Kaseya

Microsoft cloud resilience checklist

8 proof points for end-to-end recovery readiness

Cyber resilience isn't defined by the backups you have. It's defined by your ability to recover cleanly, quickly and confidently when Microsoft data, identities, configurations or workloads are disrupted.

Use this checklist to assess whether your Microsoft environment can recover from ransomware, accidental deletion, tenant compromise, account takeover, outage, misconfiguration or failed recovery testing.

How to use this checklist

For each checkpoint, mark whether the control is ready, needs review, has a known gap or is unknown. The goal isn't to confirm that backups exist. It's to verify that recovery works under real-world incident conditions.

Quick readiness scorecard

Checkpoint	Ready	Needs review	Has a known gap	Unknown
Recovery is independent from Microsoft	☐	☐	☐	☐
Data, identities, configurations and workloads are protected	☐	☐	☐	☐
Recovery is tested before an incident	☐	☐	☐	☐
Backups are hardened against ransomware and compromise	☐	☐	☐	☐
Recovery options match business operations	☐	☐	☐	☐
Microsoft protection is visible in one place	☐	☐	☐	☐
Recovery readiness is continuously monitored	☐	☐	☐	☐
Coverage evolves with the Microsoft environment	☐	☐	☐	☐

The 8 Microsoft cloud resilience checkpoints

1 Keep recovery independent from Microsoft ☐

What to verify: Your recovery strategy for Microsoft 365, Azure and Entra ID includes backups stored independently of your production Microsoft environment that can be accessed without relying on the same Microsoft tenant or administrative controls.

Why it matters: Microsoft secures the cloud platform, but you're responsible for protecting and recovering your own data. Independent protection helps eliminate single-cloud risk and strengthens recovery readiness against ransomware, account compromise, misconfiguration or outage.

2 Protect more than files and email ☐

What to verify: Confirm protection for Microsoft 365 data, Entra ID objects, Azure workloads and other services that keep operations running.

Why it matters: Business continuity depends on more than restoring mailboxes and documents. Identity, access, policies and workload recovery can be just as critical during an incident.

3 Validate recovery before you need it

What to verify: Test restores regularly across critical Microsoft services and keep evidence of successful tests.

Why it matters: A backup is valuable only if it can be recovered. Routine testing helps ensure your Microsoft cloud is ready when the unexpected happens.

4 Harden backups against ransomware

What to verify: Your Microsoft cloud resilience strategy includes immutable backups, strong access controls (such as MFA and role-based permissions) and monitoring that alerts you to potential threats or unauthorized changes.

Why it matters: Attackers increasingly target backups and admin credentials. Resilience requires backups that cannot be encrypted, deleted or altered.

5 Recover the way the business operates

What to verify: Document recovery paths for everyday restores, full workload recovery and larger incident scenarios. Align each path with your RTO and RPO needs.

Why it matters: Some incidents require restoring a single file. Others require restoring entire workloads. Recovery plans should match the operational impact of each scenario.

6 Reduce Microsoft recovery complexity

What to verify: Make sure you can quickly see what is protected, what is failing, what changed and how to restore without jumping between disconnected tools.

Why it matters: Complexity slows response. Fragmented tools can create blind spots across Microsoft 365, Azure and Entra ID when time matters most.

7 Know your recovery readiness ☐

What to verify: Monitor backup health, failed jobs, policy drift, risky configurations, coverage gaps and restore-test results on an ongoing basis.

Why it matters: Recovery confidence should not be based on assumptions. Continuous visibility helps teams identify risk before an incident or audit exposes it.

8 Update coverage as Microsoft changes ☐

What to verify: Review resilience coverage when adding users, workloads, tenants, Azure services, security policies, compliance requirements or acquired environments.

Why it matters: Microsoft environments change constantly. A resilience plan completed last quarter may become incomplete as the environment evolves.

What good looks like

- Recovery does not depend on the Microsoft tenant being healthy.
- Critical data, identities, configurations and workloads are covered.
- Restore testing is routine, documented and tied to real scenarios.
- Backups are protected from ransomware and credential compromise.
- IT has clear visibility into coverage, health, risk and recoverability.

Next step

Use the gaps identified in this checklist to prioritize a Microsoft recovery readiness review. Focus first on areas where recovery depends on native Microsoft controls, untested backups, undocumented restore paths or incomplete workload coverage.

Need help strengthening your Microsoft Cloud resilience?

Our cyber resilience experts can help you evaluate your recovery strategy, identify potential gaps and build a roadmap for protecting Microsoft 365, Azure and Entra ID with confidence.

Schedule a Microsoft Cloud resilience assessment

Kaseya®