CAPA GRM SUITE — RISK

Effective Risk Management Plans for Renewable Generation

A step-by-step guide to renewable generation risk management plans that focus on the highest impact events — and the best route to compliance.

Every renewable generation asset carries hundreds of plausible cyber risks. Very few of them can actually ruin your year. This guide sets out how the critical infrastructure sectors of nuclear, defence and grid operations manage big risks, and how CAPA packages this intelligence capability for the renewables sector.

CAPA

THE CHALLENGE

Too many risks, too little signal

A single wind farm or BESS presents a risk surface far larger than any small operations team can meaningfully assess, let alone manage with a small team.

Let's imagine a newly built wind and BESS hybrid 200 MW site. It runs a plant controller, a SCADA master and historian, engineering workstations, turbine or inverter controllers, substation and balance of plant systems, as well as 10 other subsystems, and a set of Cloud operated facilities for three or four different OEMs.

Run any conventional risk workshop across and you will generate a register of two hundred entries inside a week. Every one of them is important, but none are conclusive about what should be done. This register then has to be scored, treated, reviewed and reported on annually by a site team of just a few people.

> *The problem is not that operators cannot identify risks. The problem is that too many risks results in an undifferentiated list that is as effective as having no risk plan at all.*

The questions that we should be asking:

- Which of these risk scenarios can lead to a genuinely bad day — injury, asset destruction, an extended outage, or a cascading outage on other infrastructure?
- Which are theoretically possible but have never once been demonstrated against a facility like ours?
- If I do prioritise a risk scenario, what are the possible mitigations that I can implement?
- Where is the evidence base for this prioritisation, when the regulator or board member asks?
- What do we do first, given limited budget, time and headcount we actually have?
- How do we show, twelve months later, that the plan is being maintained and that our posture has improved?

Where some traditional approaches have landed:

Likelihood × consequence scoring

Likelihood for a targeted cyber attack on an OT asset is not a meaningful metric. Teams end up guessing, then defending the guess. Scores cluster in the middle of the matrix and nothing is prioritised.

Control-framework gap analysis

Assessing against a catalogue of compliance controls, rather than a list of avoided consequences. It measures our diligence but not how we have materially reduced the impacts.

Annual advisory engagements

External consultants can build a credible model, but it is expensive, a point-in-time artefact, and the knowledge leaves with the consultant. Within months the plant may change but the team is unaware.

Compliance-led plans

A plan built backwards to address activity in each domain but misses the attack - security theatre.

THE METHOD

Start from the bad day, not the risk list

The approach used across nuclear, defence and national grid operations: work backwards from a small number of unacceptable outcomes.

High-consequence sectors abandoned exhaustive risk enumeration long ago. Nuclear operators do not attempt to rank every fault; they define a limited set of unacceptable outcomes and engineer against them. Defence programmes use mission-impact analysis. The discipline reached the energy sector as **Consequence-driven Cyber-informed Engineering (CCE)**, developed at Idaho National Laboratory and now embedded in critical infrastructure practice worldwide.

The premise is simple and uncomfortable: assume a capable adversary can get in. Stop asking how likely that is, and start asking what they could do once they are there that you could not tolerate. That single reframe collapses a two-hundred-line register into a handful of events worth defending.

1. **Ask what a REALLY bad day looks like**

   Rather than asking what could go wrong, what would be unrecoverable, unsafe, or career-ending. For a generator that is typically loss of dispatch control during a market event, physical destruction of plant through control manipulation, defeat of protection or safety systems, or a ransomware event that takes SCADA and the backups together.

2. **Nominate a small number of High Consequence Events**

   Five to eight per facility. Each one is a described outcome with a named impact category — safety, asset loss, operational, commercial, regulatory, national security. If a candidate HCE cannot be described in one sentence a board would take seriously, it is not an HCE.

3. **Identify the crown jewels that make each HCE possible**

   Work backwards from each HCE to the specific systems, functions and data whose compromise is a necessary condition. In practice this is a short list — the plant controller, the protection scheme, the engineering workstation, the vendor remote access path, the backup repository. These are what you defend.

4. **Use threat intelligence to build realistic attack paths**

   Ground each HCE in what has actually been done to facilities like yours. Real incidents tell you which entry points get used, which techniques recur, and which controls have historically broken the chain. This is where open-source intelligence does the heavy lifting.

5. **Choose mitigations that break the chain, not that fill the matrix**

   An attack path is a sequence. You do not need to defeat every step — you need to reliably break one, and detect the attempt at another. Prioritise controls that sit across several paths at once.

Why consequence-first survives scrutiny

A consequence-driven plan is defensible in front of a regulator, an insurer or a board because it does not rest on a guessed probability. It rests on a stated outcome, an evidenced attack path, and a control that demonstrably interrupts it. When someone asks “why did you fund that and not this?”, the answer is a traceable line from a real event to a specific decision.

IN PRACTICE / TRANSLATING TO YOUR FACILITY

The same method, six architectures

HCEs are architecture-specific. The method is not. Each asset class inherits a different set of crown jewels and a different exposure profile.

WIND FARM

Fleet control and turbine integrity

Loss of dispatch control; turbine damage via pitch, yaw or brake manipulation; protection defeated.

Crown jewels: plant controller, WTG configuration, vendor LTE gateway, protection scheme.

UTILITY-SCALE SOLAR

Array-wide setpoint control

Mass inverter disconnect or forced curtailment; firmware manipulation across a single-vendor array.

Crown jewels: inverter management platform, PPC, vendor cloud portal.

BESS

Thermal event and market exposure

BMS limits overridden to push cells outside their safe envelope; unauthorised discharge against market position.

Crown jewels: BMS, EMS/PPC, thermal management, market interface.

TRANSMISSION

Availability and resilience

Loss of a connection asset at peak; protection maloperation cascading; restoration without visibility.

Crown jewels: substation SCADA and RTUs, protection and teleprotection, EMS.

DISTRIBUTION NETWORK

Switching and protection

Unauthorised switching across feeders; protection settings changed; ADMS visibility lost during an event.

Crown jewels: ADMS, RTUs and relays, engineering workstations, telemetry backhaul.

DER FLEET

Aggregated control at scale

The aggregation layer is what matters: unsafe commands issued fleet-wide, identity compromise blocking legitimate control.

Crown jewels: aggregator platform, CSIP / IEEE 2030.5 certificate hierarchy.

BROADENING THE LENS

The same method, every hazard class

Cyber is one hazard among several. The HCE discipline works identically across every hazard class.

A separate process per hazard produces plans that cannot be compared. Nominating consequences first solves it: a bad day is a bad day whatever caused it, and the same crown jewels sit behind several hazard classes at once.

HAZARD CLASS	WHAT A BAD DAY LOOKS LIKE	WHERE THE EVIDENCE COMES FROM
IT / OT cyber	Ransomware taking SCADA and the backups together; protocol-native manipulation of plant control	Sector incident record, ASD and CISA advisories, ATT&CK for ICS
Plant failure	Thermal runaway in a battery enclosure; protection or transformer failure cascading to an extended outage	Condition monitoring, maintenance history, OEM defect notices
Natural hazards	Bushfire or flood taking the site and its comms together; heat derating plant in an event	Hazard mapping, BoM and fire agency data, event history
Supply chain	Malicious firmware via a legitimate vendor update channel; OEM outage removing remote service	SBOM and vendor attestation, PSIRT and VEX feeds, FOCI assessment
Physical access	Unescorted access to a substation or containerised BESS; tampering with edge devices at unmanned sites	Site access logs, patrol and incident history
Governance *cross-cutting*	An owner who cannot evidence the plan; risk accepted without authority; plant changed without reassessment	Audit findings, board papers, regulator correspondence

APPLYING IT

Organisation, site, subsystem, vendor hierarchy

A risk plan that lives only at the corporate level is disconnected, and one that lives at the site level cannot be properly governed. Effective plans cascade through four tiers, each inheriting from the one above and contribute to reporting.

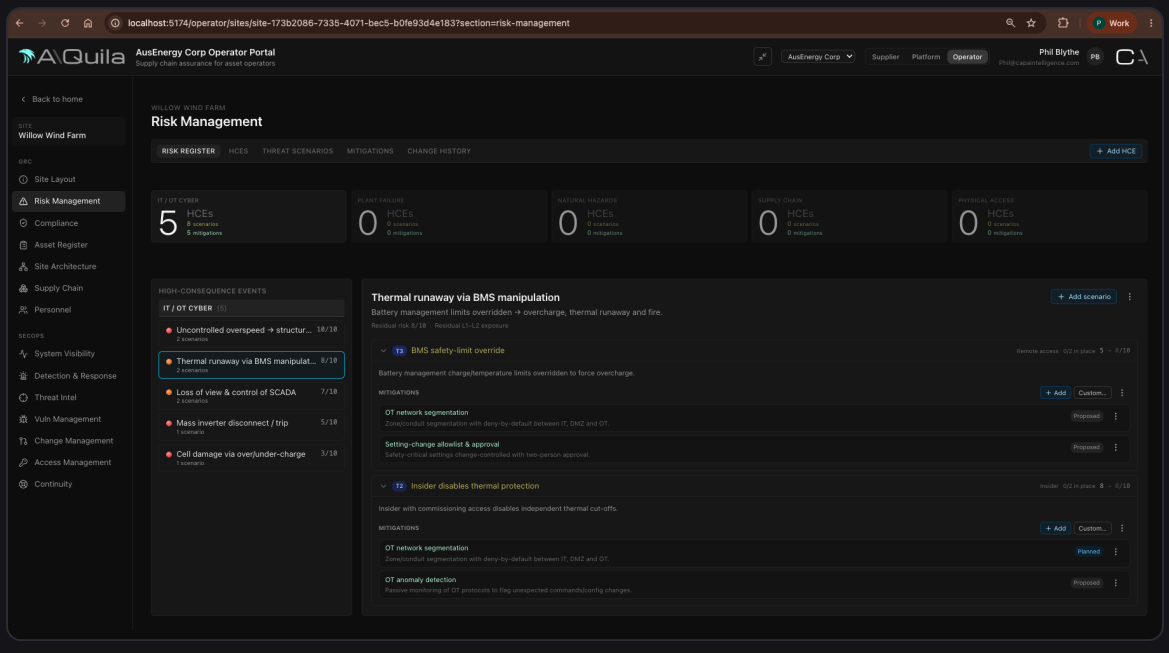
TIER	WHAT IS MANAGED	WHAT IS INHERITED
Organisation	Risk appetite, HCE categories, mandatory controls, reporting obligations, assurance model	—
Site	Facility-specific HCEs, crown jewel register, site attack paths, treatment plan and residual risk acceptance	Appetite and mandatory control baseline
Subsystem	Zone and conduit boundaries, control implementation, configuration and firmware baselines	Site HCEs and the paths that traverse this subsystem
O&M vendor	Contracted control obligations, remote access conditions, patching SLAs, evidence and reporting duties	Subsystem control requirements, flowed down contractually

The cascade enables delegations. Every mitigation obligation in an O&M contract maps to subsystem, to a site attack path, to a nominated HCE, to a stated organisational risk appetite.

THE ARTEFACT

What a maintainable plan looks like

The result is a compact, hierarchical, and traceable set of records — not a two-hundred-line spreadsheet.



The site risk register — hazard classes, nominated HCEs, and the scenarios and mitigations for the selected event.

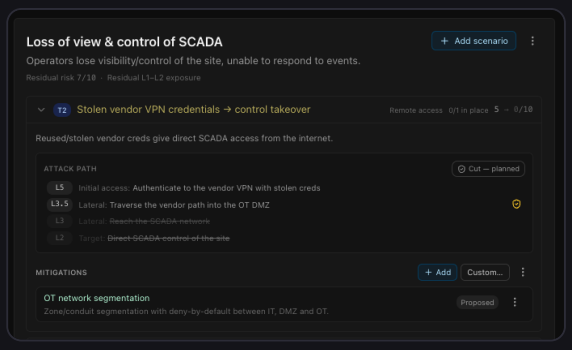
THE SOLUTION

CAPA GRM Risk

A risk management toolset that ships with the threat model already built — the documented history of attacks on energy infrastructure, and links to your IT/OT architecture for cyber risks.

Everything in this guide is achievable from first principles. It is also months of specialist effort, repeated annually, at every site — and it is largely the same work at every renewable asset in the country. It should be done once, properly, and maintained.

CAPA Risk provides a pre-built library of High Consequence Events and threat scenarios for Wind, Solar, BESS, hybrid, distribution and DER fleet architectures. Each cyber scenario carries the attacker techniques that make it real, a traceable link to the incidents that evidence it, and IT/OT layered mitigations that break the kill chain at each stage.



A scenario in CAPA Risk — the attack path by Purdue level, the stage at which a mitigation cuts the chain, and the controls attached.

What sits inside a CAPA threat scenario

TTPS

Attacker techniques, mapped

- Each scenario decomposed into its stages — initial access, credential access, lateral movement, escalation, inhibit response, impair control, impact
- Mapped to MITRE ATT&CK for ICS technique identifiers
- Expressed against real OT components, not generic IT assets

EVIDENCE

Traceable to real events

- Every scenario cites the public incidents, advisories and research that establish it as realistic
- The provenance is visible to your board, your auditor and your insurer
- Updated as the threat environment changes, so the model does not go stale between reviews

MITIGATIONS

Kill-chain interruption

- Mitigations attached at the stage they interrupt, not bolted on at the end
- Shows which controls break multiple scenarios at once — the basis for sequencing spend
- Separates prevention, detection and recovery contributions

TRACEABILITY

A complete audit trail

- Every change to the asset inventory, the threat model and the risk plan is versioned and attributed
- Decisions, acceptances and treatment changes carry rationale and date
- Reporting is generated from the record, not reconstructed before an audit

ALIGNMENT

One plan, many obligations

A consequence-driven model is not an alternative to the frameworks — it is the analytical layer they all assume you have. CAPA Risk structures the plan so one body of work satisfies obligations across jurisdictions: the hazard-based programme under the SOCI Act's enhanced CIRMP rules, the domain and maturity structure of AES-CSF and the US C2M2, the risk treatment and Statement of Applicability logic of ISO/IEC 27001, and the zone-and-conduit assessment of IEC 62443-3-2 — all on the process discipline of ISO 31000.

SOCI CIRMP · AES-CSF · C2M2 · ISO 27001 · ISO 31000 · IEC 62443

WHY IT IS DIFFERENT

Built for small, effective teams

Credible threat modelling has been the preserve of organisations with scale, yet a site team of four carries the same obligations as a gentailer with a security function of forty. CAPA GRM Risk changes that calculus: the domain expertise and intelligence arrive with the product, tailored to renewable generation architectures, so your team applies it to the plant it runs and owns the result.

BEYOND COMPLIANCE

Continuous posture improvement

Compliance is periodic; attackers are not. The value of holding the threat model, the asset inventory and the risk plan in one versioned system is that improvement becomes measurable between audits rather than at them. Each closed mitigation visibly removes an attack path. Each configuration or firmware change is tested against the model as it happens. Each new sector incident flows into the scenario library and is assessed against your site without waiting for the next review cycle. The discipline shifts from producing a document once a year to running a posture that demonstrably improves.

THE SUITE

CAPA GRM

Risk is the second stage of the CAPA GRM product suite. The three stages share one asset inventory, one threat model and one audit trail.

G Governance

Obligations, policy, roles and responsibilities, asset and supply chain inventory, and the evidence base beneath them.

R Risk

High Consequence Events, threat scenarios, attack paths and kill-chain mitigations, cascaded from organisation to vendor.

M Maturity

Treatment execution, posture measurement, change traceability and continuous reporting against obligation.

ABOUT CAPA

CAPA Intelligence is an Australian based cybersecurity company servicing the global electricity / renewables sector, and global supply chains involved in supporting critical infrastructure. Our clients sit across the supply chain – governments, networks, retailers, system operators, IPPs, integrators and OEMs with operations in Australia and abroad.

Contact info@capaintelligence.com to arrange a demo

capaintelligence.com