

FREE RESOURCE • SELF-ASSESSMENT

DR Readiness Self-Assessment.

Twenty scored questions that turn "we think we're covered" into a number you can act on. Score it in fifteen minutes, see exactly where recovery would break, and walk into your next review with evidence instead of optimism.

QUESTIONS

20

scored across five domains

DOMAINS

5

backup, testing, RPO/RTO, docs,
security

MAX SCORE

60

with a four-band results key

TIME

15m

to a number you can act on

Score where you stand.

Most teams overestimate recovery until the day they test it. Score each statement honestly. The point isn't a good number, it's an accurate one, because the gaps you can name are the gaps you can close before they cost you.

**SCORE EACH
0 TO 3**

0 Not in place • **1** Partial / ad hoc • **2** Mostly, with gaps • **3** Fully in place and verified

Backup COPIES & INTEGRITY

Subtotal ____ / 12

- | | | |
|-----------|---|---|
| A1 | We keep backups that follow 3-2-1-1-0: three copies, two media, one offsite, one offline or immutable, zero errors. | <input type="text" value="0"/> <input type="text" value="1"/> <input type="text" value="2"/> <input type="text" value="3"/> |
| A2 | At least one copy is immutable or air-gapped and cannot be altered by an admin credential. | <input type="text" value="0"/> <input type="text" value="1"/> <input type="text" value="2"/> <input type="text" value="3"/> |
| A3 | We back up Microsoft 365 and our SaaS data with a third-party tool, not just native retention. | <input type="text" value="0"/> <input type="text" value="1"/> <input type="text" value="2"/> <input type="text" value="3"/> |
| A4 | Backup jobs are monitored and a human is alerted on every failure. | <input type="text" value="0"/> <input type="text" value="1"/> <input type="text" value="2"/> <input type="text" value="3"/> |

Recovery testing PROOF IT WORKS

Subtotal ____ / 12

- | | | |
|-----------|--|---|
| B1 | We perform full test restores of real workloads on a regular schedule. | <input type="text" value="0"/> <input type="text" value="1"/> <input type="text" value="2"/> <input type="text" value="3"/> |
| B2 | Our most recent restore test succeeded end to end and was documented. | <input type="text" value="0"/> <input type="text" value="1"/> <input type="text" value="2"/> <input type="text" value="3"/> |
| B3 | We test recovery of the full environment (AD, DNS, networking, certificates), not just data. | <input type="text" value="0"/> <input type="text" value="1"/> <input type="text" value="2"/> <input type="text" value="3"/> |
| B4 | We run at least one drill a year assuming the primary site is completely unavailable. | <input type="text" value="0"/> <input type="text" value="1"/> <input type="text" value="2"/> <input type="text" value="3"/> |

RPO & RTO TARGETS VS REALITY

Subtotal ____ / 12

- | | | |
|-----------|---|---|
| C1 | We have defined RPO and RTO targets for critical systems, approved by leadership. | <input type="text" value="0"/> <input type="text" value="1"/> <input type="text" value="2"/> <input type="text" value="3"/> |
| C2 | We have measured actual recovery time and data loss in a drill against those targets. | <input type="text" value="0"/> <input type="text" value="1"/> <input type="text" value="2"/> <input type="text" value="3"/> |
| C3 | Our backup frequency genuinely supports our stated RPO. | <input type="text" value="0"/> <input type="text" value="1"/> <input type="text" value="2"/> <input type="text" value="3"/> |
| C4 | Critical systems are prioritized so the most important services recover first. | <input type="text" value="0"/> <input type="text" value="1"/> <input type="text" value="2"/> <input type="text" value="3"/> |

Documentation & security.

Documentation **RUNBOOK & OWNERSHIP**

Subtotal ____ / 12

D1	We have a written DR runbook with step-by-step recovery procedures.	0	1	2	3
D2	Someone other than the primary engineer can execute the runbook unaided.	0	1	2	3
D3	Emergency contacts, vendors, and escalation paths are documented and current.	0	1	2	3
D4	The DR plan is reviewed after major changes and at least quarterly.	0	1	2	3

Security **STOPPING THE CAUSE**

Subtotal ____ / 12

E1	MFA is enforced for all remote access and privileged accounts.	0	1	2	3
E2	We have endpoint detection and response (EDR) with someone monitoring it.	0	1	2	3
E3	We carry cyber insurance and know its notification and vendor requirements.	0	1	2	3
E4	We patch known vulnerabilities on a defined, tracked cadence.	0	1	2	3

Total readiness score (add all five subtotals)

____ / 60

What your score means.

46–60

RESILIENT

Tested, documented, recoverable.

You're in strong shape. Keep validating on a schedule, and pressure-test the one or two domains where you scored lowest before they drift.

31–45

EXPOSED

Backups exist, recovery is unproven.

The common mid-market profile. You'd probably recover, but slower and with more loss than you expect. Close the testing and documentation gaps first.

16–30

AT RISK

Major gaps in recovery or security.

An incident today would hurt. Prioritize a real DR plan with validated RPO/RTO and an immutable backup copy now, not next quarter.

0–15

CRITICAL

An incident today means serious loss.

Treat this as urgent. The fastest path to safety is a tested backup copy you can't lose and a documented way to restore it. Get help this week.

Disaster Recovery (DRaaS)

theitvortex.com/disaster-recovery-as-a-service/

Validated RPO and RTO with tested failover, the fastest way to move up a band.

Backup as a Service (BaaS)

theitvortex.com/veeam-baas-offerings/

Immutable, monitored, 3-2-1-1-0 backups across servers, M365, and SaaS.

Talk through your score: (201) 225-8670 • www.theitvortex.com

TURN YOUR SCORE INTO A PLAN

Send us your number, or don't, and book a readiness session. We'll validate the domains you scored lowest and map the shortest path to the next band up.

BOOK A READINESS AUDIT