CAPABILITY INTELLIGENCE

iluminr

Third-Party Risk in the Age of Capability Intelligence

Third party risk is no longer a compliance exercise. It is an operational reality that requires continuous, evidence-based intelligence.

iluminr Capability Intelligence gives organizations verified, continuous insight into how their third parties actually perform under pressure.

iluminr

Visibility into third-party resilience is dangerously thin

Organizations depend on complex webs of vendors, partners and suppliers.

30%

of breaches

now involve a third party, double the share recorded a year earlier

70%

of organizations

report at least one material third-party incident in the past year

45%

of organizations

assess supplier security once a year, and 9% only at onboarding

Sources: Verizon DBIR 2025 · SecurityScorecard Supply Chain Trends 2025 · ISC2 Supply Chain Risk Survey 2025

Why traditional approaches fall short

THE OLD WAY

- Annual questionnaires, self-reported and unverified
- Point-in-time snapshots that age the moment they land
- Assessment fatigue leading vendors to game the process
- No stress-testing under real disruption conditions
- Risk scores with no operational context
- Compliance checkbox, not resilience evidence

CAPABILITY INTELLIGENCE

- Continuous, behavior-based capability data
- Dynamic profiles that update in real time
- Verified performance, not self-reported
- Microsimulations that stress-test disruption response
- Actionable intelligence tied to resilience outcomes
- Evidence regulators and boards can rely on

CAPABILITY INTELLIGENCE

What it is. What it changes.

Capability Intelligence is the practice of assessing what organizations and their third parties can actually do when disruption strikes. The evidence comes from exercises, not declarations.

1

Observable

Evidence from exercises, not self-reported checklists.

2

Dynamic

Profiles update continuously as capabilities evolve.

3

Comparable

Benchmarked against peers and industry standards.

4

Actionable

Linked directly to resilience gaps and investment decisions.

Replaces

Self-reported questionnaires and point-in-time attestations.

Produces

Behaviour-based capability data on every critical third party.

Serves

Risk, procurement, compliance and the board, from one dataset.

How iluminr delivers Capability Intelligence

Four steps from zero visibility to continuous intelligence on every critical third party.

Step 1

Select

Use a microsimulation out of the box, modify one to fit your context, or build a custom scenario from scratch.

Step 2

Activate

Run exercises across your vendor ecosystem, individually or at scale, with minimal overhead.

Step 3

Measure

Capture granular response data: detection speed, decision quality, escalation and recovery.

Step 4

Inform

Generate Capability Intelligence profiles that drive risk decisions, contracts and assurance.

Run individually

A single critical vendor, exercised against the scenario that carries the most exposure.

Or at scale

An entire vendor tier exercised at once, with results comparable across the group.

With or without the vendor

Exercises can run with your own teams responding on the vendor relationship.

THREE WAYS TO RUN

Your microsimulations, your way

Option 1

Catalog, out of the box

Pick a pre-built scenario from the iluminr catalog and run it as-is. Covers the most common third party risk situations and is ready to go immediately.

FASTEST TIME TO VALUE

Option 2

Catalog, modified

Start with a catalog scenario and adjust it to fit your vendors, sector or regulatory context. Same structure, tailored to your situation.

BALANCED EFFORT AND FIT

Option 3

Custom built

Build a microsimulation from scratch for a specific vendor relationship or risk. Full control over the scenario, injects and scoring criteria.

MAXIMUM SPECIFICITY

The five capability domains iluminr assesses

1

Crisis Detection

Speed and accuracy in identifying disruption. How quickly does a third party recognize a problem and escalate appropriately?

2

Decision Quality

Calibre of judgment under pressure. Are decisions documented, rational and defensible? Is decision authority unambiguous?

3

Communication Integrity

Internal and external communication during incidents. Does the right information reach the right people at the right time?

4

Recovery Execution

Ability to restore services within agreed timeframes. RTO and RPO performance tested under realistic, high-pressure conditions.

5

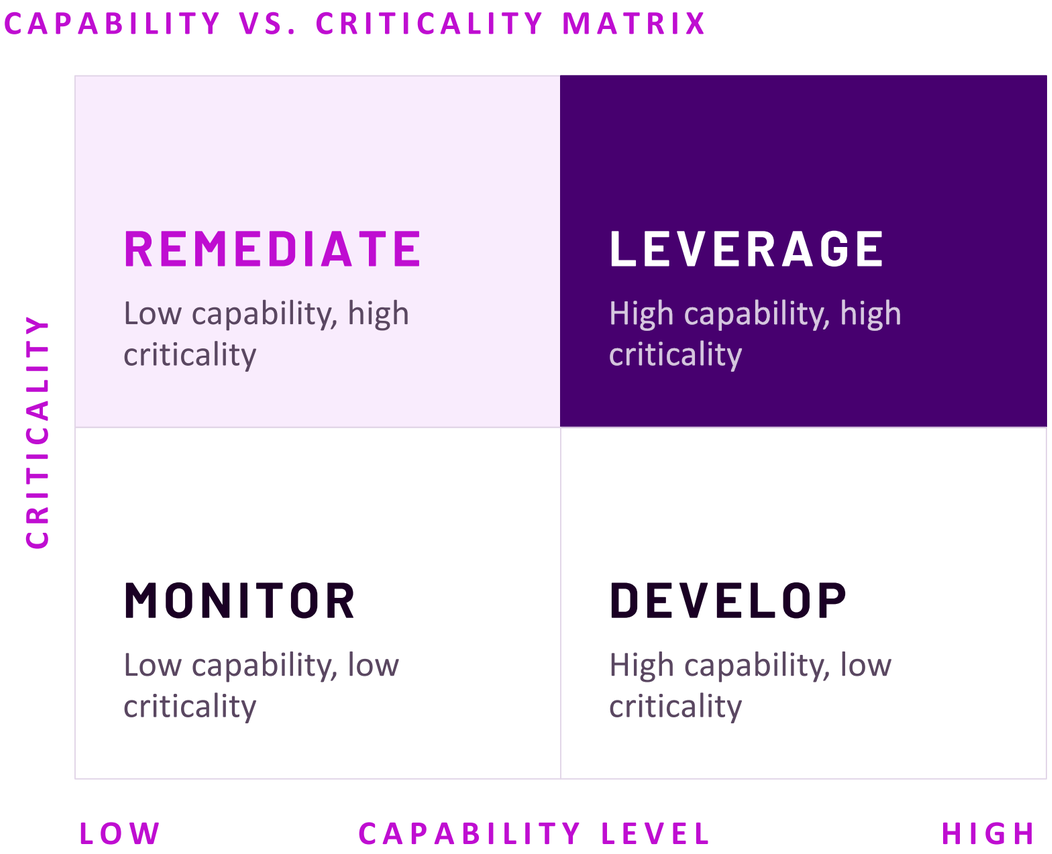
Adaptive Capacity

Capability to learn and adapt from each exercise. Do teams improve systematically? Are lessons embedded into ongoing operations?

From assessment to intelligence

Capability Intelligence gives risk teams a live view of third-party resilience.

Identify high-capability vs. high-risk vendors
Prioritise audits and remediation on real evidence
Meet regulators' ongoing oversight requirements
Build SLAs grounded in demonstrated performance



Capability Intelligence across the risk lifecycle

Procurement and onboarding

Require vendors to demonstrate capability before contracts are signed. Set resilience baselines as selection criteria.

Ongoing due diligence

Replace annual questionnaires with continuous microsimulation data. Flag degradation before it becomes an incident.

Regulatory compliance

Produce evidence-backed assurance for DORA, ISO 22301, APRA CPS 230 and other frameworks requiring ongoing third-party oversight.

Incident response planning

Know before a crisis which vendors will hold. Sequence recovery plans around your most and least capable partners.

Contract negotiation

Anchor SLAs and performance penalties to demonstrated data rather than assumed capability or industry averages.

Board reporting

Present a clear, evidence-based intelligence picture showing where third-parties are strongest and where they need attention.

The regulatory pressure is mounting

Regulators are moving from ‘do you have a policy’ to ‘can you prove it works?’ Capability Intelligence answers that question.

DORA

EU · FINANCIAL SERVICES · APPLIES JAN 2025

Mandates ICT third-party risk management with evidence-based testing of critical providers.

ISO 22301

GLOBAL · ALL SECTORS

Requires documented and exercised supply chain resilience capabilities.

APRA CPS 230

AUSTRALIA · FINANCIAL SERVICES · IN FORCE JUL 2025

Demands continuous monitoring, testing and assurance of all material service providers.

FCA / PRA

UK · FINANCIAL SERVICES · IN FORCE MAR 2025

Operational resilience rules require third parties to demonstrate and evidence recovery capabilities.

NIST CSF 2.0

USA · ALL SECTORS · PUBLISHED 2024

Govern function explicitly includes third-party and supply chain risk obligations.

Getting started with iluminr

Most organizations are 30 days from meaningful Capability Intelligence on their critical third parties.

WEEK 1 TO 2

Scope

Identify critical third parties and the capability domains most relevant to your sector and regulatory obligations.

WEEK 2 TO 3

Design

Collaborate with iluminr to build tailored microsimulations for each vendor tier.

WEEK 3 TO 4

Run

Activate exercises across your vendor ecosystem, with or without direct vendor participation.

WEEK 4 ON

Inform

Receive Capability Intelligence profiles and a prioritized remediation roadmap ready for board and regulatory use.

What you provide

A list of critical third parties and the obligations you report against.

What iluminr provides

Scenario design, delivery and the Capability Intelligence profiles that follow.

Vendor participation

Optional. Exercises can run with your own teams responding on the vendor relationship.

NEXT STEP

iluminr

Know your third parties. Know your risk.

Third party risk managed through Capability Intelligence.

Ready to close the gap?

A Capability Intelligence briefing tailored to your sector
A live microsimulation run against a third party scenario
A customized third party risk maturity assessment

BOOK A BRIEFING