Renmaker

Independent Cleantech Consultancy

PV & BESS Vendor Due Diligence Checklist

How to Safely Isolate High-Risk Components

Version 1.0 — July 2026

Renmaker Ltd.

Prepared by: John Mustardé

PV & BESS Vendor Due Diligence Checklist

1. Company Identity & Ownership

Verify:

- Legal entity name
- Country of incorporation
- Ultimate beneficial ownership
- Parent company jurisdiction
- Any state-ownership links
- Any links to foreign intelligence or national security laws

Record:

- Ownership structure diagram
- Disclosure statements
- Risk notes

2. Cloud Infrastructure & Data Governance

Ask the vendor:

- Where is operational data stored?
- Who owns the cloud infrastructure?
- Is the cloud provider subject to foreign intelligence laws?
- Does the device require cloud connectivity to operate?
- Can the system function offline?
- Is data encrypted at rest and in transit?

Require:

- Data flow diagrams
- Cloud ownership disclosures
- Data localisation guarantees

3.

Firmware Governance & Update Control

Verify:

- How firmware updates are delivered
- Whether updates can be blocked or manually approved
- Whether updates originate from foreign servers
- Whether remote reboot or override commands exist
- Whether firmware signing is used

Require:

- Firmware governance documentation
- Update process description
- Version history
- Change-control logs

4. Remote Access & Support Practices

Ask:

- Does the vendor require remote access?
- What protocols are used (SSH, VPN, proprietary)?
- Can remote access be terminated at your gateway?
- Are remote commands logged?
- Is MFA required?
- Can remote access be time-limited and manually approved?

Require:

- Remote access policy
- Access logs
- Support workflow documentation

5. Network Behaviour & Connectivity Requirements

Verify:

- All outbound IPs, ports, and protocols the device attempts to use
- Whether the device can operate with outbound traffic blocked
- Whether telemetry frequency can be controlled
- Whether the device attempts to contact multiple cloud endpoints

Require:

- Connectivity specification
- Network behaviour documentation
- Whitelisting requirements

6. MSP Status Under the UK Cyber Security & Resilience Bill

Your vendor is legally a **Managed Service Provider (MSP)** if they:

- Monitor your system
- Push firmware
- Provide remote support
- Send load-control signals
- Operate an EMS platform

Require:

- Evidence of MSP compliance
- Incident reporting processes
- Risk management documentation
- Security controls for remote access
- ICO/NCSC guidance adherence

7. Cybersecurity Certifications & Standards

Ask for:

- ISO 27001
- ISO 62443 (OT security)
- Cyber Essentials / Cyber Essentials Plus
- SOC 2
- Penetration test reports
- Vulnerability disclosure policy

Record:

- Certification validity
- Scope of certification
- Gaps or exceptions

8. Supply-Chain Transparency

Verify:

- Component origin
- PCB manufacturing location
- Firmware development location
- Third-party subcontractors
- Any known vulnerabilities in the supply chain

Require:

- Supply-chain map
- Component origin list
- Risk assessment notes

9. Operational Resilience & Failure Modes

Ask:

- Can the system operate without cloud connectivity?
- What happens if the vendor cloud goes offline?
- What happens if the gateway blocks outbound traffic?
- Are there safe-mode or fallback modes?
- Can the system be fully controlled locally?

Require:

- Resilience documentation
- Failure mode analysis
- Local control procedures

10.

Red-Flag Indicators

Avoid or escalate if the vendor:

- Cannot disclose cloud ownership
- Cannot provide data flow diagrams
- Requires foreign cloud connectivity for core operation
- Cannot disable automatic firmware updates
- Refuses to disclose remote access methods
- Cannot operate offline
- Cannot be isolated without breaking functionality
- Has opaque supply-chain origins
- Has no MSP compliance evidence

If any red-flag is present, document the risk and consider alternative suppliers.