Operational readiness checklist for Energy suppliers

The evidence suppliers need to provide so energy operators can trust assets to perform safely, securely and reliably in live operation.

Proving operational readiness starts with evidence

As renewable energy portfolios grow more complex, operators are asking tougher questions about asset performance, system resilience, cyber security and operational readiness.

Whether delivering battery storage, solar, wind, EV charging infrastructure, grid-connected systems or energy management platforms, suppliers are increasingly expected to provide evidence that systems will perform safely, securely and reliably throughout their operational lifecycle.

Suppliers that can provide clear, structured evidence reduce commissioning delays, strengthen confidence and make the transition into live operations significantly smoother.

The goal is no longer simply delivering infrastructure. It is proving that the infrastructure can operate reliably under real-world conditions.

Who should use this checklist?

- ✓ Renewable energy engineering, procurement and construction contractors
- ✓ Battery energy storage system providers
- ✓ Inverter and control system manufacturers
- ✓ Wind and solar equipment manufacturers
- ✓ Supervisory control and data acquisition, energy management system and energy software providers
- ✓ Electric vehicle charging infrastructure suppliers

The 6 evidence areas every energy supplier should be ready to provide

1. Technical and asset configuration evidence

Operators need confidence that systems are built, documented and configured correctly.

- Provide evidence including:
- System architecture and design documentation
- Asset inventories and component registers
- Configuration baselines
- Software and firmware versions
- Network architecture
- As-built documentation
- Factory and site testing records
- Known system limitations and dependencies

Why it matters

Without accurate configuration information, operators struggle to troubleshoot faults, assess risk and maintain system integrity after handover.

2. Cyber security and access evidence

Energy assets are increasingly connected, remotely managed and subject togrowing regulatory scrutiny.

Provide evidence including:

- Remote access routes
- Multi-factor authentication implementation
- Privileged access controls
- Patch-management status
- Vulnerability management processes
- Incident notification procedures
- Security monitoring arrangements
- OT and IT security responsibilities

Why it matters

Operators need confidence that connected infrastructure can be managed securely without introducing cyber or operational risk.

3. Operational performance evidence

Asset owners need evidence that systems perform reliably under normal and peak operating conditions.

Provide evidence including:

- Availability and uptime data
- Performance and efficiency metrics
- Alarm and event history
- Asset health monitoring records
- Maintenance activities
- Operational exceptions
- Curtailment and outage records
- Data retention and export capabilities

Why it matters

In modern energy systems, performance issues can affect revenue, grid commitments, regulatory obligations and customer confidence.

4. Commissioning and operational readiness evidence

The greatest operational risk often occurs during the transition from delivery into live operation.

Provide evidence including:

- FAT and SAT records
- Grid compliance testing evidence
- Commissioning approvals
- Open defect and issue registers
- Operator training records
- Handover packs
- Access transfer documentation
- Operational support arrangements
- Escalation procedures

Why it matters

Operations teams need assurance that they can safely own, operate and maintain the asset from day one.

5. Supply chain and service visibility

A modern energy asset depends on a broad ecosystem of technology and service providers.

Provide evidence including:

- Named subcontractors
- Support responsibilities
- Escalation paths
- Software support arrangements
- Change notification procedures
- Service dependencies
- Exit and transition plans

Why it matters

Operators need visibility across the wider ecosystem to understand risks, dependencies and responsibilities when incidents occur.

6. Compliance and assurance evidence

Assurance requirements continue to grow across operational, cyber and regulatory domains.

Provide evidence including:

- Audit-ready documentation
- Compliance evidence
- Governance records
- Support for independent assurance reviews
- NIS2-related evidence where relevant
- UK cyber security and resilience requirements where relevant
- IEC 62443 and ISO 27001 alignment evidence where relevant

Why it matters

Evidence that is difficult to produce often becomes a business risk during audits, financing reviews, operational due diligence or regulatory investigations.

10 questions energy operators will increasingly ask

1. Can you provide the evidence required to safely operate and maintain this asset after handover?
2. How are cyber vulnerabilities, incidents and security updates communicated?
3. What remote access capabilities exist, and how are they controlled?
4. Can you demonstrate all configuration, software and firmware changes?
5. Can commissioning and performance results be independently reviewed?
6. Can operational and cyber evidence be supplied quickly if regulators, insurers or investors request it?
7. How are third-party technology providers governed and managed?
8. Who owns evidence, documentation and operational records once the asset is live?
9. What happens if evidence is incomplete, unavailable or disputed?
10. Can operational knowledge, access rights and support responsibilities be transferred without disrupting service?

If supplier evidence is weak, risk shows up as:

- Delayed handover and acceptance
- Reduced confidence in asset performance
- Slower incident response
- Greater cyber and operational risk
- More difficult audits and reviews
- Reduced operational visibility
- Increased commercial and regulatory exposure

Where Resillion can help

Strengthen operational readiness before handover

Identify gaps in documentation, evidence and asset readiness before they become operational issues.

Improve commissioning and handover confidence

Validate that testing records, operational procedures and handover packs support a smooth transition into live operation.

Reduce cyber and operational risk

Assess access controls, connected systems and operational technology environments to help improve resilience across critical energy assets.

Improve visibility across suppliers and systems

Create a clearer picture of responsibilities, dependencies and evidence across complex, multi-vendor energy ecosystems.

Support audit and regulatory readiness

Help demonstrate compliance, support assurance activities and prepare evidence for operators, regulators, insurers and investors.

Build evidence that stands up to scrutiny

Develop structured, evidence-led responses to operational, cyber and resilience assurance requests.

Get in touch

Energy systems are increasingly complex, connected and critical. Ensure the evidence behind your assets is as robust as the assets themselves.

✉ | Email us at: hello@resillion.com