



BOMA DIGITAL WORKS

FREE GUIDE & SELF-EVALUATION

Data Resiliency for Small to Large Businesses

Adding Value, Performance and Reliability to Your Work Environment

- RPO, RTO and system tiers
- Hybrid protection layers
- A 5-step resiliency roadmap
- The 3-2-1-1-0 rule
- Platform landscape for 2026
- Self-evaluation form

FREE · 5 PAGES

bomadw.com

For business owners, IT leaders and backup administrators

Resiliency is more than backup

Data resiliency is your ability to keep working, and recover quickly, when data is lost, damaged or held to ransom. It combines three things: **protection** (copies you can trust), **recovery** (proven, fast restores) and **continuity** (keeping critical work running).

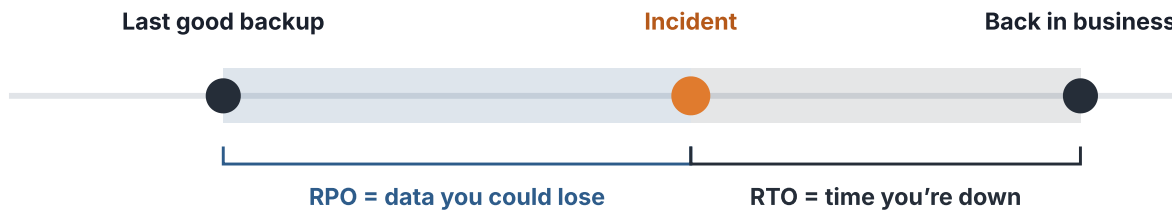
VALUE

Less downtime, fewer lost hours, and evidence that satisfies auditors, insurers and customers.

PERFORMANCE & RELIABILITY

Faster restores, fewer surprises, and systems your team can depend on every day.

The two numbers that drive every decision



Tier your systems

Tier	Examples	RPO	RTO	Approach
1 · Critical	ERP, order processing, core databases, identity	Minutes	Under 1–4 hours	Snapshots + replication, immutable copies
2 · Important	Email, file shares, CRM	1–4 hours	4–24 hours	Backups several times a day, offsite copy
3 · Standard	Archives, dev/test	24 hours	1–3 days	Nightly backup, low-cost storage

What usually causes data loss

- **Ransomware** that targets backups first
- **Human error**: deletions, overwrites
- **SaaS gaps**: Microsoft 365 and Google Workspace data is your responsibility
- **Hardware and site failures**: power, fire, flood, outages
- **Stolen admin credentials** used to delete copies

The 3-2-1-1-0 rule and hybrid layers

The classic 3-2-1 rule still works. Two extra digits protect you against today's ransomware.



Three copies, on two kinds of storage, with one offsite, one that nobody can tamper with, and proof they all restore.

Layer your protection

Layer	Covers	Restore speed	Watch-out
Snapshots	Quick rollback of recent changes	Seconds–minutes	Same system: not a backup on its own
Local backup / appliance	Daily backups, fast restores	Minutes	Same site; harden and make immutable
Object storage	Scalable, immutable copies (on-premises or cloud)	Minutes–hours	Needs a second location to count as offsite
Cloud backup	Offsite and SaaS protection	Hours	Egress fees, bandwidth for large restores
Tape / offline	Long-term retention, true air gap	Hours–days	Slower restores; handling discipline

Confidence checklist

- ☐ An immutable or offline copy for every Tier 1 and 2 system
- ☐ Separate backup admin accounts, with MFA
- ☐ Backups encrypted in flight and at rest
- ☐ Restore tests at least quarterly, results recorded
- ☐ Microsoft 365 / Google Workspace protected
- ☐ A written runbook someone else can follow

COMMON MISTAKE

Treating file sync or replication (OneDrive, a mirrored NAS) as backup. Sync copies deletions and encrypted files too. Backups keep history.

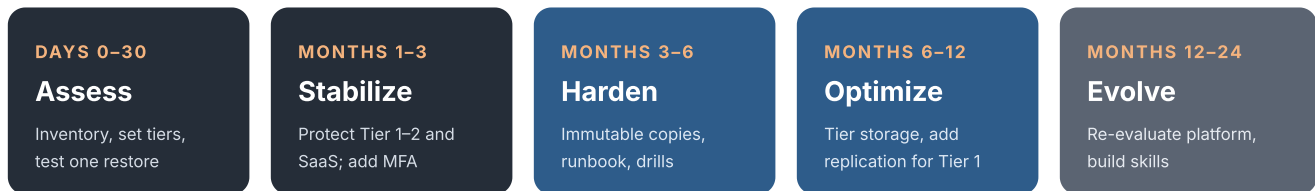
The platform landscape and your roadmap

Gartner's 2026 Magic Quadrant for Backup and Data Protection Platforms (June 29, 2026) named six Leaders. With IBM, these are the platforms most enterprises shortlist.

Vendor	Gartner 2026	Known for
Veeam	Leader	Broad workload coverage; placed highest in Ability to Execute
Commvault	Leader	Very broad feature depth across on-premises, cloud and SaaS
Rubrik	Leader	Security-first design and cyber recovery
Cohesity	Leader	Scale-out platform plus NetBackup (Veritas)
Druva	Leader	100% SaaS, nothing on-premises to manage
Dell Technologies	Leader	PowerProtect software with Data Domain appliances
IBM	Visionary	Storage Protect and Storage Defender for large estates

Smaller businesses often start with Veeam, Acronis Cyber Protect, Datto / Unitrends, Synology Active Backup for Business, NAKIVO, Backblaze or MSP360. Pick based on what you need to protect, and test a restore before you buy.

A 5-step resiliency roadmap



START THIS WEEK

Restore one critical system from backup and time it. If it doesn't meet its RTO, that's your first project.

Go deeper: Backup for Business

Our 31-page e-book adds feature-by-feature comparisons of the top 7 platforms, storage options, replication planning, certifications and a full buyer's evaluation toolkit.

bdwpdfguides.com

Gartner and Magic Quadrant are registered trademarks of Gartner, Inc.; Gartner does not endorse any vendor, product or service depicted in its research. Boma Digital Works is independent and not affiliated with any vendor named. Information current as of October 2026.

Data Resiliency Self-Evaluation

Tick one box per statement. Score **0** for No, **1** for Partly and **2** for Yes, then add up your total.

Organization _____ Completed by _____
 Date _____ Employees / key systems _____

#	Statement	No (0)	Partly (1)	Yes (2)
PLANNING				
1	We know which systems are critical (Tier 1) and have agreed RPO and RTO targets.	☐	☐	☐
2	We have an up-to-date inventory of where our data lives, including cloud and SaaS apps.	☐	☐	☐
3	Someone is clearly responsible for backup and recovery.	☐	☐	☐
PROTECTION				
4	Every Tier 1 and Tier 2 system is backed up automatically.	☐	☐	☐
5	Microsoft 365 / Google Workspace and other SaaS data is backed up.	☐	☐	☐
6	We keep at least one copy offsite (another site, region or cloud).	☐	☐	☐
7	At least one copy is immutable or offline.	☐	☐	☐
SECURITY				
8	Backup consoles use MFA and separate admin accounts.	☐	☐	☐
9	Backups are encrypted in flight and at rest.	☐	☐	☐
10	We're alerted to failed backups and unusual activity (possible ransomware).	☐	☐	☐
RECOVERY AND REPORTING				
11	We restore-test critical systems at least quarterly and record the results.	☐	☐	☐
12	Our last full restore test met its RTO.	☐	☐	☐
13	We have a written recovery runbook someone other than the admin can follow.	☐	☐	☐
14	Tier 1 systems can fail over or run from backup within their RTO.	☐	☐	☐
15	Leadership receives a regular backup and recovery report.	☐	☐	☐

Total score

out of 30 _____

0–12 · At risk

Start with steps 1–2 of the roadmap now.

13–22 · Developing

Close gaps in immutability, testing and SaaS.

23–30 · Resilient

Keep testing and reporting; optimize cost.

WANT A SECOND OPINION?

Email your completed form to hello@bomadw.com and Boma Digital Works will suggest your top three next steps.