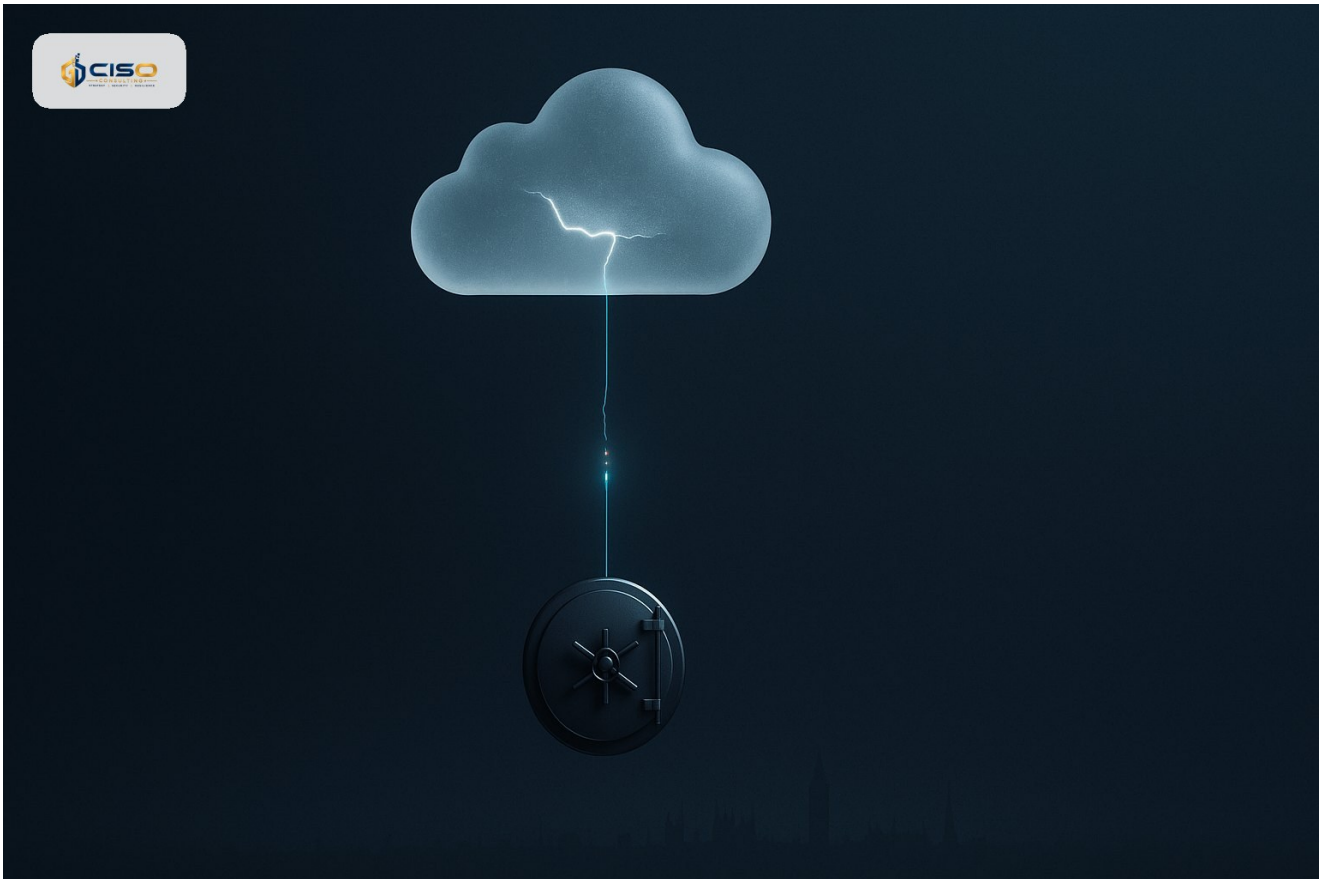


Revolut outage tied to Google Cloud London incident; services restored



Revolut suffered a worldwide outage affecting 28 services, which it linked to a Google Cloud incident. The company says services are restored and that customer money and data stayed safe.

- Revolut's status page listed 28 affected services, including sign-ins, card payments, transfers, currency exchange, stock trading and live chat.
- Reuters linked the disruption to a 'power event' at Google Cloud's europe-west2 data center in London.
- Revolut later confirmed the cause was a Google Cloud outage and said services were restored.
- The company states customer money and data remained safe throughout.
- Revolut served more than 80 million customers across 160+ countries and regions.

Fintech company Revolut experienced a large outage that disrupted most of its services worldwide. Thousands of users reported problems with the app, mobile banking and transfers between accounts on the Downdetector tracking platform.

What happened

Revolut's status page flagged 28 services as partially unavailable, including sign-ins, card payments, transfers, currency exchange, stock trading and live support chat. According to Reuters, the disruption was reportedly connected to problems at Google Cloud's europe-west2 data center in London following a 'power event'.

Revolut first said the cause was still being investigated, then linked the outage to the Google Cloud incident. It reports that all services are now restored and that customer money and data were safe throughout.

Why it matters

The incident shows how a fault at a single cloud provider location can interrupt customer-facing financial services across many countries. It was an availability event; the source does not describe an attack. Separately, the source notes that Revolut disclosed a data breach last month, which is unrelated to this outage as reported.

For Saudi institutions that rely on cloud-hosted platforms or third-party fintech services, this is a practical prompt to review how dependent critical services are on one provider or region, and whether recovery plans have been tested against such a failure.

What to do now

1. Map which critical services depend on a single cloud provider, region or third-party fintech.
2. Check that business continuity and disaster recovery plans cover loss of a cloud region, and test them.
3. Confirm that contracts and SLAs with cloud and fintech providers define incident notification and recovery commitments.
4. Prepare customer communication templates for outages, stating clearly whether money and data are affected.
5. Review concentration risk in third-party risk assessments and record any accepted dependencies.