DOWNLOADABLE WORKSHEET · CLOUD BACKUP

The Backup-as-a-Service Evaluation *Worksheet*

A working document for IT leaders evaluating a backup-as-a-service (BaaS) provider — or stress-testing the one they already have. Built around one question: not whether you have backups, but whether you could actually recover.

How to use this worksheet

Work through the eight sections below with your prospective (or current) provider in the room, or alongside your internal documentation. Each question is scored on the same three-point scale. Be honest — the point of this exercise is to find the gaps before an incident does, not to make the program look good.

Scoring scale

Score	Meaning
0 — Absent	Capability does not exist, or no one can answer the question.
1 — Partial	Capability exists but is incomplete, manual, untested, or unverified.
2 — Proven	Capability is in place AND demonstrated with evidence (a report, a drill, a documented restore).

> The "proven" bar is deliberately high: A confident verbal "yes" is a 1, not a 2. A 2 requires an artifact — a recovery verification report, a restore-drill log, a screenshot of an enforced object-lock policy. If they can't show it, it isn't proven.

40 questions × 2 points = 80 points maximum. Tally at the end and use the scorecard to decide your next step.

S1 — Scope & Coverage Inventory

What data are we actually protecting — and what are we silently leaving out?

- [ ] 1. Are all physical and virtual servers in scope, with a documented inventory? (0 / 1 / 2)
- [ ] 2. Are employee endpoints (laptops/desktops) backed up, or are they assumed to hold no unique data? (0 / 1 / 2)
- [ ] 3. Is Microsoft 365 Exchange Online (mail) backed up independently of Microsoft's retention? (0 / 1 / 2)
- [ ] 4. Are SharePoint sites and document libraries backed up? (0 / 1 / 2)
- [ ] 5. Is OneDrive for Business backed up for every user? (0 / 1 / 2)
- [ ] 6. Is Microsoft Teams backed up across its spread (chat, files in SharePoint/OneDrive, channel structure)? (0 / 1 / 2)

- [ ] 7. Is Entra ID configuration (users, groups, conditional access, app registrations) captured? (0 / 1 / 2)
- [ ] 8. Are other business-critical SaaS apps (CRM, ERP, line-of-business) backed up, or is each one's protection confirmed by name? (0 / 1 / 2)

Section S1 subtotal _____ / 16

S2 — Immutability & Anti-Tampering

Can an attacker who owns our credentials destroy our recovery path?

- [ ] 9. Is at least one backup copy immutable (object lock / WORM) for a defined retention period? (0 / 1 / 2)
- [ ] 10. Can an administrator — or a stolen admin credential — disable or delete the immutable copy on demand? (Score 2 only if the answer is a clear no.) (0 / 1 / 2)
- [ ] 11. Does overriding immutability require a separate, time-delayed process by design? (0 / 1 / 2)
- [ ] 12. Are backup repositories protected by MFA and separate authentication from production? (0 / 1 / 2)
- [ ] 13. Is there alerting on deletion attempts or unexpected changes to backup data? (0 / 1 / 2)

Section S2 subtotal _____ / 10

S3 — The 3-2-1-1-0 Audit

Does the strategy survive the modern threat model, not just hardware failure?

- [ ] 14. (3) Are there at least three copies of the data — production plus two backups? (0 / 1 / 2)
- [ ] 15. (2) Are copies stored on two different media or storage types? (0 / 1 / 2)
- [ ] 16. (1) Is at least one copy genuinely off-site? (0 / 1 / 2)
- [ ] 17. (1) Is at least one copy offline, air-gapped, or immutable — unreachable from a compromised production environment? (0 / 1 / 2)
- [ ] 18. (0) Are zero errors verified through automated recovery testing and integrity checks? (0 / 1 / 2)

Section S3 subtotal _____ / 10

S4 — RTO / RPO Engineering

Are our recovery targets real numbers we've hit, or aspirations from a template?

- [ ] 19. Is there a documented RTO (tolerable downtime) per system tier? (0 / 1 / 2)
- [ ] 20. Is there a documented RPO (tolerable data loss) per system tier? (0 / 1 / 2)
- [ ] 21. Has the RTO been measured end-to-end in a drill, not just quoted? (0 / 1 / 2)
- [ ] 22. Is there tiered recovery — a defined order so critical systems come back first? (0 / 1 / 2)
- [ ] 23. Do the estimates account for restoring everything at once (full environment, not one server)? (0 / 1 / 2)

- [ ] 24. Is recovery infrastructure ready to receive a full restore without waiting on hardware procurement? (0 / 1 / 2)

Section S4 subtotal _____ / 12

S5 — Restore Testing Evidence

Can they prove a restore, or only assert one?

- [ ] 25. Is automated recovery verification in place (backups booted/checked in a sandbox)? (0 / 1 / 2)
- [ ] 26. Can the provider produce a recovery verification report as an artifact? (0 / 1 / 2)
- [ ] 27. Has a full-environment restore been performed (drill or real) in the last 12 months, with elapsed time recorded? (0 / 1 / 2)
- [ ] 28. Can restores be performed from multiple historical dates, not just the latest point? (0 / 1 / 2)
- [ ] 29. Is restore testing performed on a regular cadence (at least quarterly) and logged? (0 / 1 / 2)

Section S5 subtotal _____ / 10

S6 — M365 / SaaS Shared-Responsibility Gap

Have we closed the gap everyone assumes Microsoft covers?

- [ ] 30. Is it documented and understood that Microsoft's shared responsibility model makes the customer responsible for the data? (0 / 1 / 2)
- [ ] 31. Can the provider demonstrate a granular M365 restore (single mailbox, single file, single Teams channel)? (0 / 1 / 2)
- [ ] 32. Is Entra ID / conditional access recoverable, not just mailbox and file data? (0 / 1 / 2)
- [ ] 33. Is protection against OneDrive/SharePoint ransomware sync (encrypted files propagating to cloud) addressed? (0 / 1 / 2)
- [ ] 34. For each other critical SaaS, can you name the third party taking independent restorable copies? (0 / 1 / 2)

Section S6 subtotal _____ / 10

S7 — Provider & Operating Model

Who owns the restore at 2 a.m., and what does accountability actually look like?

- [ ] 35. Are SLAs specific about restore responsibilities, response, and escalation — with named contacts? (0 / 1 / 2)
- [ ] 36. Can the provider describe a real, recent full restore in concrete terms (size, time, outcome)? (0 / 1 / 2)
- [ ] 37. Is there a clear answer to who drives the recovery during an active incident (provider vs. you)? (0 / 1 / 2)
- [ ] 38. Does the provider have a strategy for reaching a known-clean restore point after delayed-detection ransomware? (0 / 1 / 2)

Section S7 subtotal _____ / 8

S8 — Exit & Portability

If this relationship ends, do we get our data — and our recoverability — back?

- [ ] 39. Is there a documented, fast path to extract all data in a usable, standard format on exit? (0 / 1 / 2)
- [ ] 40. Are retention windows deep enough to survive a breach that goes undetected for days or weeks? (0 / 1 / 2)

Section S8 subtotal _____ / 4

Red-Flag Summary — 10 Deal-Stoppers

Any single item here should pause a purchase until it's resolved in writing and demonstrated — not promised.

- [ ] R1. "Immutable" backups an administrator can disable or delete on demand.
- [ ] R2. No automated recovery verification — "the job succeeded" is the only proof of health.
- [ ] R3. Backup infrastructure shares credentials and network reachability with production.
- [ ] R4. RTO/RPO quoted from marketing with zero restore-drill evidence.
- [ ] R5. "Microsoft 365 is handled by Microsoft" — or M365 coverage that's a single retention policy.
- [ ] R6. Recovery estimates based on one server, presented as if they apply to a full event.
- [ ] R7. No strategy for reaching a known-clean restore point after delayed-detection ransomware.
- [ ] R8. Retention too short to survive a breach undetected for days or weeks.
- [ ] R9. No clear, fast, documented path to extract your own data on exit.
- [ ] R10. Provider can't describe a real, recent full restore in concrete terms.

Red flags counted (any > 0 = stop and resolve before signing) _____ / 10

Scorecard Tally & Next Step

Section	Score	Max
S1 — Scope & Coverage Inventory		16
S2 — Immutability & Anti-Tampering		10
S3 — The 3-2-1-1-0 Audit		10
S4 — RTO/RPO Engineering		12
S5 — Restore Testing Evidence		10
S6 — M365 / SaaS Shared-Responsibility Gap		10
S7 — Provider & Operating Model		8
S8 — Exit & Portability		4
TOTAL		80

Interpreting your score

Total	What it means	Next step
68–80	Strong, provable recoverability.	Confirm any 1s, fix red flags, schedule recurring drills.
50–67	Real gaps, often in immutability or restore testing.	Remediate the weakest two sections before relying on this program.
30–49	You have storage, not proven recoverability.	Treat as high-risk; prioritize a full recoverability review now.
Below 30	You'd be hoping, not recovering.	Stop. Rebuild the strategy around the six core capabilities.

> Any red flag at all overrides the score: A program can total 70 and still be undeliverable if R1 or R3 is unresolved.

Next step: bring the lowest-scoring two sections — and every counted red flag — to a recoverability assessment. The goal isn't a higher score on paper; it's a restore you've watched happen, timed, under the conditions you'll actually face.

Can You Prove You'd Recover — or Are You Hoping?

Plow helps IT leaders pressure-test backup and recovery for real, provable recoverability.

Request a Backup & Recovery Assessment →