Concentration Risk: The Threat You're Underestimating



Ritu Jethani

Director, ERM & TPRM, KPMG US

2026 KONnect

What You'll Walk Away With

Three learning objectives for today's session

01

Identify & Quantify

Surface concentration risk across your third-party portfolio — technology stack dependencies, geographic clusters, and single-vendor relationships.

02

Elevate & Integrate

Build concentration risk into your enterprise risk framework so it's reported, monitored, and owned at the right level of the organization.

03

Diversify & Contract

Develop diversification strategies and contractual contingency plans before a disruption forces your hand.

A Rough Month, Twice Over

Two outages. One quarter. Millions of businesses.

9 hrs

AWS US-EAST-1 outage, Oct 20, 2025 — DNS failure cascaded into DynamoDB, EC2 and IAM, taking down Snapchat, Ring, Robinhood and more

32%

of the global cloud market runs on AWS alone — one region's DNS issue, felt worldwide

28%

of global HTTP traffic flows through Cloudflare — its Nov 18, 2025 outage broke access to X, ChatGPT and payment platforms

Neither event was a cyberattack. Both were single points of failure inside infrastructure that thousands of unrelated companies happened to share.

Vendor Risk vs. Concentration Risk

They sound similar. They are not the same problem.

VENDOR RISK

Is this one supplier financially sound, secure, and compliant?

- Assessed one relationship at a time
- Owned by procurement / TPRM teams
- Scored on the vendor's own control environment
- Answers: 'Can I trust this vendor?'

CONCENTRATION RISK

What happens when many relationships fail together, at once?

- Assessed across the entire portfolio
- Owned at the enterprise risk level
- Scored on shared exposure — platform, region, subcontractor
- Answers: 'What breaks if this fails?'

2026 KOnnect

Why It Goes Unmeasured

The TPRM blind spot

1 **Assessments run vendor-by-vendor**

Most TPRM programs score each relationship in isolation — nothing rolls up to show shared exposure across the portfolio.

2 **Fourth parties stay invisible**

Your vendor's cloud provider, payment processor, or data center rarely appears in your risk register at all.

3 **Ownership sits below the line of sight**

Concentration is a portfolio-level property; TPRM teams manage relationships, not the portfolio's shape.

4 **It's cheap and convenient — until it isn't**

Consolidating on fewer, larger providers reduces cost and complexity, which quietly increases correlated exposure.

Three Faces of Concentration Risk

Where hidden concentration accumulates in a third-party ecosystem

Technology Stack

Multiple "different" vendors all run on the same cloud region, the same core platform, or the same code library beneath the surface.

Geographic Clusters

Critical suppliers, data centers, or back-office operations physically concentrated in one country, port, or seismic zone.

Single-Vendor Relationships

One provider handles a critical process end-to-end with no qualified alternative and no practiced fallback.

CASE STUDY — TECHNOLOGY STACK CONCENTRATION

One DNS failure, one region, global fallout

AWS US-EAST-1 Outage — October 20, 2025

- A DNS resolution failure in AWS's Virginia region disrupted DynamoDB endpoints.
- The fault cascaded into IAM, EC2 instance launches, and dozens of dependent services.
- Outage lasted roughly nine hours, with residual errors for hours afterward.
- Affected services included Snapchat, Ring, Robinhood, McDonald's mobile ordering, Signal, and Fortnite — companies with no direct relationship to each other, all exposed through the same region.

THE TAKEAWAY

"It could have just as easily happened at Azure or Google Cloud."

The lesson isn't to abandon the cloud — it's that resilience has to be designed for, tested, and made a board-level conversation.

CASE STUDY — CONCENTRATED INTERNET BACKBONE

A configuration bug, not an attack — and still global

Cloudflare Outage — November 18, 2025

- Came weeks after the AWS incident — part of a string of 2025 infrastructure disruptions.
- Root cause was an internal configuration bug, not a cyberattack.
- Broke access to platforms including X, ChatGPT, major e-commerce sites, financial services, and public-sector portals.
- Even the outage-tracking site Downdetector was reportedly unreachable — a reminder that monitoring tools can share the same fate as what they monitor.

SCALE OF DEPENDENCY

28%

of global HTTP traffic passes through Cloudflare's network

Concentration isn't only a cloud-compute problem — it lives in CDNs, DNS, identity providers, and payment rails too.

CASE STUDY — SINGLE-VENDOR SOFTWARE CONCENTRATION

When one update grounds a global economy

CrowdStrike / Microsoft Outage — July 19, 2024

- A flawed content update to CrowdStrike's Falcon sensor crashed Windows machines worldwide.
- Grounded flights and stranded passengers at airports across the globe.
- Disrupted hospitals, banks, broadcasters, and emergency dispatch systems.
- No cyberattack, no exotic exploit — a routine update to endpoint security software that sat on a huge share of enterprise devices.

THE TAKEAWAY

Standardizing on one security vendor for uniformity is exactly what makes the failure uniform too.

Homogeneity in your endpoint, identity, or security stack is efficient — and it is also a single point of failure at enterprise scale.

The Pattern Behind the Headlines

Three very different incidents. The same underlying shape.

It wasn't a security failure
None of the three incidents involved a breach. Concentration risk materializes through ordinary operational failure, not just attack.

The affected companies had no relationship to each other
Diversified vendor lists still converged on the same underlying platform, region, or code path.

Recovery time depended on visibility, not intent
Organizations that had mapped their dependencies recovered faster — the ones that hadn't were still discovering exposure hours in.

LEARNING OBJECTIVE 1

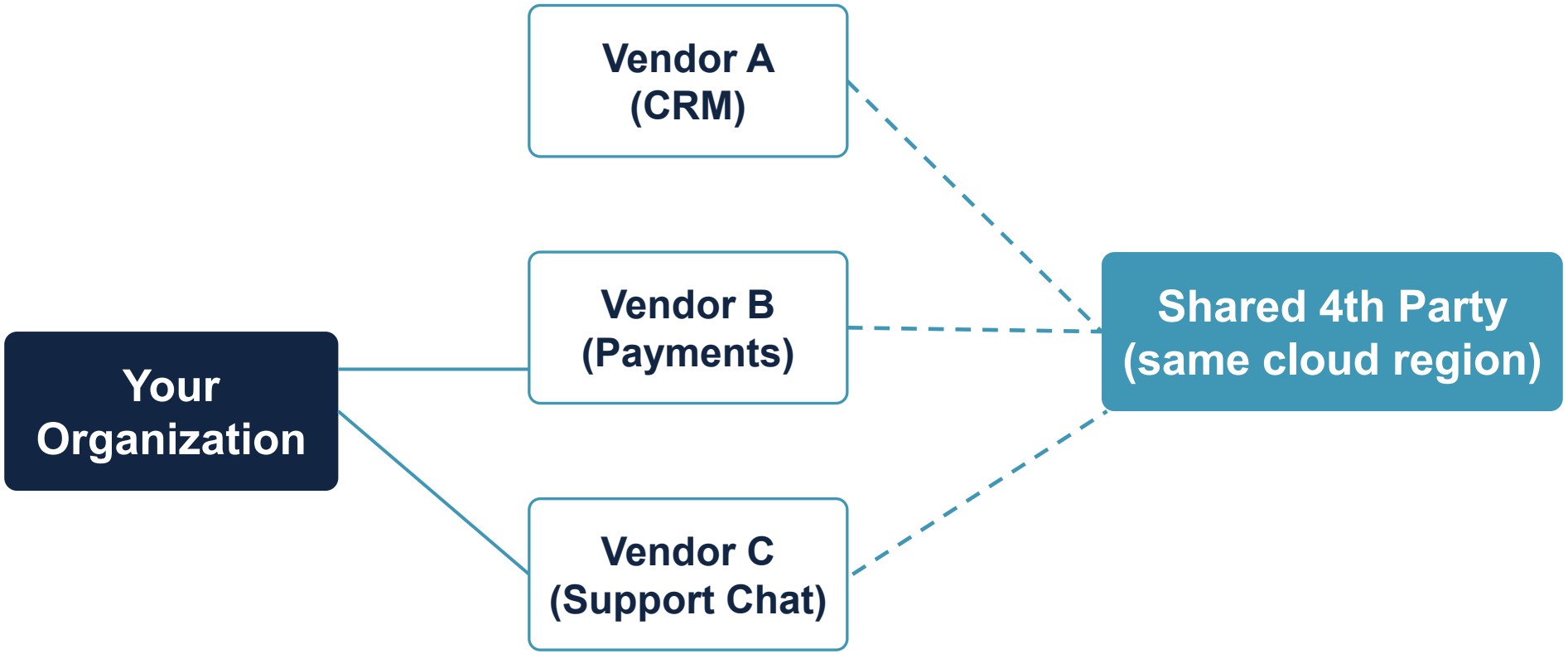
Identify & Quantify Concentration Risk

Finding the exposure hiding inside a diversified-looking vendor list

2026 KOnnect

Uncovering Hidden Dependencies

Your vendors' vendors are your risk too



Three "independent" vendors — CRM, payments, and support chat — can all run their infrastructure on the same cloud region. On paper you have diversified suppliers; underneath, you have one dependency.

What to Measure

Concentration dimensions and the questions each one answers

Dimension	Key Question	Example Data Point
Technology stack	How many critical vendors sit on the same cloud, platform, or core system?	% of critical apps hosted in one cloud region
Geographic clusters	Are critical suppliers or facilities concentrated in one country or corridor?	# of Tier-1 suppliers within one geography
Single-vendor criticality	Does one vendor run a process with no qualified backup?	Revenue tied to processes with zero substitutes
Nth-party exposure	Do multiple vendors quietly share the same subcontractor?	# of vendors reliant on the same 4th party

A Simple Way to Score It

Build a Concentration Index per critical process, not per vendor

1

Map the process

Identify every vendor, platform, and region touching one critical business process end-to-end.

2

Weight by impact

Score each dependency by revenue at risk, customer impact, and recovery time if it fails.

3

Score shared exposure

Add points where multiple "different" vendors converge on the same cloud, region, or subcontractor.

4

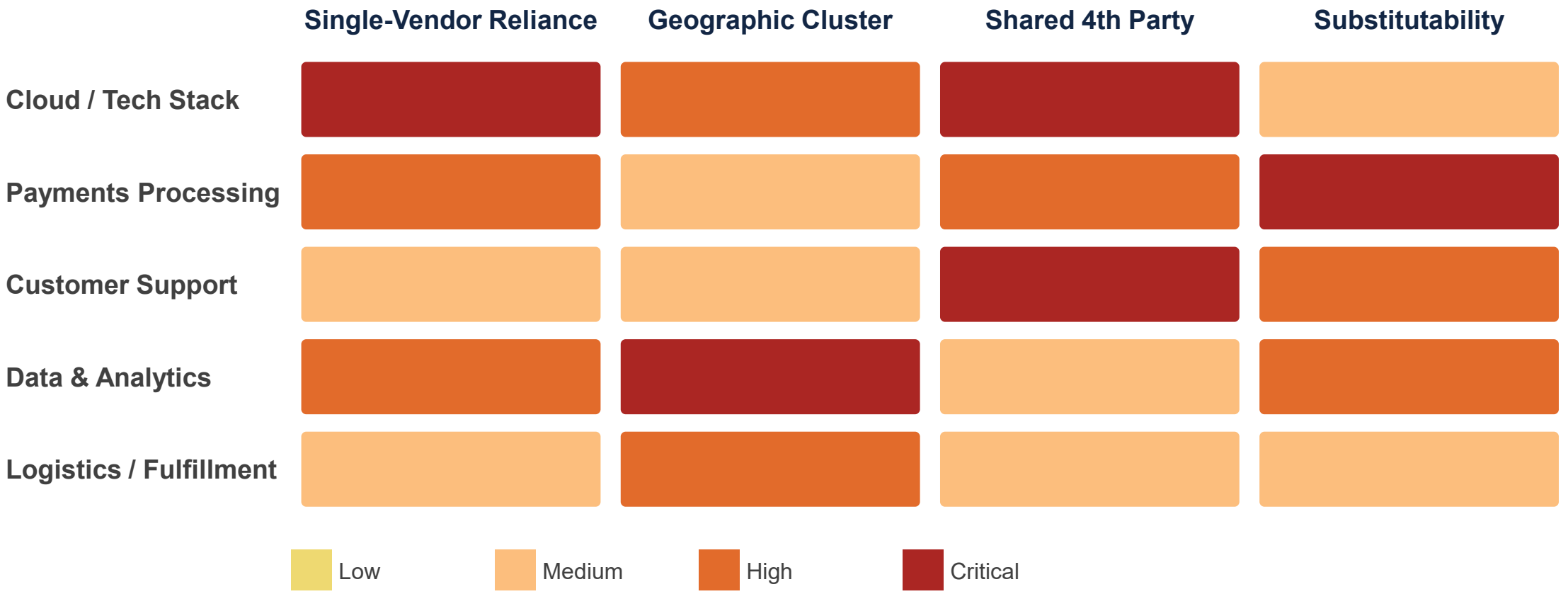
Rank & prioritize

Rank processes by combined score to focus diversification effort where it matters most.

The output isn't a vendor score — it's a process-level view of "how many ways can this one thing break, and do they share a root cause?"

Visualizing Exposure

An illustrative concentration heat map by critical process



Illustrative example — build yours from the scoring exercise on the previous slide.

2026 KOnnect

LEARNING OBJECTIVE 2

Elevate Concentration Risk to the Enterprise

Getting it out of a TPRM spreadsheet and into ERM reporting

2026 KOnnect

From TPRM Silo to Enterprise Visibility

Concentration risk needs a reporting line, not just a register entry

1

TPRM Team

Scores individual vendors; flags shared platforms & subcontractors

→

2

Enterprise Risk Function

Aggregates concentration scores across vendors into portfolio-level exposure

→

3

Risk Committee

Reviews concentration exposure alongside other principal risks quarterly

→

4

Board / Audit Committee

Owns risk appetite for concentration; approves diversification investment

The goal: concentration risk shows up in the same reporting cadence as credit, market, or operational risk — not only inside a vendor management tool.

2026 KOnnect

Reporting Concentration Risk in ERM

What a useful dashboard actually shows leadership

%

Critical Processes Single-Sourced

Share of critical processes with no qualified backup vendor

$

Revenue at Risk by Cluster

Revenue tied to the top geographic or platform concentration

#

4th-Party Overlaps

Count of vendor pairs sharing the same critical subcontractor

▲

Trend vs. Appetite

Direction of concentration score against board-approved risk appetite

Report quarterly at minimum — and immediately following any disruption at a shared provider, even one your organization didn't feel directly.

2026 KOnnect

Regulators Are Already Watching

The EU's Digital Operational Resilience Act (DORA)

What DORA requires of financial institutions

- In force across the EU since January 2025
- Explicitly targets ICT third-party concentration risk, not just individual vendor due diligence
- Requires firms to maintain a register of all ICT third-party arrangements, including subcontractors
- Designates certain critical ICT providers for direct oversight — recognizing that some vendors are systemically important across the whole sector

WHY THIS MATTERS BEYOND FINANCIAL SERVICES

Regulation tends to spread from finance to other critical-infrastructure sectors. Building the concentration risk muscle now — the register, the scoring, the reporting line — puts you ahead of a requirement rather than reacting to one.

LEARNING OBJECTIVE 3

Build Resilience Before Disruption Forces It

Diversification and contractual contingency planning



2026 KOnnect

Diversification Strategies

Reduce correlated exposure without losing the benefits of consolidation

Multi-region, not just multi-cloud

A second vendor in the same region doesn't help — diversify the physical location of critical infrastructure.

Qualify a warm backup, not just a name on paper

An alternate vendor is only a mitigant if it's tested, integrated, and ready to take load on short notice.

Tier by criticality, not by spend

Reserve diversification investment for processes where failure is existential, not for every vendor equally.

Diversify geography for physical suppliers

Avoid single-corridor sourcing for critical materials or components exposed to port, weather, or political risk.

Watch for consolidation creep

Vendor mergers and acquisitions can quietly turn a diversified panel into a concentrated one — revisit the map after every M&A announcement in your supply chain.

Contractual Contingency Planning

Negotiate the fallback before you need it, not during the outage

Before Signing

- Require subcontractor disclosure, including cloud region and 4th parties
- Negotiate data portability and export rights up front
- Set concentration-aware SLAs tied to your criticality tier

During the Relationship

- Right to audit subcontractor changes
- Advance notice clauses for material infrastructure changes
- Joint incident response and communication commitments

When Things Go Wrong

- Defined step-in rights for critical processes
- Exit and transition-assistance clauses with realistic timelines
- Pre-negotiated alternate vendor terms, ready to activate

Your First 90 Days

A practical starting sequence — not a full program redesign

Days 1–30

Map & Discover

Inventory critical processes; pull subcontractor and region data from existing TPRM records; identify obvious clusters.

Days 31–60

Score & Prioritize

Apply the concentration index; rank processes by combined impact and shared-exposure score; brief the risk committee.

Days 61–90

Report & Commit

Add concentration KPIs to ERM reporting; select the top 2–3 processes for diversification or contract renegotiation.

2026 KOnnect

Key Takeaways

1. Concentration risk is a portfolio property — it can't be seen by scoring vendors one at a time.

2. The biggest failures of the past two years weren't attacks; they were ordinary outages in shared infrastructure.

3. Give concentration risk a reporting line to the enterprise risk committee and the board, not just a field in a TPRM tool.

4. Diversify and contract for contingency before a disruption forces the decision under pressure.

QUESTIONS

2026 KOnnect

CONNECT WITH ME



Ritu Jethani

kpmg.com/us

in/ritusainanijethani/

2026 KONnect


THANK YOU
2026 Konnect