



FREE GUIDE

Diversity and resilience.

You paid for a second route to stay online. Here's how to be sure it'll actually **save you** when the first one's cut.

SICOM CONNECTIVITY SICOM.UK FREE GUIDE

When the connection's down, **what stops?**

So many services are hosted in the cloud now that losing connectivity doesn't just cost you the internet and email. It can take down everything you run a business on:

• Telephone system

• Finance & accounting

• Project management

• Teams & Zoom

• Data storage & backup

• CRM systems

• Service & fault tracking

• Sales meetings

Staff can't work, can't talk to customers except on a mobile, miss meetings, can't handle faults. So diverse, resilient connectivity matters. But what do those two words actually mean? There are four things to get right.

1. Physical pathway diversity

Two physically separate routes (5m apart, minimum) so one event can't cut both. The infamous JCB through the cable, a lorry crushing a duct, copper thieves. And it's not just the street — inside the building too: do the fibres use separate risers, different paths to the comms room?

Diversity all the way to the core

2 · Different PoPs or nodes

Your premises connect to the carrier's local Point-of-Presence. If that PoP has a power outage or fire, both circuits could go. Know which PoPs you route to — and whether they have dual fibre and generators, or just one link and 20 minutes of battery.

3 · ISP core nodes

The ISP's network centres on core nodes connecting to Tier-1 global providers. It should have at least two, in separate buildings — ideally separate cities — each able to carry the full load if the other fails.

4 · Resilient equipment

No good having separate paths, PoPs and core nodes if it all lands on one router in your comms room. Two routers, each with dual power supplies (the part most likely to fail), with separately-routed cables to your switches.

The principle

Diversity has to hold end-to-end: the street, the building risers, the PoPs, the carrier networks, the core nodes, and the kit in your rack. A single shared link anywhere breaks it.

— WHAT THE PERCENTAGES ACTUALLY MEAN

"99%" sounds great. It isn't.

The architecture above should give you 99.99% availability. But read the small print on availability figures — here's the downtime each one really means over a five-year contract.

AVAILABILITY	DOWNTIME	WHAT IT MEANS
99%	438 hrs / 5yr	18 days down over the contract. Sounds fine on paper — it isn't.
99.9%	43.8 hrs / 5yr	If a typical fault takes 6 hours to clear, that's still more than a day's outage a year.
99.99%	52.56 min / 5yr	In practice, maybe one incident in five years. This is what we aim for — but there are no guarantees, only SLAs.

Averages don't spread evenly. You might get two outages in a month and nothing for two years. How much does a day's downtime cost your business — and what's the reputational hit of two close together?

Even then — there's the ISP.

A common-mode failure

For all the diversity built in, if the ISP hits an issue common to all its kit, you can still go down. It's rare — but it happens. We've seen a software upgrade take down every router across an ISP at once, and two separate carriers hit by unrelated faults 30 minutes apart. Stuff happens. Not often.

"Can't I just use two ISPs?"

Yes — but not easily. Two ISPs means two IP ranges, and traffic won't know which to use. You'd need your own Provider-Independent (PI) IP space and Border Gateway Protocol (BGP) to auto-reroute on an outage. That's expert-level networking.

If you want PI space and BGP, we can bring in specialists to set it up.

The questions that expose a weak ISP

1 Do you have route maps for the services?

- Essential on high-bandwidth links — different carriers may own fibres in the **same cable**.
- For diverse access via Openreach, both lines must be ordered with **Resilience Option 2 (RO2)** — otherwise both run in the same cable to the same exchange.
- Even Openreach + an alt-net can end up in two ducts side-by-side. Better, but not truly diverse.

2 Show me the network diagram.

- PoPs, core nodes, Tier-1 IP transit providers and capacities. A good ISP has this to hand.
- Do you peer directly with my hosted voice provider, or with Microsoft / others I send heavy traffic to?

3 Tell me about the PoPs and the carrier network.

- Where are they? Resilient power, battery, generators? If battery only, how long?
- Two or more fibre links upstream? Will traffic auto-reroute on a fault? (Ethernet/MPLS self-heal; a fixed-path wavelength won't.)

FINAL WORDS

Be pragmatic — but **ask the questions.**

- Work out the lost business if you're down for a day. The number's usually bigger than you think.
- Be pragmatic about cost: if both circuits share one locked, managed riser, how much risk is that really?
- If both leave the building in one duct then split left and right — would you not notice the JCB in your car park?
- With 99.99% you'll probably still see one outage in five years. Have a Disaster Recovery Plan, even a simple one, and know when to invoke it.

Proper diversity costs a little more in time and rentals. But the most expensive circuit in the world is **the diverse circuit that isn't diverse.**

TALK TO US

We select the ISP partners and check the diversity — **at no extra cost to you.**

[sicom.uk](https://www.sicom.uk)

Richard · 07803 737321