Why compliance evidence is becoming as important as energy yield

For most of its history, the solar industry has been measured on output: capacity factors, yield ratios and availability metrics. However, a second scorecard is now emerging alongside energy yield; one that asks operators to prove their assets are governed, monitored and resilient. For many, particularly those operating at scale, that is proving far harder to answer than expected.

A sector that can no longer fly under the radar

The solar sector's rapid digitalisation has brought with it a risk profile that is only now being fully understood.

Modern utility-scale and commercial solar assets are no longer isolated generation units. They are networked systems: inverters communicating via cloud platforms, SCADA systems integrated with corporate IT networks, BESS units connected to remote monitoring portals and OEM vendor pathways providing permanent remote access into operational environments. Each connection introduces additional cybersecurity and supply-chain dependency that operators must now actively govern.

That dependency on OEM connectivity and foreign-manufactured hardware is fuelling growing concern about supply chain integrity. In 2025, undocumented communication devices were identified in certain Chinese-manufactured inverter equipment, triggering investigations and political scrutiny on both sides of the Atlantic and forcing the industry to confront a question it had largely avoided: how much do operators actually know about what is running inside their assets?

On 29 December 2025, coordinated attacks struck wind and solar farms across Poland simultaneously. Malware corrupted firmware, destroyed operational data and severed the communication link between sites and grid operators. Crucially, the plants kept generating power, but the operators lost the ability to see, control or provide evidence of what their assets were doing. That loss of operational visibility is not just an operational failure. Under today's regulatory frameworks, it is a compliance failure too.

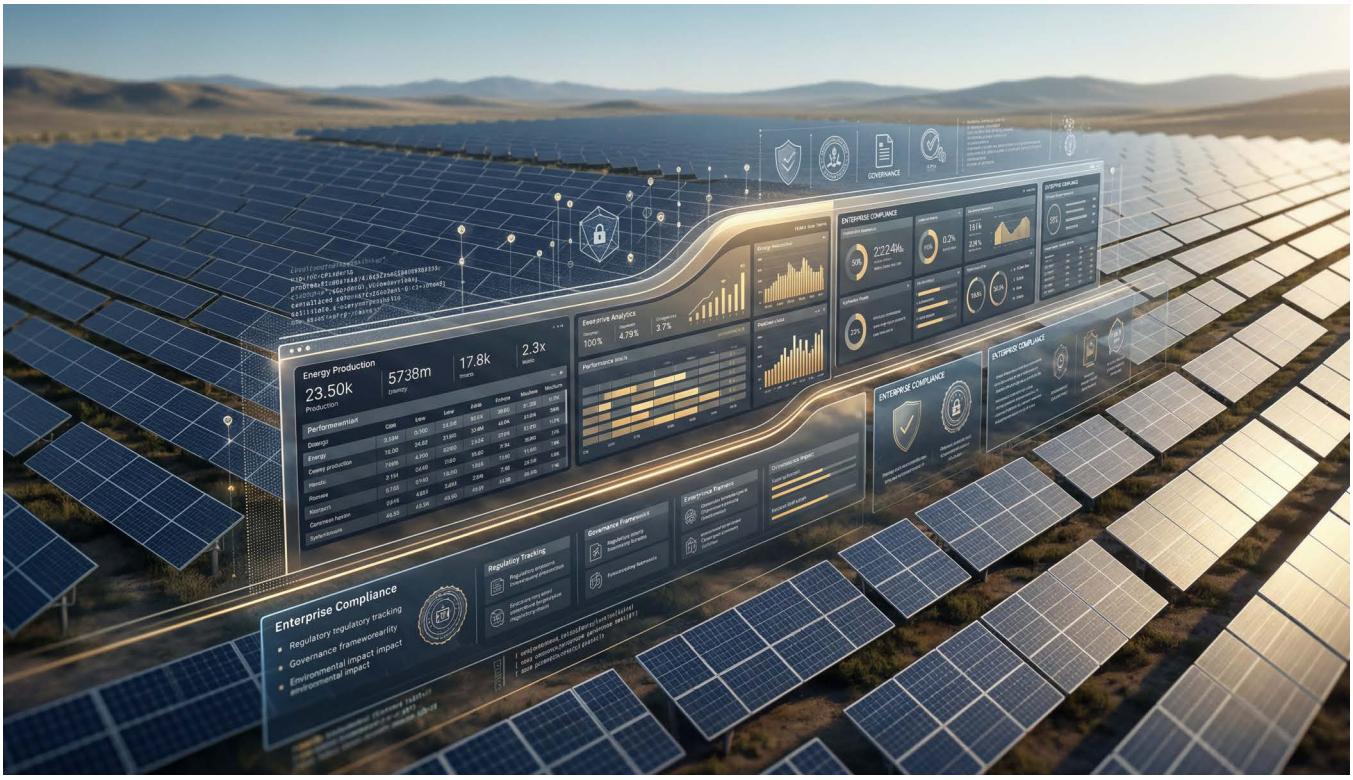
Solar, once considered a low-risk subsector of the energy transition, is now firmly within the crosshairs of state-sponsored threat actors, ransomware groups and supply chain attackers.

The regulatory shift: compliance from a checkbox to a continuous obligation

Alongside the threat landscape, the regulatory environment governing solar operators has undergone a structural shift. The EU's NIS2 Directive, the Critical Entities Resilience (CER) Directive, national cybersecurity frameworks and sector-specific standards such as IEC 62443 have collectively raised the bar not just for what operators must do, but for what they must be able to prove.

NIS2 is particularly significant. It requires operators to implement comprehensive risk management, maintain documented incident response capabilities and demonstrate supply chain oversight. Critically, it places personal liability on senior management for cybersecurity failures, meaning that compliance has moved from the IT department to the boardroom. Fines for non-compliance can reach €10 million or two per cent of global annual revenue.

This is not only a European trend. In North America, NERC's inverter-based resource registration initiative is bringing solar, wind and storage assets that historically sat outside formal compliance thresholds into a more structured reliability and governance



environment. The direction of travel is consistent on both sides of the Atlantic: operators are expected to show that resilience is managed, governed and evidenced.

The result is that solar operators face not a single compliance obligation but a converging set of expectations, from regulators, investors, insurers and grid stakeholders simultaneously, all pointing in the same direction: demonstrate that your assets are resilient and show your workings.

What demonstrable resilience actually requires

That means visibility over SCADA and control system configurations, knowing what is connected, how it communicates and whether those pathways are monitored and controlled. It means understanding inverter and BESS communications, including remote access pathways used by OEMs and vendors and being able to evidence that those access points are governed.

Third-party oversight is particularly important in solar and storage environments, where OEMs, O&M contractors, asset managers, aggregators, telecom providers and cloud platforms can all play a role in operational continuity. Knowing which third parties have access to operational systems, under what conditions and with what security obligations attached is no longer optional; it is a core governance expectation.

It means logging and monitoring coverage that creates an auditable trail of operational activity, not just point-in-time snapshots. And it means incident response readiness that is not theoretical: tested procedures, defined escalation paths and evidence that the organisation can respond effectively when something goes wrong.

Across a single asset, this is manageable. Across a portfolio of 10, 20 or 50 assets, spread across multiple countries, jurisdictions and regulatory frameworks, it becomes an entirely different proposition.

The scale problem: why manual compliance has reached its limits

The challenge for most solar operators is not that they are doing nothing. It is that what they are doing is fragmented. Security controls exist, but are not consistently documented. Supplier agreements contain security clauses, but nobody is tracking whether they are being fulfilled. Incident response procedures are written, but have not been tested and evidenced. Regulatory obligations are understood in principle, but the evidence required to demonstrate compliance cannot be produced on demand.

This gap, between having controls in place and being able to demonstrate them, is the compliance evidence problem. And it is a problem that scales badly. Manual tracking via spreadsheets, periodic audits and siloed documentation systems creates point-in-time snapshots that age quickly. When regulations change, and they are changing rapidly, manual processes cannot keep pace. When an insurer requests evidence of supply chain oversight, or a regulator asks for proof of monitoring coverage, assembling that evidence from disparate systems takes weeks, not hours.

The solar industry solved an analogous problem in operational monitoring years ago. Nobody would operate a portfolio of assets without automated performance monitoring: SCADA systems that provide real-time visibility across every inverter, every string, every transformer. The case for automated compliance evidence management rests on the same logic: the complexity and pace of modern solar operations have simply outgrown what manual processes can reliably deliver.

The compliance risk register: from governance burden to operational intelligence

The answer to this challenge is not more documentation. It is creating a more structured governance process: specifically, a compliance risk register that helps organisations maintain a clearer operational view of assets, dependencies, risks, mitigation activities and supporting evidence over time.

A well-designed risk register for a solar operator brings together operational assets, supplier dependencies, identified risks, mitigation activities, ownership and supporting evidence into a more manageable governance process.

For each risk, it should be able to answer: what assets and systems does this relate to? Which supplier or dependency is involved? Which regulation or stakeholder requirement does it map to? What controls are in place and what evidence proves they are working? Who owns the risk and the remediation? What actions have been taken and what has changed since the last review?

The solar industry is entering an era in which megawatts and evidence packs will be evaluated side by side. The operators who understand that and build accordingly will be the ones that lenders, insurers and regulators trust most.

From that more structured view, organisations can assess likelihood, impact, mitigation progress, ownership and supporting evidence more consistently across the portfolio. It supports treatment planning by helping organisations track remediation activities, assign ownership and maintain governance evidence in a more structured and auditable way.

It is a problem that Centrii, a compliance and cyber-risk management platform built for energy asset owners, has designed its risk register to solve. Hybrie De Jager, Centrii's Compliance Officer and the architect of the platform's risk register framework, describes the problem she's encountered firsthand when working with operators across the sector.

'What we keep seeing is operators who have done the groundwork.

We created the risk register because many operators were tracking cybersecurity and compliance information across too many different places. Risks, actions, supplier issues, audit findings, mitigation activities, and supporting evidence were often spread across spreadsheets, emails, documents and different teams.

This made it difficult to maintain a consistent view of what risks existed, which actions were still outstanding and what evidence was available to support operational or compliance activities. The purpose of the register is to bring that information into a more structured process so risks, ownership, actions and supporting evidence can be tracked more consistently over time.'

This is the shift that leading operators are beginning to make: from viewing the risk register as an annual compliance exercise to treating it as a continuous operational capability. The output is not a compliance report. It is an evidence pack: a structured, auditable record of how the organisation manages, monitors and demonstrates its resilience over time.

Crucially, it also creates accountability. Every risk has an owner. Every control has evidence. Every remediation action has a timestamp. That trail of documented decisions and actions is exactly what regulators and insurers are looking for and exactly what most operators currently cannot produce.

'The operators who get this right are not just protecting themselves from regulatory risk. They are building a capability that protects and demonstrates the value of their assets.' Hybrie De Jager argues.

A commercial differentiator, not just a regulatory requirement

It would be a mistake to frame this shift purely in terms of regulatory compliance. The operators building continuous compliance evidence capabilities are doing so not only to avoid fines, but because demonstrable resilience is becoming a commercial differentiator.

For lenders and investors, the ability to produce a structured evidence pack on operational resilience reduces due diligence risk and can determine whether financing proceeds at all. For insurers, documented evidence of continuous risk management directly influences underwriting terms and increasingly, whether cover is available. For grid operators, demonstrated cybersecurity governance is becoming a condition of connection and dispatch agreements.

The question these stakeholders are asking has quietly shifted. It is no longer simply 'do you have a policy?' The more important question is 'can you prove how resilience is being managed in practice?'

The operators building this capability now are positioning themselves ahead of a market shift that is still early but accelerating. Just as bankability, the ability to attract and satisfy project finance, became a defining competitive characteristic of the solar industry a decade ago, demonstrable operational resilience is becoming the next layer of that standard.

The question every operator should be asking

There is a simple test that cuts through the complexity: if a regulator, insurer or major investor called tomorrow and asked for your compliance evidence pack, documentation of your cybersecurity governance, your monitoring and logging coverage, your supplier oversight and your incident response readiness, how long would it take to produce it?

For most solar operators today, the answer is measured in weeks. For future-ready operators, it will be measured in hours. The difference between those two answers is not the quality of an organisation's security controls. It is whether those controls are continuously tracked, evidenced and connected to a single operational intelligence layer that makes resilience demonstrable, not just at audit time, but on demand.

Energy yield will always matter. Uptime will always matter. But in a more connected, regulated and scrutinised energy system, the ability to prove resilience is becoming just as important. The solar industry is entering an era in which megawatts and evidence packs will be evaluated side by side. The operators who understand that and build accordingly will be the ones that lenders, insurers and regulators trust most.

About the company

Centrii is an operational resilience and compliance platform built for energy asset owners.

Our risk register provides a live intelligence layer connecting assets, dependencies, risks, controls and compliance evidence, enabling operators to demonstrate resilience continuously and on demand.

centrii.com