△ VISAC TECHNOLOGIES

READINESS CHECKLIST · ENERGY & UTILITIES

A 5-Step NIS 2 Readiness Checklist for CISOs

A practical starting point for CISOs, Heads of Infrastructure and Risk Managers preparing critical energy and utilities operations for NIS 2 enforcement — from scope and risk management to incident reporting and board sign-off.

VISAC TECHNOLOGIES INTELLIGENCE TEAM

CRITICAL INFRASTRUCTURE · NIS 2 DIRECTIVE

This checklist distils the NIS 2 Directive's core obligations — risk management (Article 21), incident reporting (Article 23) and governance (Article 20) — into five practical workstreams for energy and utilities operators. Use it to identify gaps before your next audit or board review, alongside our article *Beyond Compliance: Navigating NIS 2 in the Energy Sector with Edge Intelligence*.

01 Confirm Your Scope and Map Asset Exposure

- [ ] Determine whether your organisation qualifies as an "essential" or "important" entity under NIS 2 in each relevant Member State.
- [ ] Inventory every IT, OT and physical asset connected to critical operations — substations, pipelines, control rooms, remote sites.
- [ ] Identify assets sitting in disconnected silos — OT logs, perimeter sensors, geographic or climate data — with no unified visibility.
- [ ] Flag single points of failure where a lost network link would leave your security posture effectively blind.

02 Implement the Article 21 Risk-Management Baseline

- [ ] Document risk analysis and information-system security policies, and a process to assess their ongoing effectiveness.
- [ ] Formalise incident-handling, backup management, business continuity and crisis-management plans.
- [ ] Extend security requirements to direct suppliers and service providers, including cloud providers (supply chain security).
- [ ] Enforce multi-factor or continuous authentication, encryption and access-control policies across OT and IT.
- [ ] Deliver basic cyber-hygiene practices and training to relevant staff — not only the IT department.

03 Build a 24/72-Hour Incident Reporting Pipeline

- [ ] Define what qualifies as a "significant incident" for your organisation under Article 23 — severe operational disruption or financial loss, or considerable damage to others.
- [ ] Establish a workflow that can issue an early warning to your CSIRT or competent authority within 24 hours of becoming aware.
- [ ] Prepare an incident notification with an initial severity and impact assessment within 72 hours.
- [ ] Assign clear ownership for the final report, due no later than one month after the incident notification.
- [ ] Rehearse the reporting pipeline end-to-end before you need it in a live incident.

04 Prove Operational Continuity Under Network Isolation

- [ ] Run a "loss of connectivity" drill: simulate a severed link between a remote site and central systems.
- [ ] Verify that local or edge systems continue to capture signal, evaluate risk and support workflows autonomously during the drill.
- [ ] Confirm every automated alert or human intervention taken during the drill is logged with a traceable, source-linked evidence chain.
- [ ] Fuse geospatial and operational context so teams can see not just that an asset is exposed, but why, and which nearby events are driving it.

05 Secure Management Sign-Off and Ongoing Oversight

- [ ] Brief the management body on its Article 20 obligations: approving risk-management measures, overseeing implementation, and completing training.
- [ ] Note that management bodies can be held personally liable for non-compliance — this is not a delegate-and-forget exercise.
- [ ] Schedule recurring reviews of the effectiveness of your risk-management measures, not a one-off audit.
- [ ] Put NIS 2 readiness on a standing board agenda ahead of your Member State's enforcement deadlines.

NEXT STEP

See how Edge Intelligence supports this checklist in practice

VISAC Edge™ keeps risk assessment and evidence capture running even when connectivity to the centre is lost. LOVHEN™ fuses geospatial and operational signals into a single exposure picture. Together they support Steps 1, 3 and 4 above.

Request a briefing at visactechnologies.com