, defined responsibilities and evidence rather than through tooling.

From compliance burden to operational discipline

All of which sounds like a burden, and this is where the reframe becomes available. It will be familiar to anyone who has worked offshore for long enough.

Health and safety was once treated as an imposition: forms that slowed the job down, administered by people who did not really understand the work. Nobody in this industry

Carl Ketteringham

argues that now. Safety became embedded in how the job gets done, and organisations that embedded it properly did not merely become safer.

Planning and handovers improved, surprises and stoppages reduced, and the discipline that looked like overhead became part of operational competence. It also became something you put in a tender.

OT cyber governance faces the same choice. Treated as an annual exercise assembled in the fortnight before an audit, it becomes a pure cost and produces only a snapshot of the estate on a particular day. Maintained continuously as a live record of what you own, who is responsible for it, its current state and which risks you have accepted, it becomes less work because there is nothing to reconstruct.

Decisions retain their rationale and date, so a change of personnel does not erase the reasoning behind them. When the regulator asks for evidence, the answer already exists.

The return is not only regulatory. Demonstrating a governed position is fast becoming a qualification criterion in prequalification questionnaires, supply chain assurance, insurance and due diligence when assets change hands. The organisation that can respond in two days is likely to be better positioned than one that needs three weeks to assemble the evidence.

That thinking also informs ODiGE's approach: maintaining the governance position continuously, with the evidence attached, rather than rebuilding it annually. The picture is built with the operator, and the operator then governs it.

Get it into the culture of the business and it stops being compliance and starts being competence. The regulation is simply the thing forcing the conversation.

odige.co.uk