OPERATIONAL RISK GOVERNANCE FOR CRITICAL INFRASTRUCTURE

Master Brief · Rail, Utilities & Critical Infrastructure · Confidential · 2026

"When something goes wrong on your network, Metascape shows you exactly what happened, stops it, and gives you the proof."

SHOW YOU
Clarity

STOP IT
Control

GIVE YOU THE PROOF
Accountability

metaScape

metascape.com

THE REALITY

This Happened. It Will Happen Again.

A Hitachi train management system loses communications at a signal junction on a live service corridor. At the same moment, a remote level crossing goes dark — not because of the train fault, but because an APN outage at a mobile core network has silently taken down the bearer. A contractor made an undocumented change. Nobody logged it. Nobody authorised it. Three suppliers are involved. Not one owns the SLA. There is no single throat to choke.

This is not a technology failure. This is a governance failure.

And it happens every week across rail infrastructure in the UK.

THE PROBLEM

Five Symptoms of the Same Root Cause

The root cause is not bad technology. It is the absence of a governance layer that makes every component, every supplier, and every action accountable.

01 No Single Point of Accountability

Multiple suppliers. Multiple bearers. Multiple contracts. When something fails, accountability dissolves into a vendor conversation while you face the regulator alone. You pay the penalty for someone else's failure.

02 No Real-Time Visibility

Your suppliers know about network degradation before you do. By the time it surfaces, the level crossing is already dark. Reactive management is damage control.

03 Undocumented Changes

A contractor accesses a remote asset, makes a change, and does not log it. Without cryptographic attribution you cannot defend yourself or hold anyone responsible.

04 Failover Exists in Design. Not in Evidence.

When the ORR asks whether failover triggered at what time, you cannot answer with a signed, timestamped record. Assembled evidence is not produced evidence.

05 Detection Without Enforcement

You have dashboards. Between the alert and the action is a human and a delay. On a live rail network, that delay is a risk to safety, service continuity, and your SLA.

WHY NOW

The Regulatory and Commercial Pressure Is Here

The regulatory environment has shifted. Governance is no longer advisory. It is a condition of operation.

NIS2

Not optional. The Network and Information Systems Directive requires critical infrastructure operators to demonstrate active cyber governance with exportable evidence. Monitoring dashboards do not satisfy this. Signed audit records do.

ORR INQUIRIES

The Office of Rail and Road now expects operators to produce attributable, timestamped records of what happened and who authorised it. Retrospective log reconstruction is no longer a sufficient response to a formal inquiry.

INSURANCE

Cyber and operational underwriters are beginning to require demonstrable governance frameworks as a condition of coverage. Evidence-grade records reduce your risk profile and your premiums.

CONTRACTOR LIABILITY

As third-party access to critical infrastructure increases, the inability to attribute actions to specific authorised individuals exposes operators to unlimited liability in the event of contractor-related faults.

HYBRID INFRASTRUCTURE

LTE, 5G, satellite, private APN, public APN — modern rail connectivity is a hybrid fabric. No single bearer is reliable. No single supplier is accountable. The governance layer is not a luxury. It is a necessity.

THE ANSWER

One Platform. Three Outcomes.

Metascape is the control plane that sits across your entire connectivity fabric — every bearer, every supplier, every device, every contractor action. It does not replace your infrastructure. It makes every component of it accountable.

SHOW YOU CLARITY	STOP IT CONTROL	GIVE YOU THE PROOF ACCOUNTABILITY
Within seconds of any event, you have a complete, readable timeline — which device, which bearer, which supplier, which policy triggered. No log-diving. No reconstruction.	When a device or bearer behaves outside defined policy, enforcement is automatic: connectivity suspended, device isolated, bearer switched. The network logs every step.	Every action generates a signed, timestamped evidence record for ORR submission, board review, insurance claims, and contractor disputes. Seconds, not days.

IN PRACTICE

The Same Scenario. With Metascape.

The APN outage occurs. The level crossing bearer degrades. Here is what happens next — without a human initiating anything:

TIME	EVENT	ACTOR
00:00:01	Bearer degradation detected at mobile core. Baseline deviation confirmed.	**Automatic**
00:00:03	Policy evaluated. Failover to secondary bearer initiated.	**Automatic**
00:00:04	Level crossing reconnected on backup bearer. Service continuity maintained.	**Automatic**
00:00:05	Signed evidence record created: primary failure, failover trigger, restoration	**Immutable**
00:00:08	Plain English incident summary generated. Available to operations team.	**Metascape**
00:02:00	Supplier notified with timestamped evidence of their bearer failure.	**Metascape**
00:04:00	Exportable evidence package ready for ORR, board, or insurance submission.	**You**

The level crossing never went dark. You had the proof before anyone asked for it.

HOW IT WORKS

Platform Architecture

Five Integrated Layers

We do not rebuild what already exists. We integrate best-of-breed, battle-tested components behind a single governance layer and make every one of them accountable.

01 DEVICE IDENTITY

eSIM bootstrap · Smallstep CA · ACME/EST protocol

Every gateway generates its own cryptographic identity on-device. Private keys never leave the hardware. Devices enrol automatically via eSIM on private APN — no tokens, no manual steps, no logistics. Certificates are short-lived, auto-rotating, and instantly revocable. A compromised device cannot re-enrol.

02 HYBRID BEARER MANAGEMENT

WireGuard · LTE · 5G · NB-IoT · LoRa · Satellite · Private & Public APN

Encrypted tunnel across every bearer type. When a primary bearer degrades, the policy engine triggers automatic failover — timestamped and logged. No single point of failure. Every failover event is signed evidence.

03 BEHAVIOUR & ANOMALY DETECTION

Skadi (primary) · Nozomi Networks (secondary) · Pluggable interface

Continuous baseline modelling per device and per fleet. Supplier network degradation visible in real time — before it surfaces in your operations. The supplier layer is pluggable; the architecture does not change if the supplier does.

04 POLICY ENFORCEMENT

SIMBIOSYS · Predictable and provable policy decisions

Every enforcement decision is predictable and provable. Same conditions, same response. On trigger: connectivity suspended, device isolated, bearer switched, action logged — simultaneously. Human overrides are fully attributed: who, when, under which authority.

05 GOVERNANCE & EVIDENCE LAYER

Metascape Console · Claude API / Azure OpenAI · Regulator-ready export

Every policy decision, failover event, and human override generates a signed, immutable evidence record. Plain English narrative synthesised in seconds. Evidence bundles exportable for ORR, Network Rail, NIS2, and insurance submissions.

OWNERSHIP

What Metascape Owns

METASCAPE OWNS

- Governance console and evidence layer
- Cryptographic evidence bundle format and signing
- Abstraction interfaces across all supplier layers
- SLA accountability framework and commercial model
- The integration that makes it a single accountable fabric

WE INTEGRATE

- **Smallstep** — PKI and certificate issuance
- **WireGuard** — Encrypted bearer transport
- **Skadi / Nozomi Networks** — Behaviour and anomaly detection
- **SIMBIOSYS** — Policy enforcement engine
- **Claude API / Azure OpenAI** — Evidence narrative generation

HOW WE WORK WITH YOU

Two Engagement Models. One Guarantee.

If we cannot show you exactly what happened, stop it, and give you the proof — we pay the SLA penalty. That is the commitment.

	GOVERNANCE ONLY	MANAGED GOVERNANCE + CONNECTIVITY
What you get	Full visibility, enforcement and evidence layer across your existing connectivity.	We manage every bearer, orchestrate failover, and own the governance layer end-to-end.
Supplier accountability	We give you the evidence to hold your suppliers accountable.	We are the supplier. We hold ourselves accountable.
SLA ownership	You own it. We give you the tools and evidence to defend it.	We own it. Defined service credits. Cryptographic proof.
Best for	Operators with existing bearer contracts who need the governance layer.	Operators who want a single accountable partner for connectivity and governance.
Pricing	Licence + per-device per month.	Managed service + per-device + SLA-linked credits.

PROOF OF CONCEPT

Evidence From Day One. Not Day Thirty.

We do not ask you to take this on faith. The PoC runs a live scenario — detection, enforcement, failover, evidence — and produces a signed evidence bundle in seconds. You can read it, export it, and submit it before you leave the room.

Device enrols automatically

eSIM identity established. Certificate issued. No manual steps. No logistics.

Anomaly detected and stopped

Device behaviour taken outside policy. Enforcement fires automatically. Watch it on screen.

Evidence produced in seconds

Signed record generated. Plain English narrative immediately available.

Bearer failover demonstrated

Primary bearer degraded on command. Secondary activates. Transition logged and timestamped.

Contractor action attributed

Simulated undocumented change logged, attributed, and flagged. Full audit record produced.

Export demonstrated in the room

One document. ORR-ready. Regulator-safe. Produced before you leave.

NEXT STEPS

Three Ways to Start

SEE IT LIVE	HAVE THE CONVERSATION	TAKE THE TECHNICAL SPEC
One demonstration. No slides. No decks. We run the PoC scenario in your environment and you watch the evidence produce itself.	If you recognise the problem but want to understand the fit before committing to a PoC, speak to us. One call. No obligation.	For your engineering and architecture team. Full layer-by-layer specification including supplier stack, protocol detail, and integration architecture.

Book a demonstration · Have the conversation · Request the spec

hello@hyperlogical.com

"When something goes wrong on your network, Metascape shows you exactly what happened, stops it, and gives you the proof."

metascape.com