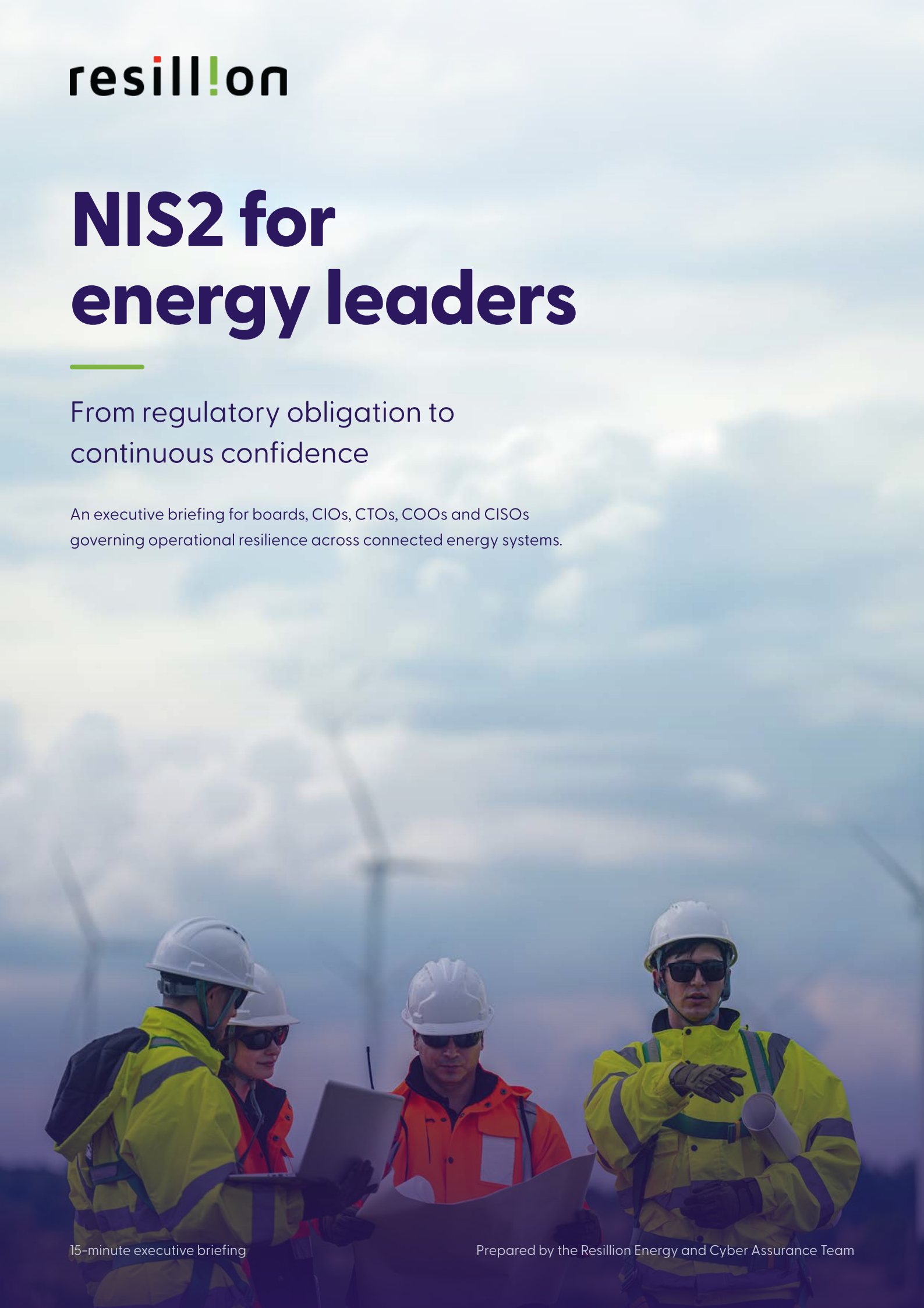
resillion

NIS2 for energy leaders

From regulatory obligation to continuous confidence

An executive briefing for boards, CIOs, CTOs, COOs and CISOs governing operational resilience across connected energy systems.



15-minute executive briefing

Prepared by the Resillion Energy and Cyber Assurance Team

Operational resilience is now a leadership outcome

NIS2 raises the regulatory baseline. The harder question is whether leadership can prove that essential energy services remain secure, available and recoverable as the operating environment changes.

This briefing is not written on the assumption that energy organisations are starting from zero. Most large operators already have cyber teams, governance forums, security operations, operational processes and established technology controls. The leadership challenge is whether those capabilities combine to provide current, defensible confidence in the complete essential service.

Three conclusions for energy leadership

1 **The unit of risk is the essential energy service.** Generation, network operation, balancing, customer service, market settlement and field operations increasingly depend on combinations of operational technology, enterprise IT, cloud, identity, communications, data and suppliers. Governance has to follow the service outcome, not stop at a department or platform boundary.

2 **NIS2 makes governance of that service a management responsibility.** Management bodies must approve cybersecurity risk-management measures, oversee implementation and understand the material exposure those measures are intended to reduce.

3 **Confidence depends on current evidence.** Policies, plans and supplier declarations are necessary, but they do not demonstrate that a service can remain safe and recoverable under realistic disruption. Higher confidence comes from observed tests, exercised decisions, recovery outcomes, validated supplier arrangements and re-tested remediation.

EXECUTIVE TAKEAWAY

The strongest resilience programme is not the one with the most controls. It is the one that gives leadership the clearest evidence that essential energy services can continue under pressure.

CONNECTED ENERGY OPERATING MODEL

Every component can appear healthy while the service still fails

Modern energy outcomes are delivered across a chain. Leadership needs an end-to-end view of the service, the dependencies that sustain it and the conditions that could push it beyond tolerance.

Customer / market → Digital platform → Cloud / identity → Comms / suppliers → OT / field assets

Consider a network-control decision, a balancing instruction, a smart-meter data flow or a field-engineering intervention. The outcome may begin in a digital platform, pass through cloud services and identity controls, depend on telecoms and supplier infrastructure, influence operational technology and physical assets, and then return evidence to market, billing, monitoring and support systems.

One incident, several leadership decisions

A critical operational platform becomes unavailable during a period of high demand. Control-room teams retain partial visibility, but a cloud identity dependency is failing and field communications are degraded. Security teams restrict remote engineering access because a privileged supplier account may be involved. That reduces exposure but removes a recovery route. The supplier is slow to confirm whether its own platform or a fourth party is affected. When the platform can be restored, the latest state across operational data, queued instructions and field devices is uncertain.

The leadership challenge is not only technical restoration. It is how long the service can remain degraded, who can authorise containment and recovery, whether the incident may be significant, what evidence must be preserved and how the organisation will demonstrate that the complete service is trustworthy again.

FRAMEWORK PRINCIPLE

The assurance boundary should follow the energy service and its consequence of failure – not the organisation chart or technology ownership model.

Energy cannot be governed like a conventional digital enterprise

Energy organisations are modernising an operating system that cannot simply be paused, rebuilt or recovered on a purely IT timetable.

Always-on services and physical consequence

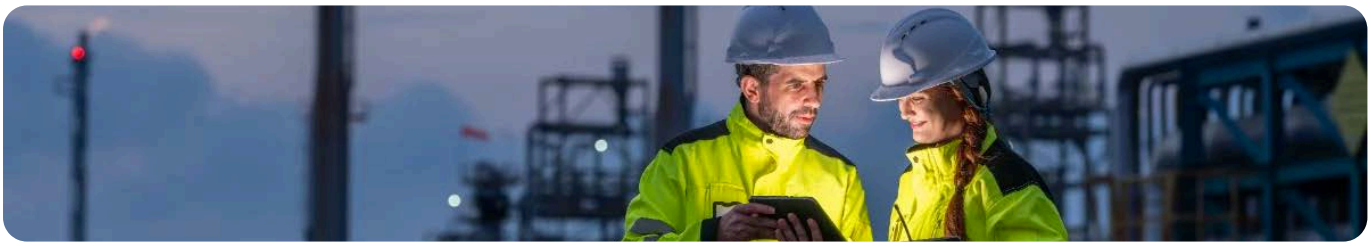
Electricity, gas, oil, heating, cooling and hydrogen services support economic activity, public services and daily life. Failure can affect safety, supply continuity, customers, markets and other critical infrastructure. Impact tolerance must therefore be expressed in operational and societal terms, not only availability percentages or financial loss.

Long-lived OT and fast-changing digital services

Operational technology may remain in service for decades and be constrained by safety, maintenance windows and vendor support. Cloud, identity, software and data services may change weekly or continuously. Leaders must govern the interaction between these different lifecycles and know where compensating controls or targeted validation are required.

Distributed operations and supplier participation

Essential services may depend on geographically distributed sites, field teams, telecoms, OEMs, systems integrators, cloud providers and specialist support partners. Those suppliers can participate directly in operation, incident response and recovery. Their access, concentration, replaceability and evidence quality are part of the service-risk picture.



What this means for each leadership mandate

Board / CEO	Accountability, investment and acceptance of material exposure.
CIO / CTO	Whether architecture, cloud, identity, software and OT change can proceed without creating unacceptable service risk.
COO / asset leadership	Safe continuity, degraded operation and recovery within approved tolerance.
CISO	Whether measures, suppliers, access and incident arrangements are proportionate, effective and evidenced.
Risk / compliance	Whether scope, decisions, reporting and residual-risk treatment can withstand regulatory challenge.

THE LEGAL BASELINE

What NIS2 requires leadership to establish

NIS2 is a governance and resilience regime, not a shopping list of cyber tools. For energy leaders, four duties form the practical legal baseline.

1 SCOPE AND NATIONAL IMPLEMENTATION

Energy is a high-criticality sector, but the practical position depends on legal entity, activity, size, establishment and national law. Scope must be kept current as groups acquire, outsource, enter markets or launch new services.

2 MANAGEMENT ACCOUNTABILITY

Article 20 requires management bodies to approve cybersecurity risk-management measures, oversee implementation and undertake relevant training. Approval should connect critical services, risk appetite, resources, exceptions and evidence.

3 APPROPRIATE AND PROPORTIONATE MEASURES

Article 21 requires technical, operational and organisational measures using an all-hazards approach. The ten measure areas work as one resilience system spanning prevention, continuity, suppliers, secure lifecycle, people, access and effectiveness.

4 SIGNIFICANT-INCIDENT DECISION AND REPORTING

Article 23 establishes staged reporting: an early warning within 24 hours, an incident notification within 72 hours and a final report generally within one month. Decision rights and evidence sources must be prepared before the clock starts.

The evidence standard

Leadership should be able to explain what service is being protected, which scenario could push it beyond tolerance, who owns the decision, what measures were selected, how effectiveness has been tested, what remains uncertain and when the evidence will be refreshed. Policy alone is not operating evidence.

EXECUTIVE IMPLICATION

The regulatory requirement is cybersecurity risk management. The leadership outcome is confidence that an essential energy service can withstand disruption and recover.

A practical operating model for energy leadership

The framework begins with the essential energy service rather than the control catalogue. It connects regulatory obligation to service consequence, operating scenarios, current evidence and defensible decisions.

LAYER 1 **Direction and visibility**	1. Scope, applicability and regulatory exposure 2. Governance and management accountability 3. Risk governance and critical-service visibility
LAYER 2 **Delivery resilience**	4. Critical technology, IT and OT assurance 5. Operational resilience and business continuity 6. Supply-chain and third-party security
LAYER 3 **Response and sustained confidence**	7. Incident preparedness, reporting and communications 8. People, access, effectiveness and continuous assurance

The domains are not sequential compliance stages. They are interdependent conditions. Strong governance cannot compensate for an untested recovery assumption. A secure platform cannot compensate for a critical supplier that cannot recover within tolerance. An effective incident plan cannot compensate for unclear authority or stale evidence.

How evidence becomes confidence

The chain is: obligation → essential service → material scenario → proportionate measure → current evidence → leadership decision. A useful confidence statement is always conditional: which service, which configuration, which scenario, which tolerance, which evidence, which limitation and which next assurance date.

FRAMEWORK STATUS

The framework is a Resillion-developed leadership and assurance model mapped to NIS2. It is not the Directive's official structure, a statutory audit, a certification scheme or an externally validated peer benchmark.

Know where the obligation sits, who owns the decision and what cannot fail

Layer 1 creates the leadership line of sight. It prevents NIS2 from becoming a control programme disconnected from the essential services it is intended to protect.

1 **Scope, applicability and regulatory exposure**

Energy groups often operate through multiple legal entities, joint ventures and shared platforms. New storage, EV, flexibility, retail or hydrogen activities can alter the legal position. Strong practice maintains one approved record linking entities and activities to critical services, national routes, authorities and change triggers. Scope becomes a living governance decision, not a legal memo filed once.

2 **Governance and management accountability**

Management accountability becomes credible when board direction reaches service owners and current operating evidence returns to the board. Risk appetite should be expressed in safety, service, customer, financial and regulatory terms. Material exceptions need one owner, a time limit, compensating measures, an evidence requirement and a re-test date.

3 **Risk governance and critical-service visibility**

Many organisations can list important systems. Fewer can trace an essential service across OT, enterprise applications, cloud, communications, data, people, sites and suppliers. Leadership needs a service map, an impact tolerance and realistic scenarios that reveal concentration and hidden hand-offs. The objective is to understand which dependency could create the most unacceptable consequence and how that resilience claim has been demonstrated.

EVIDENCE LEADERSHIP SHOULD EXPECT

A current scope record; named accountable executives and service owners; approved impact tolerances; end-to-end dependency maps; material scenarios; documented residual-risk decisions; and explicit triggers for reassessment.

Prove that technology, operations and suppliers keep the service within tolerance

Layer 2 is where NIS2 becomes operational. It tests the service and its relationships rather than assuming separate cyber, engineering and continuity workstreams will combine successfully.

4 Critical technology, IT and OT assurance

Energy assurance must work within real operating constraints. OT may be long-lived, difficult to patch and subject to safety or availability limits, while software, cloud and identity can change frequently. Strong practice uses architecture and trust-path review, secure-change gates, Quality Engineering, integration and performance testing, vulnerability handling, rollback evidence and representative recovery validation. No material change should create live exposure without a clear resilience claim and accountable go-live decision.

5 Operational resilience and business continuity

A backup job or documented plan is not recovery evidence. Leadership needs observed proof that the service can remain within tolerance, move into a safe degraded state and return to trusted operation. Testing should include decision authority, manual or alternative operation, restoration sequence, data integrity, backlog clearance, supplier coordination and operational acceptance.

6 Supply-chain and third-party security

A modern energy service may depend simultaneously on OEMs, telecoms, cloud providers, identity platforms, software vendors, integrators and field contractors. Questionnaires and certifications provide context; they do not prove how the supplier will behave in the organisation's deployment. Strong assurance links each critical supplier to the service, privileged access, concentration, fourth parties, recovery, incident support and exit evidence.

LEADERSHIP QUESTION

Which technology, recovery assumption or supplier relationship could move the service outside tolerance — and what current evidence supports confidence in it?

Make the right decisions under pressure and keep evidence current afterward

Layer 3 closes the loop. It tests whether governance and delivery arrangements remain usable during an incident and whether change, lessons and evidence expiry trigger reassessment.

7 Incident preparedness, reporting and communications

A significant incident is both an operational response and a timed governance process. Leadership may need to decide whether to isolate or continue a service, how to balance restoration and evidence preservation, when to notify and how to coordinate suppliers whose information is incomplete. A useful exercise forces those trade-offs and records who decided, on what evidence and with which fallback when facts were uncertain.

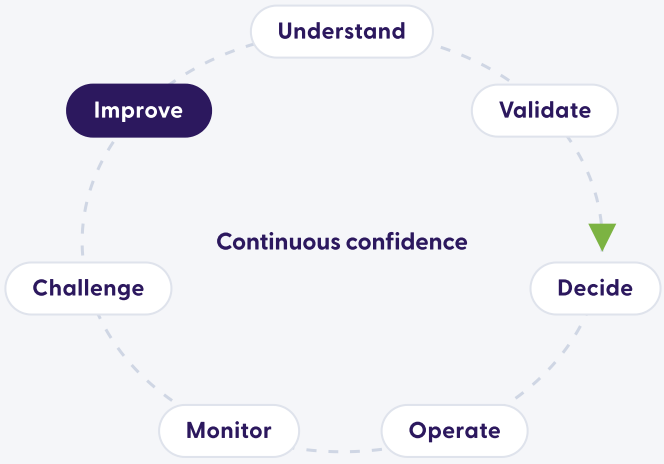
8 People, access, effectiveness and continuous assurance

Controls degrade, privileges accumulate, suppliers change and evidence expires. Management, control rooms, field engineering, developers and incident roles need training for the decisions they own. Privileged and supplier access must remain current. Measures should be assessed through service coverage, observed results, open findings, residual risk and re-test – not policy presence or tool deployment alone.

Continuous confidence

Annual review remains useful, but it should not be the only assurance rhythm. A major software or cloud release, new critical supplier, acquisition, OT upgrade, significant incident, recovery failure, material vulnerability or expiry of key evidence should trigger targeted reassessment. Continuous confidence does not mean testing everything continuously. It means keeping the evidence behind material decisions current.

CONTINUOUS-CONFIDENCE CYCLE



Start with one high-consequence service and produce one visible proof point

The first quarter should not attempt to complete every NIS2 workstream. It should establish control, expose the largest evidence gap and demonstrate the framework on one service that matters.

DAYS 1–30

Mandate and scope

Confirm executive sponsor, relevant entities and national routes. Select one high-consequence service. Define decision rights, impact tolerance and the most important evidence gaps.

DAYS 31–60

Map and design

Map technology, operational, supplier and people dependencies. Select material scenarios. Review current measures, exceptions, recovery claims and supplier evidence. Design the first assurance activity.

DAYS 61–90

Validate and decide

Run one cross-functional scenario or targeted technical/operational validation. Record findings, decisions and residual risk. Fund treatment, define re-test and set the next assurance date.

A practical quarterly rhythm

A leadership forum should review the highest-consequence services, material change, supplier concentration, recovery and incident evidence, significant open findings and next assurance dates. The purpose is not to receive every technical metric. It is to identify where the service could exceed tolerance, where evidence is weakest and which management decision is now required.

The hand-off test

For every material issue, leadership should be able to name one accountable decision owner, the trigger and time limit, the evidence required, the fallback when information is incomplete and the closure or re-test step. Shared accountability must not become shared ambiguity.

MOBILISATION PRINCIPLE

Progress is not the number of workstreams launched. It is the quality of the first evidence-led decision and the repeatable governance rhythm created around it.

INDEPENDENT ASSURANCE FOR MATURE ENERGY ORGANISATIONS

Strengthen the capabilities already in place

Resillion does not replace the organisation's cyber, engineering or operational teams, and management retains ownership of strategy and risk decisions. Its role is to strengthen those capabilities through independent challenge, specialist validation and evidence that leadership can rely on.

Resillion helps energy organisations reduce risk across complex cyber-physical, software-defined systems through cyber security, Quality Engineering, conformance and interoperability, performance and operational resilience assurance.

Where independent assurance adds value

Cyber and OT assurance

Penetration testing, architecture and trust-path review, OT and remote-access assessment, cloud and identity assurance, and validation of remediation.

Quality and secure change

Quality Engineering, system integration, test automation, performance, resilience, failover and recovery validation across critical energy journeys.

Supplier and ecosystem assurance

Implementation-specific assessment that goes beyond questionnaires to test products, access, evidence, interoperability and recovery assumptions.

Continuous Confidence

A repeatable assurance rhythm linked to material change, incidents, supplier transitions and evidence expiry.

Resillion's wider energy work includes connected-service programmes spanning software delivery, interoperability, operational technology, grid-facing systems and multi-party assurance. Work with organisations including Octopus Energy and ScottishPower informs this whole-service perspective; these engagements demonstrate energy-sector capability rather than NIS2 compliance case studies.

PARTNERSHIP

The objective is not a one-off NIS2 exercise. It is an assurance relationship that helps the organisation keep evidence current as technology, suppliers, operations and the threat environment evolve.

CLOSE THE CONFIDENCE GAP

Five questions for the next executive meeting

The framework is most valuable when it changes the evidence leadership demands and the decisions it is prepared to make.

01

Which essential service creates the greatest unacceptable impact?

02

Which dependency or supplier is least evidenced?

03

What material change has occurred since confidence was last established?

04

Which decision would be hardest to make if a significant incident began tomorrow?

05 When did we last demonstrate recovery of the complete service – not only the technology?

FINAL PRINCIPLE

Confidence is not the absence of uncertainty. It is leadership's ability to understand the uncertainty, decide within it and keep the supporting evidence current.

Legal and diagnostic note

NIS2 is implemented through national law. Scope, competent authorities, registration, reporting routes, supervision and sanctions can differ by Member State. This briefing provides strategic guidance rather than legal advice. The Resillion framework is a management and assurance model; it is not a statutory audit, certification or externally validated peer benchmark.