Preptorum

FAILURE SCENARIOS

EXAMPLE PACK: GRIDTORUM PLC
DOCUMENT 03
FICTIONAL · NOT A REAL COMPANY

GridTorum PLC · Continuity pack document 03

> **FICTIONAL EXAMPLE CONTENT – GridTorum PLC is not a real company.** The scenarios are generic examples. AWS, Azure and Microsoft are named only as platforms. OT, safe-state and black start guidance is deliberately general. A real company follows its own approved plans, safety rules and technical procedures.

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 fault and repair systems are affected in any scenario, run the first-hour runbook (document 02) at the same time.

SCENARIO A: AWS REGION OUTAGE

GridTorum runs analytics, forecasting, customer portals and parts of outage management in a primary AWS region, with a standby in a second region.

Signs

- Outage management screens stop loading or show stale data; the customer fault portal fails.
- Forecasting dashboards stop updating.
- Technology alerts about the primary region; the AWS Health Dashboard reports a problem.

First actions

1. Start document 02 if fault intake or outage management is affected.
2. IT 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: 30 minutes), the Incident Lead decides whether to fail over to the second region.
4. Control engineers use on-premises forecasts and the last saved forecast on the drive.

What still works

- SCADA, the EMS and OT networks (on premises).
- Email, Teams and the intranet (on Microsoft).
- Operational telecoms and radio.

Workarounds

- Open fallback fault intake for customers and DNOs (document 02, section 4).
- Track faults on the paper log and board.
- After failover, check the standby holds the latest fault records before switching back to it.

Stand down when outage management and the portal run normally in either region, records made by hand have been entered, and any failover has been reviewed.

SCENARIO B: AZURE OR MICROSOFT 365 OUTAGE

Teams, Outlook and the intranet are down, and staff may not be able to sign in with company accounts. Work management and field dispatch may depend on the same sign-in.

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.
- Field crews cannot open job packs on their tablets.
- 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. IT On-Call Lead checks which fault and repair systems depend on company sign-in. If any do, start document 02.
3. Do not sign out of any working session; it may not come back.
4. Switch to the plans, diagrams and contact sheets on the Preptorum drive.

What still works

- SCADA, the EMS and OT networks, which do not use corporate sign-in.
- Control-room phones, operational radio and satellite phones.
- Offline break-glass accounts held for named technology roles only.

Workarounds

- Dispatch crews by radio and phone; issue job details read aloud and logged.
- Use paper job sheets and paper permits from the site packs.
- Use the out-of-band bridge and SMS cascade instead of Teams.

Stand down when sign-in, email and Teams work across all sites, 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

- Outage management, work management, dispatch, the customer portal, email and Teams are all down together.
- Corporate internet links may also be failing.

First actions

1. Start document 02 and set the operating mode to at least **Degraded**.
2. Open the out-of-band bridge and fallback fault intake.
3. Assume the outage may last hours. Plan for shift changes and staff welfare.
4. Check whether the cause could be a cyber event. If there is any sign of it, follow Scenario E too.

What still works

- SCADA, the EMS and OT networks, if they are fully separated from the clouds.
- Preptorum drives: this pack, the network state snapshot, diagrams and contact sheets.
- Control-room phones, radio and satellite phones.

Workarounds

- Run fault and repair work entirely on paper: log, board, job sheets and permits.
- Post staff at key sites and keep a fixed reporting schedule.
- Move key people to the control room or backup site with the best working links.

Stand down when both platforms are confirmed sound, systems have been brought back in steps, and every manual record has been entered and checked.

SCENARIO D: LOSS OF AN ON-PREMISES DATA CENTRE

One of GridTorum's two data centres is lost through fire, flood, power failure or a building problem. Some control and fault systems run there.

Signs

- Systems hosted in one data centre stop at the same moment.
- Alarms from the building, its power or cooling.
- Some SCADA or EMS displays fail over, freeze or show stale data.

First actions

1. Make sure everyone at the site is safe and accounted for. Follow the site emergency plan first.
2. Incident Lead checks whether the control room still has trusted SCADA and EMS. If not, set the mode to **Blind** and start document 02.

3. OT On-Call Lead confirms failover to the second data centre for control systems, and IT On-Call Lead for business systems.
4. If control from the PCR depends on the lost site, prepare to transfer control to the BCR (document 04, section 3).

What still works

- The second data centre and the systems it hosts.
- The backup control room, if it does not depend on the lost site.
- Cloud services, email and Teams, if their links did not run through the lost site.

Workarounds

- Run from the second data centre and accept reduced resilience until the first is back.
- Use the network state snapshot and paper diagrams for anything the second site does not show.

Stand down when systems are running and checked at the second site, resilience has been restored or a plan agreed, and every manual record has been entered.

SCENARIO E: CYBER OR RANSOMWARE EVENT AFFECTING IT AND OT

Business systems behave strangely, files are encrypted, or attackers may be inside the IT or OT networks.

Signs

- Files that will not open, ransom notes, or unusual account activity.
- Unexpected commands, settings changes or alarms on OT systems.
- Alerts from monitoring tools or a warning from a provider, partner or government body.

First actions

1. Report it at once to the IT and OT On-Call Leads 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. On the cyber response lead's advice, and under the OT plan, **separate OT from IT** at the agreed boundary points.
4. Put affected OT systems into the **safe state set out in your OT procedures**. Where control systems cannot be trusted, prepare for manual operation at sites under the safety rules.
5. Start document 02. Move all incident talk to the out-of-band bridge; assume company email and Teams may be read by the attacker.
6. Government and Regulatory Liaison starts the notification checklist in our own procedures; involve legal counsel.

What still works

- The Preptorum drive, the network state snapshot and paper diagrams, because they are not connected to the network. Treat any snapshot made after the suspected start time with care.
- Staff at substations who can see and report plant directly.
- Radio and satellite phones.

Workarounds

- Confirm every instruction by calling back on a known number from the contact sheet, never one given in an email or message.
- Use clean, pre-prepared laptops for the incident team if your plan includes them.
- Run fault intake and dispatch on paper until systems are confirmed clean.

Stand down when the cyber response lead confirms IT and OT are clean and restored from trusted backups, credentials have been reset, OT has been reconnected step by step under the OT plan, and government, the regulator and law enforcement have been told what they need to know under our procedures.

SCENARIO F: WIDE-AREA POWER LOSS AFFECTING OUR OWN SITES

A large part of the network has lost power, including some of GridTorum's own offices, depots and sites. In the worst case this is a full or partial shutdown that needs **black start**: restoring the network from generators able to start without power from the grid.

Signs

- Large parts of the network de-energised at once; many alarms or none.
- Mains power lost at offices and depots; standby generators running.
- Public phone and mobile networks weakening as their own batteries run down.

First actions

1. Incident Lead declares the incident and sets the mode to **Blind** unless SCADA and the EMS are trusted.
2. Start the **black start plan** kept on this drive and in the control room. Follow it as written; do not improvise the restoration sequence.
3. Field Operations confirms standby power, fuel and batteries at control rooms, data centres and key substations, and reports the time each can last.
4. Partner Liaison opens contact with the generators named in the plan and with DNOs, using radio and satellite phones if needed.
5. Start the welfare plan for staff on long shifts.

What still works

- Sites with standby power and fuel, for as long as it lasts.
- Operational telecoms and radio with their own battery and generator back-up.
- Satellite phones and the Preptorum drive (keep drives and laptops charged from standby power).

Workarounds

- Rebuild the network in the steps set out in the black start plan, with each step confirmed before the next.
- Post staff at the sites named in the plan.
- Use fuel and battery reports to decide which sites need attention first.

Stand down when the network has been restored and is stable, our own sites are back on normal supplies, standby fuel has been replenished, and partners, government and the regulator have had a closing message.