Ekselens

EKSELENS360

EKSELENS INSIGHT · CYBER & RESILIENCE

Concentration risk: when one supplier failure stops the business

Modern operations depend on a small number of platforms and providers. Map that dependency by business service, decide what is acceptable and plan for the rest.

THE EIGHT-PHASE METHOD

01 Discover
02 Diagnose
03 Design
04 Plan
05 Mobilise
06 Deliver
07 Embed
08 Optimise

Ekselens Consulting
ekselens.com · info@ekselens.com

Changing how transformation is done
The EKSELENS360 family

CYBER & RESILIENCE · 12 NOVEMBER 2026 · 4 MIN READ

The global IT outage of July 2024, caused by a single faulty security software update, showed how far one supplier's failure can reach. Airlines, hospitals, banks and retailers were disrupted at the same time — not because they had made the same mistake, but because they depended on the same provider.

That is concentration risk. It is growing as organisations consolidate onto fewer platforms, and it is easy to miss because each individual decision to standardise looks sensible on its own.

Why concentration is hard to see

Supplier risk is usually assessed contract by contract. Concentration only appears when you look across them. Three patterns are common:

- **Hidden common dependencies.** Different suppliers rely on the same cloud provider, security tool or data centre.
- **Platform gravity.** Core processes, data and integrations accumulate on one platform until leaving is impractical.
- **Single points of expertise.** A niche supplier, or a small team within one, is the only party that understands a critical system.

None of these shows up in spend analysis. A low-cost service can sit underneath several critical processes.

Map dependency by business service

Start from what the organisation must keep running, not from the supplier list. For each important business service:

- trace the people, processes, technology and suppliers it depends on;
- include the suppliers' own critical providers where you can find them;
- identify where several services share the same dependency;
- set a tolerance for how long the service can be disrupted.

Financial services firms have worked this way under the UK operational resilience rules, which required them to remain within impact tolerances for important business services from March 2025. The approach works well beyond financial services: it turns an abstract risk into a specific, prioritised list.

Decide what concentration is acceptable

Concentration is not always bad. Standardising on a major platform can improve security, reduce cost and simplify operations. The aim is a deliberate decision, not zero concentration. For each significant dependency, decide whether to:

- **accept** it, with a documented rationale and a tested recovery plan;
- **mitigate** it, through architecture, alternative providers for the most critical functions, or contractual protections;
- **reduce** it over time, as contracts come up for renewal.

Record the decision and who made it. When a provider fails, the question will be whether the risk was understood and managed, not whether it existed.

Build protection into contracts and renewals

Contracts are the most practical lever. At renewal, review critical suppliers for:

- notification duties for incidents and for changes to their own key providers;
- resilience commitments, testing and the right to see evidence;
- support during an incident, including priority and escalation routes;
- exit and transition support, with data returned in usable formats.

A supplier tiering model keeps this proportionate: deep scrutiny for the few suppliers whose failure would stop the business, lighter oversight for the rest.

Test the scenario, not just the system

Run an exercise in which a critical platform or supplier is unavailable for several days. Work through which services stop, what the workarounds are, and how customers are told. Most organisations discover at least one dependency they had not mapped and one workaround that does not exist.

The board question

The test for leadership is simple: if our most critical supplier failed tomorrow, which services would stop, for how long, and what would we do? If the answer depends on finding out at the time, the mapping is the place to start. It takes weeks, not months, and it makes every subsequent supplier decision better informed.

Want to talk this through?

Book a 45-minute discovery conversation. Bring one challenge, leave with three prioritised next steps — written up within 24 hours.

ekselens.com/contact
info@ekselens.com
+44 (0) 20 7874 7217

© Ekselens Consulting. All rights reserved.