

What Observable Governance delivers in critical infrastructure

Benefits, growth and savings. Continuum as the path. Written in the voice of a working AI programme note.

GOVERNANCE FLOWS DOWN · OBSERVABLE FLOWS UP

Start here

Energy, water, transport, telecoms and other essential operators already have chat tools and first agents. People already use unofficial ones — on tickets, shift notes, vendor manuals and network change. Supervisors now ask two things: who may touch a live system or an operational file, and how do you know?

Use is common. Live operational impact is not. McKinsey finds 88 in 100 firms use AI. Only 37 in 100 can show any effect on operating profit. About 6 in 100 see a material effect. Most of the official tools never leave the trial.

Why? The official tool cannot be halted. It cannot connect to the operational system of record. Nobody can look up last month's yes or no. So OT security and the NIS2 accountable person will not bless it. Staff keep the unofficial tool.

Critical infrastructure has extra locks. NIS2 covers essential and important entities: risk, incident reporting, supply chain, management-body duty. The CER directive covers resilience of critical entities. Sector rules sit on top — energy, rail, water, telecoms, public admin. An agent that can open a change on an operational network is not a desktop chatbot.

What you get if you fix that: the assistant is allowed to finish the job on a named path. Growth is the process you can put it on — planning, maintenance, incident write-up, customer ops that must not touch OT. Saving is the waiting and the duplicate tool you stop running.

This note does not invent “saves \$X per operator.” McKinsey does not publish that. Size the first process. Then copy it.

Words used here

- Observable Governance — the rule that applies to a live step can be shown, and last month's allow or deny can be looked up, with the rule version.
- Continuum — the shared path: owner, rules, door into the official system, record.
- OT — operational technology. The controls that run the plant, the grid, the network, the railway.
- NIS2 / CER — EU rules on cyber risk, incidents, supply chain and resilience for essential operators.

1. What it delivers — three tests, for an essential operator

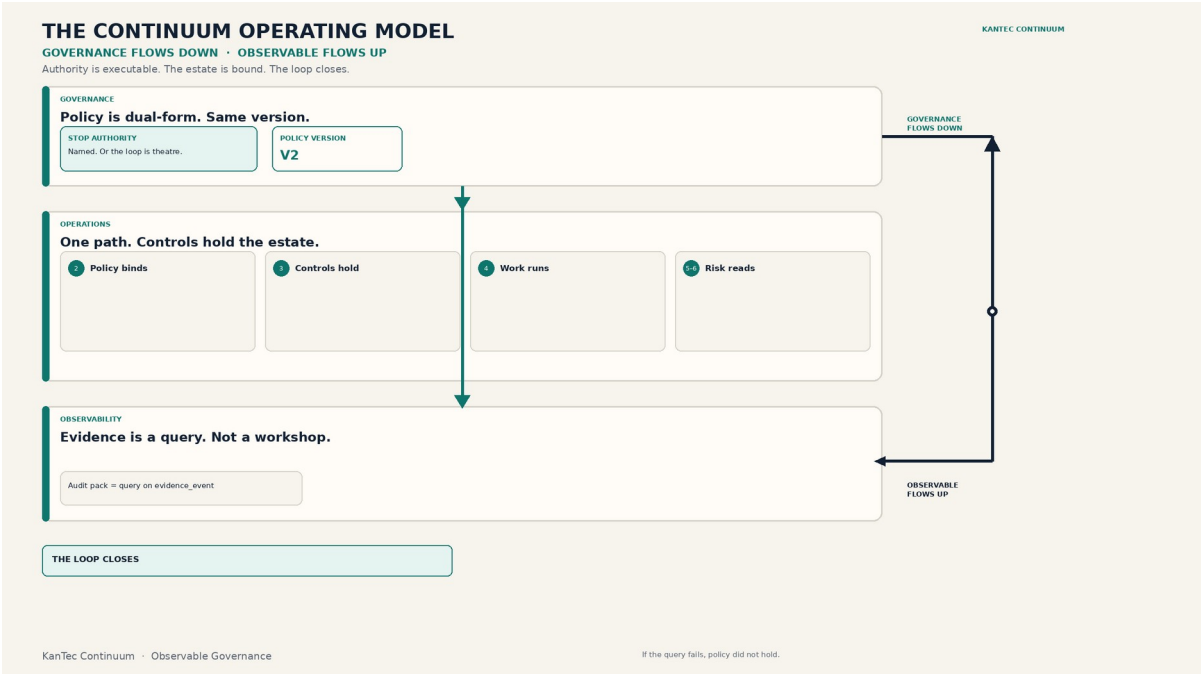


Figure. Policy down onto the ticket, the change, the field step. Proof back up to OT security, the NIS2 lead and the board.

Test	What you can show
Authority is executable	A named stop owner can halt an agent on a change, a ticket or a field path. The rule exists as intent and as code, same version.
The estate is bound	The assistant uses the same named door as every other caller. No path from a desktop agent into OT unless that door is named. Unscoped tools fail closed. If the rules engine is silent, the step is refused.
The loop closes	Allow or deny writes who (operator, engineer, bot or agent), what, which rule version, which door. The next rule cites those records. The incident pack is that look-up.

2. Benefits by the people who feel them

Business line — growth they can ship

- The assistant can update the real ticket or plan, not only draft in a side window.
- The unofficial tool becomes a named tool — or it stops.
- OT security and the NIS2 lead can answer from a look-up, not from a workshop.

Risk, compliance, audit — a pack that exists

- One record serves NIS2, the AI Act and the board.
- You can show last month's changes stayed off the OT network you promised to isolate.
- “Just this once” has an end date.

Operations and technology — one plane

- No second “AI SOC” beside OT security. One path.
- If the model or the integrator must change, the work has a named exit — not a war-room.

Customer and colleague

- Field staff and customers are told when they are talking to an AI (Article 50, live from 2 August 2026).

- A wrong step can be found. The record is searchable.

3. Growth opportunities — where the path pays

McKinsey’s operations work puts large generative-AI potential in maintenance, planning and customer operations — if the tool sits in the real process. On essential networks the bar is higher: the tool must be halt-able and must not wander into OT. That is a pool, not a promise.

Domain	What Observable Governance unblocks
Planning and field ops	Work-order and shift agents that may read and, where the rule allows, write the ticket — not a chatbot that stops at a summary.
Customer and market ops	Contact-centre and outage assistants that can be shown to the regulator. Growth without a mystery model on a laptop in a substation.
Maintenance and asset	A maintenance-copilot on a named door. It may read manuals and history. It may not open an OT session unless that door is named.
Incident and change	Incident-write-up and change assistants on a halt-able path. Annex III essential-services clock from 2 December 2027 — build the path now.
Engineering	Build and config agents that cannot land unsigned change into a live network. Throughput without a shadow pipeline.

Growth rule: pick the process that is already leaking into unofficial tools. That is the demand signal. Do not start with a platform programme.

4. Savings — what you can defend, and what you cannot

What the research lets you say

- Waiting. On programmes McKinsey watched, 30 to 50 percent of build time was permission and rework. A shared path cut that wait. They have seen approval time drop by as much as 90 percent.
- Missing profit. 88 in 100 use AI. 37 in 100 show any profit effect. About 6 in 100 show a material one.
- When it is live. A selected McKinsey client group that changed how work runs saw about \$3 back per \$1 after the tool was live. Not a promise for a demo.
- The pool. McKinsey’s operations work puts large generative-AI value in maintenance and planning. A live, halt-able path takes a slice. A stranded trial takes none.

Savings you can size on a first process

- Hours not spent rebuilding the same risk pack for each pilot.
- Unofficial licences, plugins and duplicate prompt-spend retired once the attested assistant does the job.
- Fewer dual-running teams (official bot plus the private one that actually works).
- Incident and audit cost: reconstruct-from-Slack versus query-the-store.
- Integrator and model exit drills that are paper today and a switch tomorrow (NIS2 supply chain).

What this note will not invent

There is no honest industry-wide “saves 12 percent of opex” figure. Size the first process: hours in the permission queue, unofficial tools to retire, tickets written back per week once live — and zero unauthorised OT sessions.

5. OT access — what “off OT unless named” means

OT is the plant, the grid, the signal box, the radio network. It is not the ticket system. An assistant that can open a session on OT is a control system, not a chatbot.

- Default deny. No tool-call, script or MCP action may open an OT protocol, jump host or engineering workstation unless that action is named on the path.
- Separate identities. The bot that writes a work order is not the account that talks to a PLC or an RTU. If those identities ever meet, that is an incident.
- Named door only. If OT access is required (read a historian, propose a setpoint), it goes through a checked jump path: who asked, which rule version, which asset, how long, who can halt it.
- Time-boxed. OT sessions expire. “Just this shift” has an end time.
- Fail closed. If the rules engine is silent, the OT door stays shut. A timeout is not an allow.
- Record. Every attempt — allowed or refused — is written. Last month’s “we never touched OT” is a look-up, not a hope.

That is Observable Governance on the operational side. Governance flows down to the OT door. Observable flows up as the list of attempts.

6. NIS2 — what the operator must be able to show

NIS2 (Directive 2022/2555) is live in Member State law for essential and important entities. The management body owns cyber risk. You cannot delegate that to a vendor or to an AI programme.

- Risk management — policies, access control, crypto, backup, supply chain, vulnerability handling, hygiene. An unofficial agent on a change path is a supply-chain and access-control finding.
- Incident handling — detect, respond, report to the CSIRT / competent authority in the statutory window. An agent that writes a bad change is an incident, not “just a model.”
- Reporting — early warning and follow-up. The same evidence store should feed the notice. Reconstruct-from-Slack will not make the clock.
- Supply chain — you assess the model host, the MCP farm and the integrator the way you assess any ICT provider. Concentration is a finding.
- Management duty — training and oversight. If the board cannot look up last month’s OT-adjacent allows, they do not have oversight.

NIS2 does not ban AI. It bans an essential operator who cannot halt, report or explain a digital act on a critical function. Continuum is how those three become one path.

7. Cyber Resilience Act — the product rule around the same path

The Cyber Resilience Act (Regulation 2024/2847) is about products with digital elements placed on the EU market: software, devices, components. It entered into force in December 2024. The main product duties apply from 11 December 2027. Reporting of actively exploited vulnerabilities and severe incidents starts earlier.

- If you sell or put into service an assistant, an agent runtime, a gateway or an OT connector as a product, CRA essential cybersecurity requirements apply: secure by default, no known exploitable vulnerabilities at release, support window, vulnerability handling.
- CE marking and technical documentation will be expected for in-scope products. Important and critical products face a harder conformity path.

- A product that can reach OT is not a convenience feature. It is a product with a high-impact digital element. Default-deny OT, named doors and a searchable record are how you show secure-by-default — not a slide.
- CRA does not replace NIS2. NIS2 is the operator. CRA is the product you buy or ship. An operator can be both: they run the plant (NIS2) and they ship an internal tool that behaves like a product (CRA).

Frame for the board: NIS2 asks whether the operator can run and report. CRA asks whether the digital product you put on that estate is built to be halt-able and patchable. Observable Governance is the evidence both questions share.

8. How the saving and the growth show up in 90 days

- Day 0 — stop owner named on one process (work orders, incident write-up, customer outage, change).
- Days 1–30 — unofficial tools on that path listed. Dual-form rule. Residency and key tier set.
- Days 31–60 — attested door live (API + governed MCP). Unscoped tool-call fails closed.
- Days 61–90 — query works. First rule change cites live records. NIS2 incident file and AI Act transparency file point at the same store. Unofficial twin retired or denied.

That is the first saving (permission time and a retired twin) and the first growth (write-back on a live ticket). Clone the path. Do not buy a second tower.

9. Decision

Put this under the next agent that wants to touch a live operational file — and keep it off OT unless that door is named.

Fund one path. Not a new framework.

Growth is the process you are then allowed to scale. Saving is the queue and the unofficial twin you stop running.

If you cannot look up last month's yes or no on a change or a ticket — and prove it never opened OT — you are still in the group that uses AI and cannot show control.

— KanTec Platform Engineering · Critical infrastructure brief —