Can we get back to work?

One critical service. One protected recovery path. Agree the test with its business owner and provider.

Business / critical service

Business owner / recovery lead

Maximum acceptable outage (time unit)

Maximum acceptable data/work loss (time unit)

Safe interim way of working while unavailable

IDENTIFY A USABLE RECOVERY COPY

Applications, data, equipment settings, and dependencies covered

Backup location / protected inventory reference

Recovery point: date, time, timezone

Retained versions / retention setting

Who can change, delete, or expire copies?

How are copies protected from compromised everyday access?

Protected restore-credential / key reference

Licenses / vendor tools / hardware / identities

Provider support / restore procedure reference

Who approves equipment settings / safe operation?

Rehearse. Verify. Assign.

Use an isolated test target. Never record actual secrets. Keep the existing viable copy during testing.

Test target, authorization, restore order, and how live actions are blocked

Work started: date/time + timezone

Data restored: date/time + timezone

Business use verified: date/time + timezone

Usable recovery point: date/time + timezone

Representative work verified / business and safe-operation approval reference

Elapsed time to usable service (target unit)

Usable-data age at test start (target unit)

Overall result

Not tested

Open gaps / next action / owner / due date

Test date / evidence reference

Next test / change that triggers an earlier test

Stop if the test could affect production, real transactions, or live equipment. A successful rehearsal covers this service under the tested conditions. After an intrusion, investigate other access and validate a trusted return to service.

Related guidance: CIS 11.1-11.4 (IG1); 11.5 sampled recovery testing (IG2/3). Choose an owned cadence for the service. NIST SP 1339: OT backup inventory, procedures, and recovery exercises; SP 1300: small-business risk management.

csrc.nist.gov/pubs/sp/1339/final