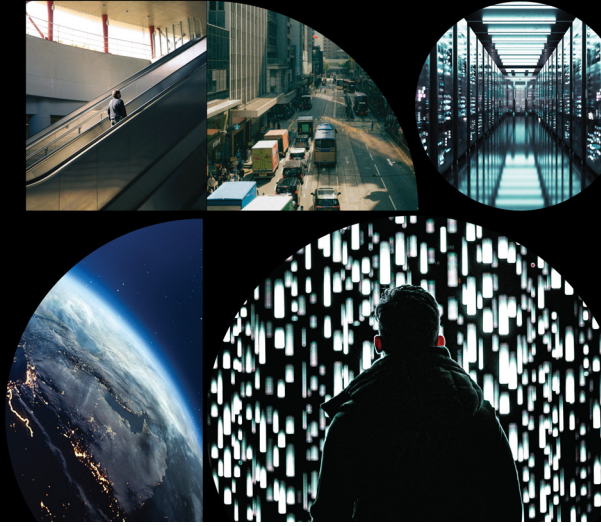
Commvault

# Resilience Review Checklist

A quick review of your critical workloads, recovery plans, and data protection policies to help identify gaps and strengthen your overall posture. Walk through each item with your team, check off what's confirmed, and flag anything that needs attention.

**Estimated time:** 20 minutes with your infrastructure team



| | Review Item | What to Look For |
|---|---|---|
| **Multi-Region Coverage** | | |
| ☐ | **Are all critical workloads backed up to a secondary region?** Cloud-native, on-prem, SaaS, and hybrid workloads. | Verify backup policies include cross-region replication for Tier 1 workloads. Identify any single-region dependencies. |
| ☐ | **Do backup copies exist outside your primary geography?** Consider both cloud regions and physical locations. | Confirm at least one copy resides in a separate geographic region from production. Review sovereignty requirements before moving data across borders. |
| ☐ | **Are replication schedules aligned with your recovery point objectives?** Frequency, lag time, and data currency. | Check that replication intervals match your documented recovery point objectives. Flag any gaps between policy and actual configuration. |
| **Air-Gapped & Isolated Protection** | | |
| ☐ | **Do you have immutable, air-gapped copies of critical data?** M365, identity systems, databases, enterprise workloads. | Verify isolated storage is enabled for your most sensitive workloads and that copies cannot be modified or deleted by compromised credentials. |
| ☐ | **Are identity systems (Active Directory, Entra ID, Okta) independently protected?** These are often the first target in a sophisticated attack. | Confirm identity infrastructure has its own backup and recovery path, separate from the systems it authenticates. |
| **Recovery Readiness** | | |
| ☐ | **Has your recovery plan been tested in the last 90 days?** Tabletop exercises, partial restores, or full disaster recovery tests. | If you haven't validated recovery in a clean, isolated environment recently, now is a good time. Document any assumptions that haven't been tested. |
| ☐ | **Can you rebuild a full environment in a secondary region?** Not just data – compute, networking, configurations. | Review whether your recovery plan covers full-stack restoration, not just file-level recovery. |
| ☐ | **Is your minimum viable recovery threshold defined?** Which systems must be online first, and in what order? | **Document your critical path:** what must recover in hours vs. days. Validate your sequencing is realistic and has been walked through with stakeholders. |

| | Review Item | What to Look For |
|---|---|---|
| **Threat Awareness** | | |
| ☐ | **Are you monitoring for elevated threat activity in your sector?** Geopolitical instability may correlate with increased cyber activity. | Review any threat intelligence feeds or advisories relevant to your industry and geography. |
| ☐ | **Have you reviewed access controls and privilege escalation paths?** Admin credentials, service accounts, API keys. | Audit privileged access. Validate that multi-factor authentication is enforced, dormant accounts are disabled, and service account credentials are rotated on schedule. |

## NEED SUPPORT?

If anything in this review surfaces a gap or a question, your CSM is here to help. We can walk through your configuration together, review your recovery posture, or connect you with our Cyber Ready Services team for a deeper assessment.

Reach out to talk to a Commvault expert at **www.commvault.com/contact-us**, or contact your CSM if you are an existing customer.