IERP®
Institute of Enterprise Risk Practitioners

GLOBAL CONFERENCE 2026

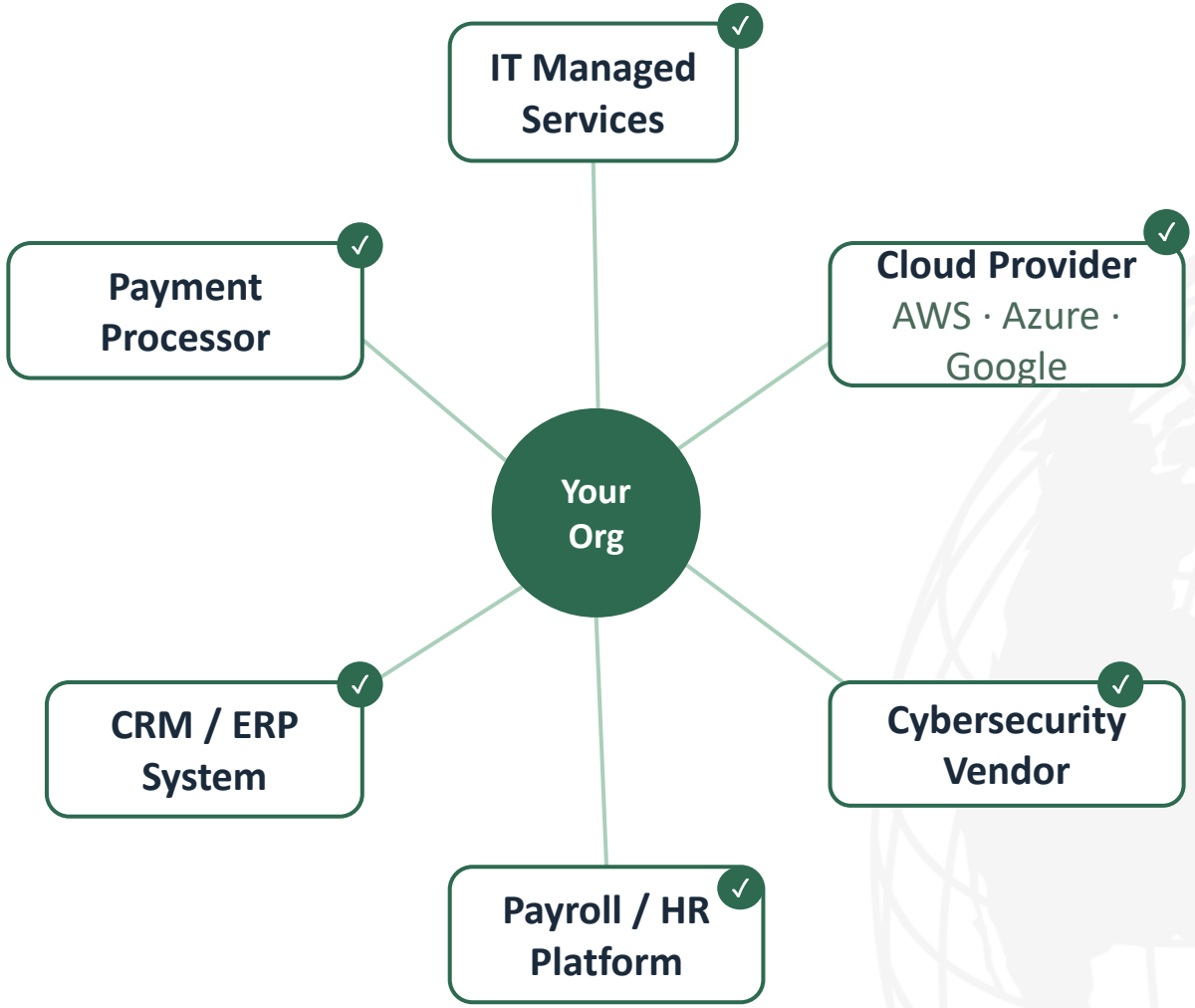
FROM CHAOS TO COMMAND:
RISK LEADERSHIP IN INDUSTRY 6.0

BEYOND FIRST-PARTY RISK: THE DEPENDENCIES YOU DON'T KNOW EXIST

Reece Soukoroff
Global Threat Intelligence Strategist
NOF Consulting

What Your Risk Register Looks Like

Assessed. Registered. Reviewed annually.



This is where most third-party risk programs stop.

The Problem: It Stops a Level Too Early

When something outside the first ring fails, your operations stop - and you had no idea what happened.

IERP®
Institute of Enterprise Risk Practitioners

The Numbers Nobody Talks About

97%

of commercial codebases contain open-source components

64%

of those components were never directly chosen - they came with something else

900+

open-source components in the average enterprise application

91%

of commercial codebases contain open-source components that are outdated or have had no development activity in the last two years

30%

of breaches now involve a third party

That's not a tail risk. That's the most common way organizations get hit.

GLOBAL CONFERENCE 2026
FROM CHAOS TO COMMAND:
RISK LEADERSHIP IN INDUSTRY 6.0

IERP®
Institute of Enterprise Risk Practitioners

3CX

A vendor on a lot of risk registers.

Business phone & communications platform

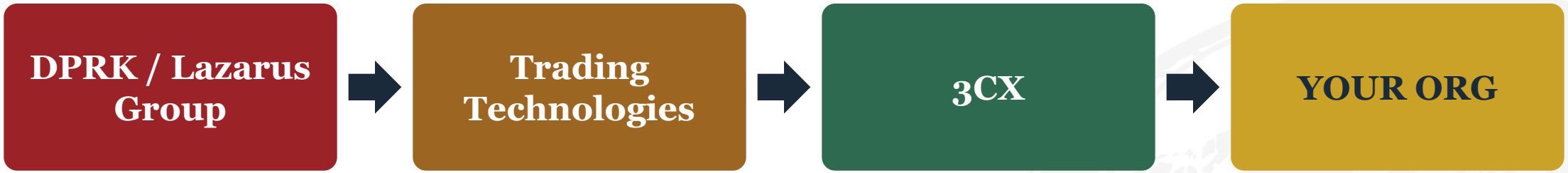
600,000 enterprise customers
12 million daily users

BMW · Honda · IKEA · Holiday Inn · UK National Health Service

Assessed. Contracted. Reviewed. Exactly like the vendors on your register.

GLOBAL CONFERENCE 2026
FROM CHAOS TO COMMAND:
RISK LEADERSHIP IN INDUSTRY 6.0

How It Reached You



No contract. No formal relationship. Trading Technologies disputed they were ever a 3CX supplier.

They were right. That's the problem.

Mandiant: the first recorded cascading supply chain compromise.

March 31, 2026

Three years later.

Axios

JavaScript library that helps software talk to the internet

100,000,000+

downloads per week

One maintainer's account compromised

⬇

Three hours of poisoned updates

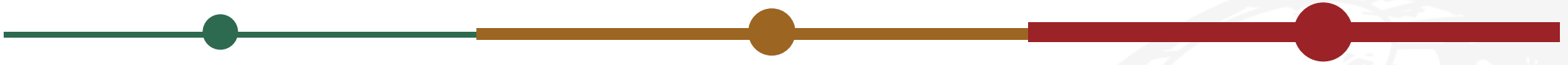
⬇

Every build system that pulled during that window

Timed for APAC business hours.

Attributed to the same actor family behind 3CX.

They Didn't Stop. They Industrialised.



2023

3CX

One vendor. 600,000 customers.
First of its kind.

November 2025

South Korean financial sector

Qilin ransomware. 2TB of banking data.
Coordinated across institutions.

March 2026

Axios

100M weekly downloads.
Three-hour window.

Same method. Three years. From a first-of-its-kind event to a repeatable technique.

They're not getting more sophisticated. They're getting better at finding the connections nobody is watching.

IERP®
Institute of Enterprise Risk Practitioners

July 19, 2024

No attacker. No breach. No malware.

A vendor pushed a routine content update.

8.5M	$5.4B	5,078	$1.94B
Windows devices	direct losses, Fortune 500	flights cancelled worldwide	healthcare sector losses

Most of the organizations that stopped had never purchased CrowdStrike.

Sources: Microsoft (8.5M devices); Parametrix (Fortune 500 and healthcare losses); Bitsight (flight cancellations)

IERP®
Institute of Enterprise Risk Practitioners

14 October 2023 - Singapore

Again: no attacker.

A contractor → **Equinix** → **DBS · POSB · Citibank** → **A customer at an ATM**

Closed the wrong valves during a planned upgrade

Chilled water system fails. Temperatures rise.

Shared data centre. Backup failed on a network misconfiguration.

Saturday afternoon. Cant get any money

12+ hours

Outage duration

810,000

Failed login attempts

2.5 million

Payment and ATM transactions that could not complete

MAS: “We do not have oversight of data centres.”

Oversight follows the contract. The failure didn’t.

THE PATTERN

A vendor you assessed. **(3CX)**

A library you never chose. **(Axios)**

A product you never bought. **(CrowdStrike)**

A provider you'd never heard of. **(Singapore)**

Four different mechanisms. One identical outcome.

Your program was built to assess who you have a contract with.

Not one of these four arrived through a contract.

You Couldn't Have Known

HIDDEN BY DESIGN

- Vendor source code is proprietary IP
- Software bills of materials are rarely shared commercially
- Sub-processor and dependency disclosures are legally minimal
- Trade secrets law protects what's underneath the product you bought

HIDDEN BY SCALE

- 900+ components per application
- Multiply by every vendor in your register
- The dependency chain is longer than any team can reasonably audit
- And it gets longer every time your vendor ships an update

You didn't miss something.

The information wasn't available to you.

WHY IT STOPS THERE

Third-party risk management follows contracts.

That's not a flaw.

The contract gives you the right to ask.

The contract gives you the right to audit.

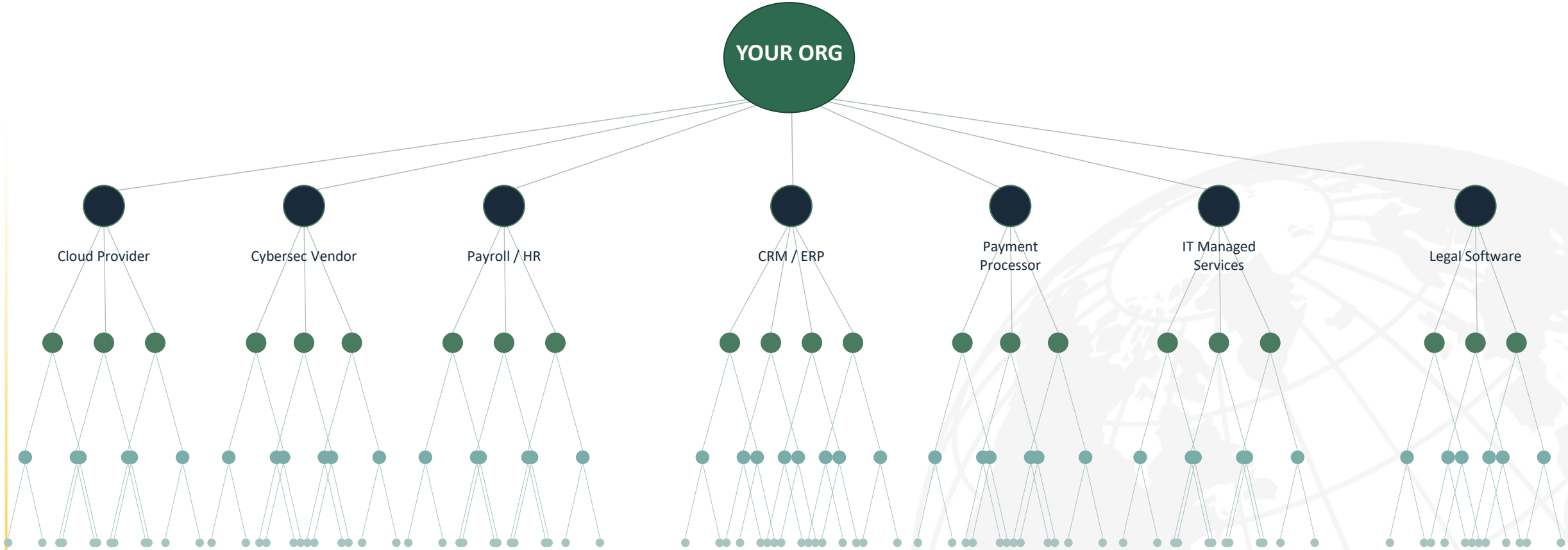
The contract gives you someone to call.

Your fourth party has no contract with you.

No right to ask. No right to audit. Nobody to call.

They are invisible to a process organised around contracts.

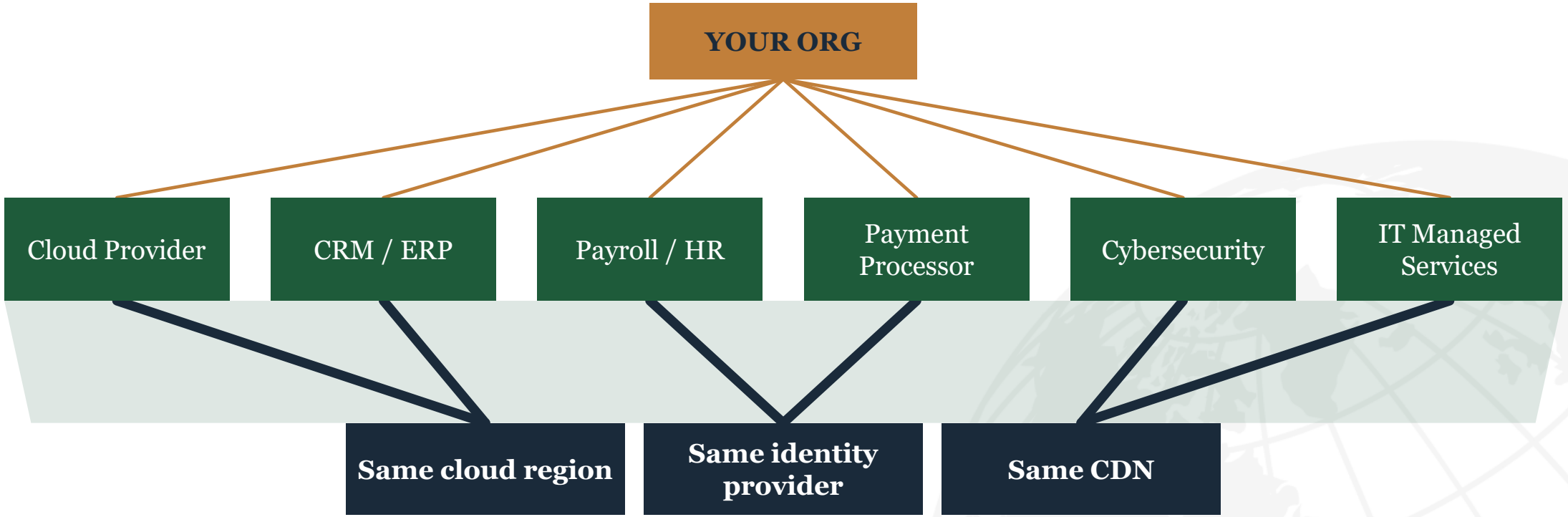
Your Vendor Didn't Know Either



This is not a supply chain. It's a living ecosystem.

Nobody has full visibility into it.

AND THEN IT CONVERGES



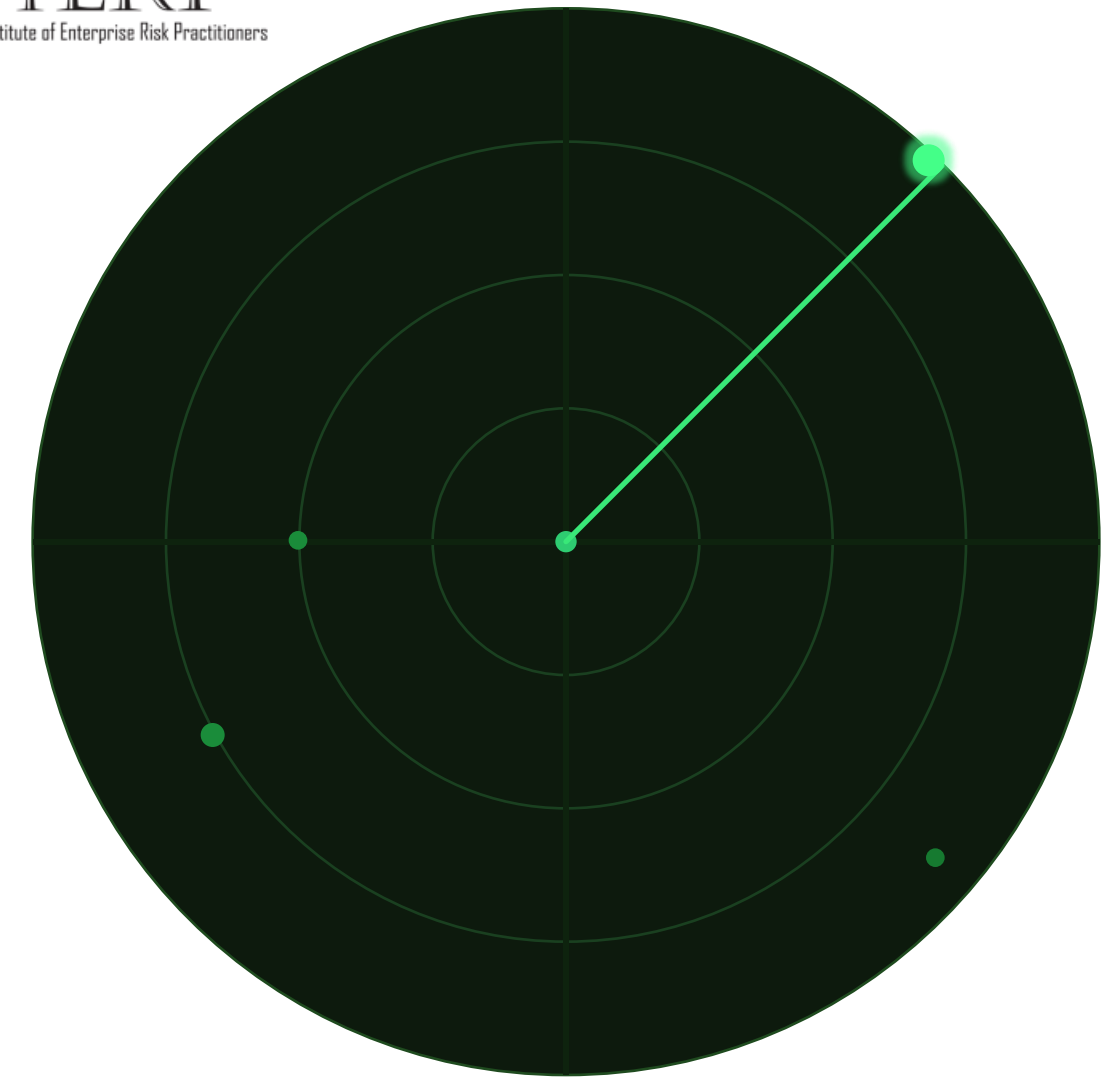
You diversified at tier one.

You re-concentrated at tier four - and nothing on your register shows it.

So what do you actually do?

Four things. None of them require a bigger budget.

IERP®
Institute of Enterprise Risk Practitioners



Which five vendors would stop your operations tonight if they went dark?

Not slow you down. Stop you.

Those five get a different level of attention.
The other thirty-five get the register.

You can't track everything in the water. ***Track what can sink you.***

GLOBAL CONFERENCE 2026
FROM CHAOS TO COMMAND:
RISK LEADERSHIP IN INDUSTRY 6.0

IERP®
Institute of Enterprise Risk Practitioners

THE QUESTIONS NOBODY ASKS

At the next renewal.

01 Sub-processor disclosure

Who else touches this, and tell us when that list changes.

02 Software bill of materials

A list of ingredients for the product we're buying.

03 Right to audit

And the right to extend it to your critical suppliers.

04 Notification of material dependency change

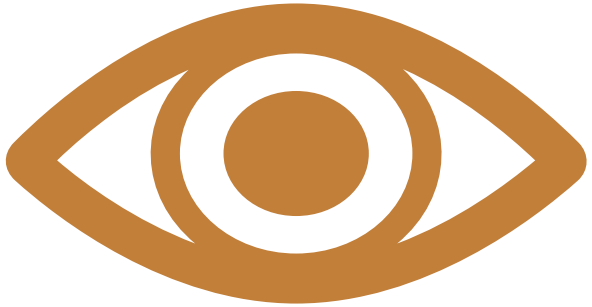
If you move cloud providers, we hear about it before it happens.

Most contracts don't include these. Most organizations never ask.

The next renewal is the opportunity.

IERP®
Institute of Enterprise Risk Practitioners

LOOK INWARD



If your most critical vendor disappeared tonight - what's your spillway?

DAM: spillway sits unused until water levels get critical. Then it's the only thing that matters.

AIRCRAFT: backup power collects dust for the entire service life of the plane. Until it doesn't.

Redundancy feels wasteful. Until it's the only thing standing between an incident and a catastrophe.

BUT DID YOU TEST IT?

An untested failover is not a control.

It's a hypothesis.

DBS had a backup data centre.

Budget approved. Regulator watching. Redundancy in place.

It failed on a network misconfiguration.

The plan existed. Nobody had opened the valve.

The Decision Only You Can Make

The organisations best at this didn't get there because they had better tools.

They got there because **someone internally drew a line and held it.**

Governments and critical infrastructure operators are the best in the world at third party risk - because they are genuinely willing to **say no**.

The dependency chain is long. You will never see all of it.

But you **can** know your critical path, draw your own lines, and stop waiting for a vendor to tell you what your risk tolerance should be.

That's where this starts

- NOF Consulting - reeces@nofconsulting.com

IERP®
Institute of Enterprise Risk Practitioners

GLOBAL CONFERENCE 2026

FROM CHAOS TO COMMAND:
RISK LEADERSHIP IN INDUSTRY 6.0

THANK YOU

SCAN THE QR CODE
TO KNOW MORE ABOUT US!

enquiry@insterp.com
www.insterp.com