Preptorum

CLOUD FAILURE SCENARIOS

EXAMPLE PACK: TORUMPREP INC
DOCUMENT 03
FICTIONAL · NOT A REAL COMPANY

TorumPrep Inc · Continuity pack document 03

> **FICTIONAL EXAMPLE CONTENT – TorumPrep Inc is not a real company.** The scenarios are generic examples. AWS, Azure and Microsoft are named only as platforms. A real firm replaces the details with its own architecture and plans.

How to use this document: find the scenario that fits, then work through the five headings in order: signs, first actions, what still works, workarounds, and when to stand down. If trading is affected in any scenario, run the first-hour runbook (document 02) at the same time.

SCENARIO A: AWS REGION OUTAGE

TorumPrep runs its trading and risk platforms in a primary AWS region, with a standby copy in a second region.

Signs

- Trading screens freeze, orders time out, or prices stop updating.
- Technology alerts about the primary region; the AWS Health Dashboard reports a problem.
- Corporate tools on Azure and Microsoft 365 still work.

First actions

1. Start document 02. Incident Lead sets trading to Restricted.
2. Technology On-Call Lead confirms whether the fault is AWS-wide, regional, or ours.
3. If regional and not fixed within the agreed decision window (example: 20 minutes), the Incident Lead decides whether to fail over to the second region.
4. Risk opens the offline position snapshot from the drive.

What still works

- Email, Teams and the intranet (they run on Microsoft).
- Voice recording and market data in each office (on premises).
- Broker, clearing and exchange portals.

Workarounds

- Hedge by voice on recorded lines (document 02, section 4).
- Coordinate on a Teams bridge; keep the out-of-band bridge ready in case.
- After failover, check that the standby region holds the latest trades before reopening.

Stand down when the platform runs normally in either region, positions reconcile, and any failover has been reviewed. Plan a controlled move back to the primary region at a quiet time, not in the middle of the trading day.

SCENARIO B: AZURE OR MICROSOFT 365 OUTAGE

Teams, Outlook and the intranet are down, and staff may not be able to sign in through Microsoft Entra ID.

Why this matters now: on 12 November 2026 a widespread Microsoft 365 outage disrupted Outlook, Teams and other services for many organisations for about a day (dated sources in SOURCES.md). Outages like this are rare, but when they happen, the plan needs to be somewhere other than the system that has stopped.

Signs

- Outlook will not connect; Teams shows errors; SharePoint and OneDrive will not load.
- Sign-in prompts fail or loop.
- The Microsoft 365 or Azure status pages, or news reports, describe a wider outage.

First actions

1. Incident Lead opens the out-of-band bridge (document 04, section 4) and sends the call-tree alert by SMS.
2. Technology On-Call Lead checks whether trading systems depend on Entra sign-in. If traders cannot sign in, start document 02.

3. Do not sign out of any working session; it may not come back.
4. Switch to the plans on the Preptorum drive. Do not wait for the intranet.

What still works

- Trading and risk platforms on AWS, if they do not depend on Entra sign-in for active sessions.
- Recorded voice lines and personal mobiles.
- Break-glass accounts held offline, for named technology roles only.

Workarounds

- Use the out-of-band bridge and SMS cascade instead of Teams.
- Use the alternate email domain or the client portal for client messages.
- Keep a paper log; copy it into the normal systems later.
- Use the offline contact sheets on the drive; do not rely on the address book.

Stand down when sign-in, email and Teams work across both offices, delayed email has been checked for anything urgent, and decisions made off-system have been written into the normal records.

SCENARIO C: BOTH CLOUDS LOST AT ONCE

Both AWS and Azure services are unavailable or cannot be trusted, for example because of a shared network fault, a large internet disruption, or a cyber event.

Signs

- Trading, email, Teams and the intranet are all down together.
- Office internet links may also be failing.

First actions

1. Incident Lead sets trading to **Halted**, apart from essential voice hedges.
2. Start document 02 and the out-of-band bridge.
3. Assume the outage may last hours. Plan for the rest of the trading day and the handover.
4. Check whether the cause could be a cyber event. If there is any sign of it, follow Scenario D too.

What still works

- Preptorum drives: this pack, the offline position snapshots and contact sheets.
- Desk phones on recorded lines (if the office voice system has its own links) and personal mobiles.
- Broker, clearing and exchange contacts by phone.

Workarounds

- Run the book from the offline position view and voice hedges only.
- Use personal mobiles on the SMS cascade; agree a fixed update time each hour.
- Move key people to the office or recovery site with the best working connections.

Stand down when both platforms are confirmed sound, trading has been reopened in steps, and every manual trade has been booked and checked.

SCENARIO D: CYBER OR RANSOMWARE EVENT

Systems behave strangely, files are encrypted, or attackers may be inside the network.

Signs

- Files that will not open, ransom notes, or unusual account activity.
- Alerts from monitoring tools or a warning from a provider or partner.

First actions

1. Report it at once to the Technology On-Call Lead and the cyber response lead by phone.
2. Do not switch off, wipe or reconnect affected machines unless the cyber response lead tells you to.
3. Incident Lead sets trading to Restricted or Halted and starts document 02.
4. Move all incident talk to the out-of-band bridge. Assume company email and Teams may be read by the attacker.
5. Compliance Duty Officer starts the notification checklist in our own procedures; involve legal counsel.

What still works

- The Preptorum drive and the offline position snapshots that risk staff copied onto it, because the drive is not connected to the network. Treat any snapshot made after the suspected start time with care.
- Outside statements from brokers, clearing houses and custodians.
- Recorded voice lines, if the voice system is not affected.

Workarounds

- Confirm every instruction by calling back on a known number from the contact sheet, never a number given in an email or message.
- Pause payments and changes to standing instructions unless confirmed by phone and approved by two people.
- Use clean, pre-prepared laptops for the incident team if your plan includes them.

Stand down when the cyber response lead confirms systems are clean and restored from trusted backups, credentials have been reset, and regulators, clients and law enforcement have been told what they need to know under our procedures.