# When One Data Centre — Idles 21 Banks

The Avaloq outage was small, brief and not a cyberattack. That's the warning.

Third-party concentration · Cloud · BCP & testing · Governed AI

**Anwarul Hasan (MBA, PhD)**

Founder & CEO · Risk Vizon LLC · Zurich, Switzerland

25+ years · UBS · KPMG · Swiss Re | anwarul.hasan@riskvizon.com

**21**
banks idled
by one data-centre fault

**63%**
of cloud
held by three providers

**$5.4B**
Fortune 500 loss
from one 2024 update

**20%**
of outages
now cost over $1M

finews.com — F. Schwab (2 Jul 2026); BCBS d516; Synergy; Parametrix; Uptime; MS Amlin (2026).

**KEY TAKEAWAYS**

- Concentration, not malice, is the systemic risk
- Map dependencies; set a tolerance for disruption
- Test third-party failure before it tests you

# When One Data Centre — Idles 21 Banks

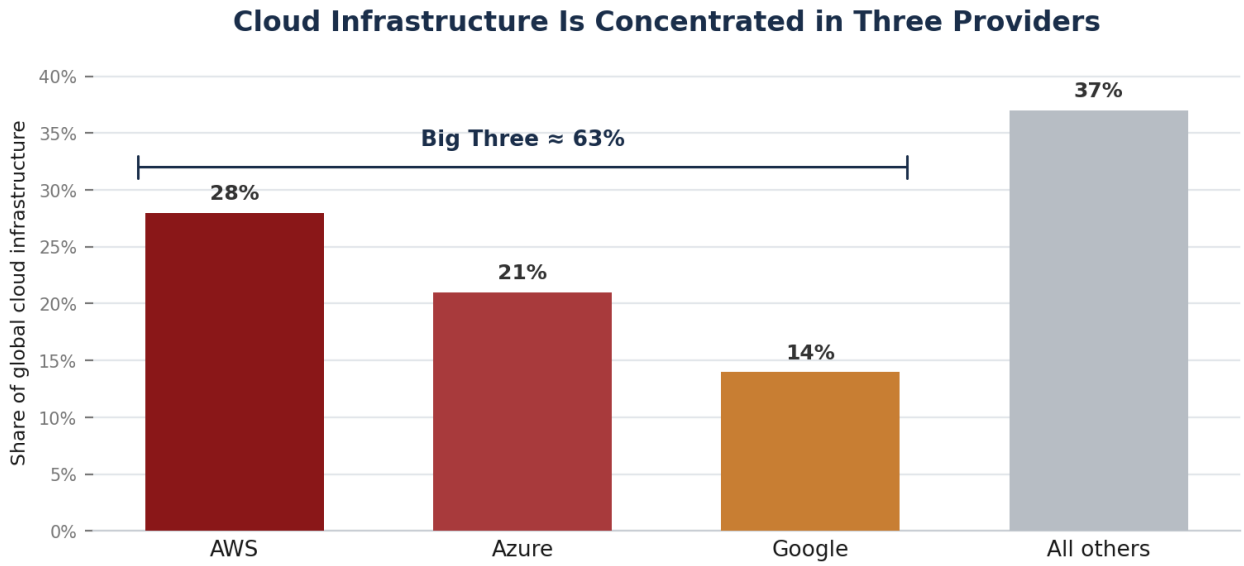
## The Avaloq outage was small, brief and not a cyberattack. That's the warning.

**By Anwarul Hasan (MBA, PhD)**
Founder & CEO, Risk Vizon LLC · Zurich · July 2026

On the afternoon of Wednesday **1 July 2026**, a hardware fault at a third-party data centre took the Avaloq software-as-a-service platform offline. **Twenty-one banks** lost their trading systems and reverted to placing orders with brokers by phone — "like thirty years ago," one affected bank told finews.com (F. Schwab, 2 July 2026). Service was largely restored by the next morning. There was no ransomware, no nation-state, no zero-day — just ordinary kit failing at one supplier. And that is exactly why it matters: a single, mundane fault idled critical operations at twenty-one institutions at once. Avaloq alone powers over **CHF 4 trillion** in client assets for **170+ financial institutions**. This is the shape of operational risk in a cloud-and-platform world — and resilience is no longer something a bank owns alone.

## Resilience You No Longer Own

The Avaloq event is a symptom of a decade-long shift: the critical operations of banks now run on infrastructure owned by a handful of providers. Three firms — AWS, Azure and Google Cloud — hold roughly **63%** of the global cloud infrastructure market. The European Central Bank has found that more than **30% of significant banks' outsourcing budgets** concentrate on just **ten providers**. Diversification is narrowing exactly as dependence deepens.




*Global cloud infrastructure market share, Q1 2026. Source: Synergy Research Group. The three largest providers together hold about 63% of the market.*

### Concentration has two faces

- **Market concentration** — a few providers behind everyone, as in public cloud.
- **Lock-in** — no practical substitute, as with a core-banking platform. A shared SaaS deployment quietly pools dozens of banks onto the same infrastructure. That is how one data-centre fault

reached 21 of them.

> *"Twenty-one banks did not each suffer their own incident. They shared one. Concentration turns a supplier's problem into a many-firm event."*

## The Loss Is Measured in Billions

Third-party outages are not a nuisance line item. The July 2024 CrowdStrike incident — one faulty security-software update — crashed some **8.5 million** Windows devices and cost the Fortune 500 about **$5.4 billion** in direct losses (Parametrix), of which banking bore roughly **$1.15 billion**. Insured losses were only **$0.3–1.5 billion** — most of it fell straight to the bottom line. And the trend is worsening: the Uptime Institute reports that **20% of outages now cost more than $1 million**, with third parties causing a rising share of major downtime. Recent history makes the frequency plain:

| Year | Event | Root cause | Reach / impact |
|---|---|---|---|
| **2021** | Fastly CDN outage | Config bug | Global sites down ~1 hour |
| **2021** | AWS US-EAST-1 | Network failure | Streaming, retail, deliveries offline for hours |
| **2024** | CrowdStrike update | Faulty sensor update | ~8.5m devices; ~$5.4bn Fortune 500 |
| **2026** | Avaloq SaaS | Data-centre hardware fault | 21 banks; manual dealing; ~half a day |

*Illustrative. Sources: press reporting; Cloud Security Alliance; Uptime Institute; finews.com (F. Schwab, 2 July 2026).*

## The Next Concentration Is Physical

Concentration is not only about market share — it is increasingly about geography. The same AI boom that is pushing banks deeper into cloud and machine-learning services is building out enormous data-centre capacity, and much of it is going up in the wrong places. A June 2026 analysis by Lloyd's specialist insurer **MS Amlin** found that **56% of 670 U.S. data-centre projects** under construction or planned sit in areas of **high natural-disaster risk** — exposed to hurricanes, severe convective storms, earthquakes and winter storms — representing **nearly $800 billion** of investment.

These are the very facilities that will host the cloud and AI workloads on which critical operations increasingly depend. An ordinary hardware fault idled 21 banks for half a day; a hurricane, seismic event or grid failure striking a concentrated data-centre hub is a different order of magnitude — and it would hit power networks and business continuity at the same time.

> *"As AI investment accelerates, insurers must adopt more advanced ways to manage aggregation risk." — Martin Burke, Chief Underwriting Officer, MS Amlin*

MS Amlin cautions that this accumulation, left unmanaged, could even **restrict the deployment of capital and the roll-out of AI infrastructure**. When the insurers of last resort worry about the physical concentration beneath the cloud, boards should treat **data-centre location and natural-hazard exposure** as a first-class third-party resilience question — not an IT footnote.

## What BCBS Already Requires

Supervisors saw this coming. The Basel Committee's 2021 *Principles for Operational Resilience* (d516) define resilience as the ability to **deliver critical operations through disruption**, tell banks to assume disruptions *will* happen, and require an explicit **tolerance for disruption**. Two of its seven principles speak straight to the Avaloq case:

- **Business continuity planning & testing (Principle 3)** — plans *and* exercises under severe-but-plausible scenarios, including third-party failure.
- **Third-party dependency management (Principle 5)** — assess substitutability, hold exit strategies (including in-sourcing), and map the dependencies behind every critical operation.

The standard exists. The gap, for most institutions, is in mapping the dependencies, setting the tolerance, and actually testing against a provider going dark.

## GRIP: Govern the Dependency You Can't Eliminate

No bank will de-risk by leaving the cloud; the job is to govern a dependency it cannot remove. That is what we built **GRIP — the Governance & Risk Intelligence Platform** to do, running the full d516 loop on one model of the business.

- **Map dependencies to critical operations** — including fourth parties — so shared-platform and cloud-region concentration is visible, not buried in procurement.
- **Set and monitor a tolerance for disruption** at the critical-operations level, with breaches routed to a body that can act.
- **Test severe-but-plausible third-party failure** — knock out a critical provider in a live model and quantify the loss, recovery time and substitution gap *before* the outage.
- **Quantify and govern concentration** with loss-exceedance analytics and governed, explainable AI that surfaces hidden overlaps and drafts exit playbooks.
- **See physical & geographic concentration** — flag where critical providers and their data centres cluster in natural-hazard zones, so location and climate exposure become a governed resilience input, not an IT footnote.

The Avaloq outage cost little because it was brief. The next one may not be. As critical operations concentrate onto a few providers, the difference between a footnote and a headline is whether you mapped the dependency, set a tolerance, tested the failure, and priced the loss in advance.

> *"You can outsource the service. You cannot outsource the accountability — or the consequences of an outage you never tested for."*

I would welcome your perspective — connect with me on LinkedIn or reach out at anwarul.hasan@riskvizon.com.

**Read the complete White Paper:**

***"Concentrated by Design — Third-Party Dependency & Operational Resilience"***

Available at: **www.riskvizon.com**

#OperationalResilience #ThirdPartyRisk #BusinessContinuity #BCBS #DORA #ConcentrationRisk #CloudRisk #AI #DataCentres #ClimateRisk #BoardGovernance #CRO #FINMA #GRIP #RiskVizon

**ABOUT THE AUTHOR**

**Anwarul Hasan (MBA, PhD)** is the Founder and CEO of Risk Vizon LLC, Zurich. With 25+ years at UBS, KPMG and Swiss Re, he is the architect of **GRIP — the Governance & Risk Intelligence Platform**, designed to empower

boards, regulators and executives to govern, monitor and steer enterprise risks in real time.

anwarul.hasan@riskvizon.com · www.riskvizon.com | © 2026 Risk Vizon LLC