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.

The Third Party Risk Problem

Organizations depend on complex webs of vendors, partners and suppliers. Visibility into their actual operational resilience is dangerously thin.

98%

of organizations

impacted by a third party breach in the last two years

51%

of supply chain risks

remain undetected until an incident actually occurs

73%

of compliance teams

say third party assessments are outdated within 90 days

Sources: Prevalent Third-Party Risk Report I Ponemon Institute I Gartner

Why Traditional Approaches Fall Short

iluminr

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

VS

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

iluminr

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

How iluminr Delivers Capability Intelligence

iluminr

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

1

Select

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

2

Activate

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

3

Measure

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

4

Inform

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

THREE WAYS TO RUN

Your Microsimulations, Your Way

Every organization comes with different internal capability and different vendor relationships. iluminr supports three approaches.

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

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

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 5 Capability Domains iluminr Assesses

iluminr

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.

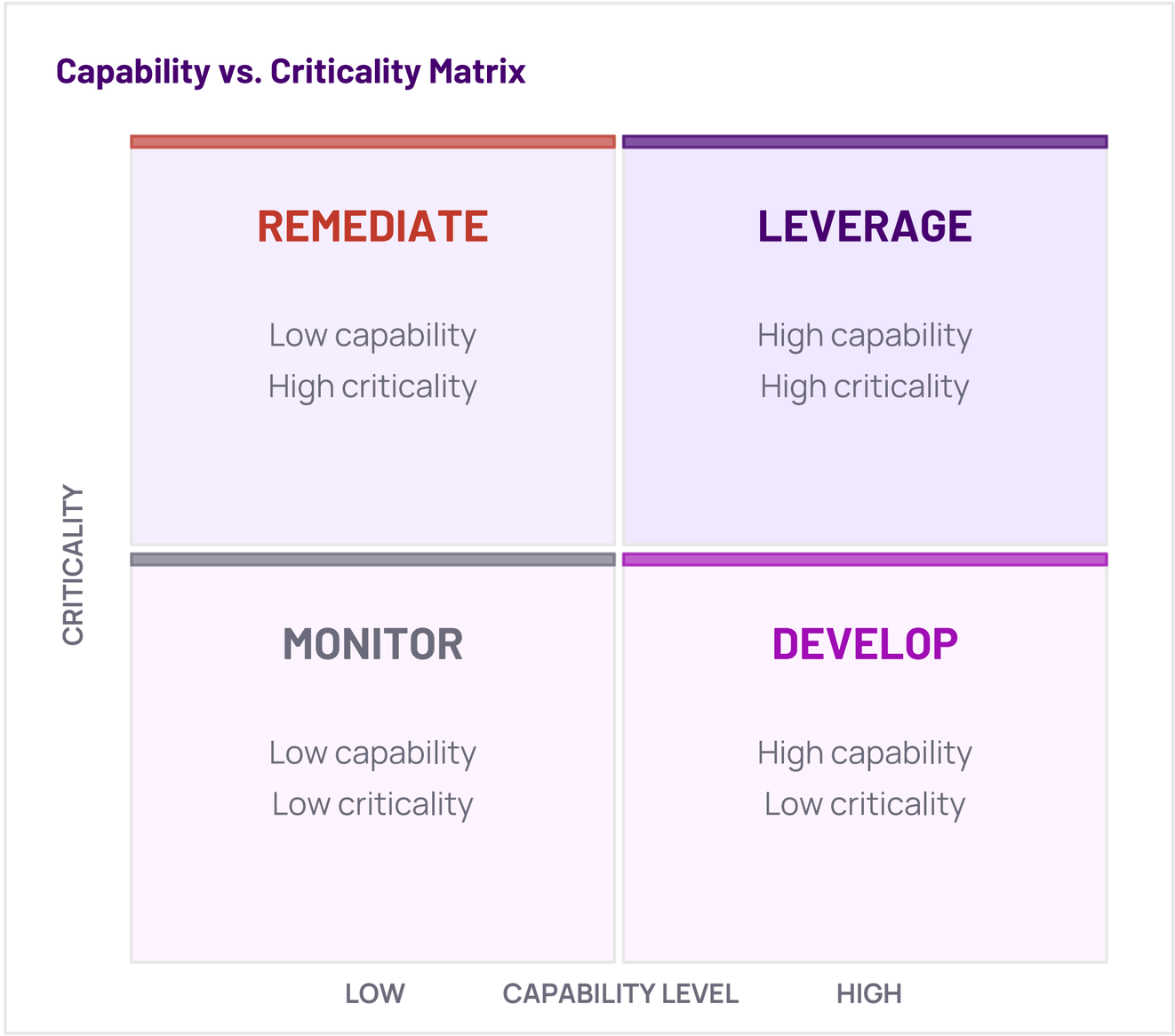
5. Adaptive Capacity

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



WHERE TEAMS USE IT

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	Mandates ICT third-party risk management with active, evidence-based testing of critical providers
ISO 22301 Global, All Sectors	Requires documented and exercised supply chain resilience capabilities with continuous improvement
APRA CPS 230 Australia, Financial Services	Demands continuous monitoring, testing and assurance of all material service providers
FCA / PRA UK, Financial Services	Operational resilience rules require third parties to demonstrate and evidence recovery capabilities
NIST CSF 2.0 USA, All Sectors	Govern function explicitly includes third-party and supply chain risk management 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.

iluminr

Know your third parties. Know your risk.

Third party risk managed through Capability Intelligence.

Book a Briefing

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

iluminr.io