BACKUP & DISASTER RECOVERY

CHECKLIST 2026

Can your business actually recover from a cyber attack or system failure?

A practical checklist for UK SMEs - including a 10-question Recovery Readiness Scorecard

THE UNCOMFORTABLE TRUTH ABOUT BACKUPS

Almost every UK business we audit has backups. Almost none of them have ever tested a real restore. That gap, between "we have backup" and "we can recover" is where most disaster recovery plans quietly fall apart.

By the time you find out, the systems are down, the data is gone, and the conversation has shifted from "what's our RTO?" to "do we still have a business?"

Backups are your last line of defence against ransomware, hardware failure, malicious deletion, accidental loss, and the long tail of things that take businesses offline. They are also, paradoxically, the controls most likely to be configured once and then ignored for years.

Most failures aren't dramatic. They're discovered at the worst possible moment, when someone confidently runs a restore, and nothing comes back.

There are two kinds of business: those that have lost data, and those that are about to. The difference between them is whether their last restore test actually worked.

- Recurring lesson from incident response engagements

This checklist gives you a clear, practical view of where your backup and recovery posture stands today. It covers the technical fundamentals, the often-overlooked gaps (Microsoft 365, immutable storage, recovery testing).

It includes a 10-question scorecard you can complete in five minutes to find out whether you'd survive a serious incident this week.

Use this guide as

- A self-assessment of your current backup and DR posture.
- A briefing document for your IT team, MSP or board.
- A justification framework for backup and DR investment.
- A pre-audit checklist for ISO 27001, Cyber Essentials Plus, or insurance reviews.

Headline numbers

- The average ransomware incident takes 21 days from breach to operational recovery, and that's when good backups exist. Without them, recovery is measured in months or simply isn't possible.
- Microsoft does not back up your Microsoft 365 data. Native retention is short, recoverability is limited, and "shared responsibility" puts the onus squarely on the customer.
- More than 40% of UK SMEs hit by ransomware never fully recover their data, even where backups existed.
- An untested backup is, in practical terms, not a backup, it is a hopeful filename.

Want us to validate your existing backups?
We offer a free Backup Validation Test, we don't replace your existing setup, we just attempt a real restore from it and tell you honestly what came back, what didn't, and how long it took. Most businesses learn something uncomfortable but useful. No commitment, no obligation, completed within five working days.

- Request your free Backup Validation Test at systemforce.co.uk

THE 3-2-1-1-0 RULE (THE 2026 STANDARD)

The classic 3-2-1 backup rule has been the backbone of data protection for over twenty years. In the era of ransomware that specifically hunts for and encrypts backup repositories, the rule has evolved. The current best-practice standard is 3-2-1-1-0.

3 copies of your data the original plus at least two backups.

2 different types of media or storage tiers not all on the same disk array.

1 copy stored offsite separated geographically from the production environment.

1 copy that is immutable or air-gapped cannot be modified, encrypted, or deleted by anyone, including a compromised admin.

0 errors after backup verification if a restore test fails, the backup is not usable, regardless of what the dashboard says.

Why this matters: modern ransomware actively targets backup systems before triggering encryption it's the standard playbook. Attackers spend days or weeks inside a network, mapping and turning off recovery options before they pull the trigger. Without an immutable copy, the backup becomes part of the problem rather than the solution. The "1" for immutable is no longer optional.

What actually needs backing up

The list of things that need backup protection has expanded considerably since most policies were written. "All the servers" is no longer the answer. Modern backup coverage is about mapping where your business-critical data actually lives which is rarely where you think it is.

Coverage checklist

- All on-premises servers (file, database, application, domain controllers).
- All virtual machines (Hyper-V, VMware, Proxmox).
- Microsoft 365, Exchange Online, SharePoint, OneDrive, Teams, and Microsoft 365 Groups.

- Other SaaS platforms, CRM (Salesforce, HubSpot), accounting (Xero, Sage), HR systems, ticketing platforms.
- Endpoints laptops and desktops storing local data, particularly for hybrid and remote workers.
- Configuration data firewall rules, switch configs, server build documentation, application settings.
- Cloud infrastructure, Azure / AWS / GCP environments where critical workloads run.
- Line-of-business application databases, even where these run on managed services.

SFIT insight: The most commonly missed categories are SaaS data ("the vendor handles it" usually they don't, beyond limited retention) and endpoint data (people save things to local drives despite policies saying they shouldn't). Both surface as gaps the moment someone needs a restore.

THE TWO NUMBERS EVERY BUSINESS OWNER SHOULD KNOW.

Recovery Time Objective (RTO) and Recovery Point Objective (RPO) are the two figures that drive every meaningful backup and disaster recovery decision.

Most business owners couldn't quote either for their own business and yet these are the numbers that determine whether they have a viable continuity plan or just a hopeful collection of backup software.

Recovery Time Objective (RTO)

How long can the business be down before the impact is unacceptable? Measured in minutes, hours or days.

The answer should differ across systems your email tolerance is probably tighter than your file server tolerance, which is probably tighter than your archive system.

Boardroom translation: "After the worst happens, how long can we be offline before it becomes a real problem for customers, revenue, or compliance?"

Recovery Point Objective (RPO)

How much data can the business afford to lose? Measured in time "we can lose the last 15 minutes" or "we can lose up to a day".

A daily backup means an RPO of up to 24 hours. Continuous replication means an RPO measured in seconds.

Boardroom translation: "If we lost everything that happened today after [last backup time], could we reconstruct it, or would it be permanently gone?"

Typical sector targets

Sector	Typical RTO	Typical RPO	Why
Professional services	4–8 hours	1 hour	Client deadlines, billable hours, document version control
E-commerce/retail	1–4 hours	15 mins	Continuous transactions, lost sales, and customer experience
Manufacturing	2–8 hours	1 hour	Production schedules, supply chain, quality records
Healthcare / clinical	1–4 hours	15 mins	Patient safety, clinical records, regulatory obligations
Financial services	1–2 hours	Near zero	FCA requirements, transaction integrity, and audit trail

SFIT insight: Tighter RTO/RPO costs more that's the trade-off. The most useful exercise is not arguing about the perfect number but agreeing on the actual number with leadership, then designing a backup strategy that genuinely supports it. "As fast as possible" is not a recovery objective; it's an aspiration.

SECURING THE BACKUP ITSELF

A decade ago, backup security meant locking the tape cupboard. Today, backups are network-attached, cloud-based, and accessible to whichever account credentials are sitting on a compromised admin's machine.

Backup security is now part of cybersecurity not an adjacent discipline.

Self-assessment

- Backup data is encrypted both in transit and at rest.
- Backup repositories are isolated from the production network, separate authentication, separate network segment.
- Backup administrative access requires Multi-Factor Authentication, ideally phishing-resistant for cloud backup consoles.
- Backup admin accounts are separate from production admin accounts.
- At least one backup copy is immutable cannot be deleted or modified for a defined retention period, even by an administrator.
- Backup activity (logins, deletions, retention changes) generates alerts to a security mailbox or SOC.
- Encryption keys are managed and recoverable independently of the production environment.

What good looks like

An attacker who has fully compromised your production environment still cannot delete, modify or encrypt your backup data.

Recovery is possible regardless of what happens to the live environment. That is the actual standard for backup security in 2026.

THE MICROSOFT 365 BACKUP GAP

If there is one section of this guide every Microsoft 365 customer needs to read carefully, it's this one. The shared responsibility model is unambiguous: Microsoft maintains the platform. You keep the data safe. And yet most businesses we audit assume Microsoft is handling backup because it's never been clearly explained that they aren't.

What Microsoft does (and doesn't) protect

- Microsoft maintains platform availability and infrastructure-level redundancy.
- Microsoft retains deleted items in standard retention windows typically 30–93 days depending on the workload.
- Microsoft does NOT protect against malicious deletion outside that window.
- Microsoft does NOT protect against ransomware that encrypts files synchronised to OneDrive or SharePoint.
- Microsoft does NOT protect against rogue or compromised admin activity.
- Microsoft does NOT provide point-in-time restore beyond the limited native Windows.
- Microsoft does NOT meet retention requirements for most regulated industries.

What you need:

A third-party Microsoft 365 backup solution covering Exchange Online, SharePoint, OneDrive, Teams, and Microsoft 365 Groups. Industry-standard products include Veeam, Datto, Acronis, Keepit and Barracuda. Costs typically range from £3 to £6 per user per month, a fraction of the cost of a single failed restore.

Microsoft 365 backup sorted in 48 hours

We can deploy third-party Microsoft 365 backup across your tenant. Exchange, SharePoint, OneDrive, Teams, and Groups, usually within 2 working days. Fixed monthly per-user cost, immutable storage, tested restore included no long-term lock-in.

- Get your Microsoft 365 backup quote at systemforce.co.u

RECOVERY TESTING / THE DISCIPLINE MOST BUSINESSES SKIP

Backup software produces green ticks. Green ticks do not equal recoverability. The only way to know whether a backup actually works is to restore from it and the only way to know whether your business can recover from a real incident is to rehearse one.

Recovery testing is the most ignored discipline in backup management, and the one that most reliably separates businesses that recover from those that don't.

The testing cadence that works

- File-level restore tests: at least monthly, ideally weekly. Pick a random file from a backup, restore it, and verify it opens correctly.
- Server / VM restore tests: at least quarterly. Restore a server to an isolated test environment, confirm it boots, and confirm that applications run.
- Microsoft 365 restore tests: at least quarterly. Restore a mailbox, a SharePoint site, a Teams channel, verify content, permissions, metadata.
- Full disaster recovery simulation: at least annually. Tabletop exercise with the leadership team, then a partial technical rehearsal.
- Test results documented, including what was restored, how long it took, and what didn't work.
- Test failures trigger remediation, not just "we'll look at it next time".

What good looks like

Recovery is a practised skill, not a theoretical capability. Your team has actually done it recently and knows how long it really takes. Your RTO is evidence-based, not aspirational. The failure modes are known, documented, and addressed.

> **SFIT insight:** We have rarely run a recovery test that worked the first time perfectly. Something is always missing, a permission, a service account, a configuration setting. The point of testing isn't to prove the backup works; it's to find out what doesn't, before it matters.

COMMON BACKUP AND RECOVERY FAILURES

Every one of these has caused a real incident in a real UK SME within the last twelve months. None of them is theoretical.

- Backups never tested green ticks on the dashboard, no actual restore in living memory.
- Local-only backups both production data and backup data destroyed in the same fire, flood, or ransomware event.
- No Microsoft 365 backup assumption that Microsoft handles it. They don't.
- Backup admin uses the same password and account as production admin attacker compromises one, owns both.
- No defined RTO or RPO when an incident happens, no one knows what "good" looks like.
- No immutable copy ransomware encrypts the backup repository alongside production.
- Critical SaaS platforms not backed up "the vendor will sort it" turns out to be false.
- The DR plan was written years ago, never updated, and half the named contacts have left.
- Endpoint data not backed up laptops with critical local files lost in transit, theft, or hardware failure.
- Backups run, but failures aren't monitored the last successful backup was three weeks ago, and nobody noticed.

If three or more apply to your business, your backup posture is functionally unreliable and an incident this year would test it very publicly.

THE DISASTER RECOVERY PLAN ESSENTIALS

A disaster recovery plan that exists but no one has read is not much better than no plan at all.

The goal is a document that someone not necessarily you could pick up at 2 am during an incident and use to make good decisions in the right order.

What the DR plan must contain

- Inventory of business-critical systems with their RTO and RPO.
- Recovery procedures for each critical system step-by-step, written for someone other than the original engineer.
- Roles and responsibilities who declares an incident, who leads recovery, who handles communications.
- Contact details, staff, key suppliers, IT support, insurance, regulatory contacts. Updated, not historical.
- Decision trees for common scenarios, ransomware, data loss, prolonged outage, supplier failure.
- Communication templates, for staff, customers, suppliers, and regulators, where applicable.
- Recovery success criteria how you know you're back, not just up.
- Storage location accessible during an incident not just on the file server that's currently encrypted.

SFIT insight: The single best test of a DR plan is to ask someone unfamiliar with it to read it under time pressure and explain what they would do first. If they can't, the plan needs to be rewritten. Plans written by experts for experts often fail this test and the people using them at 2 am during a real incident may not be the experts.

RECOVERY READINESS SCORECARD

Ten yes/no questions. Answer honestly overestimating now means a worse surprise later. Tick "Yes" only if you could provide evidence to an auditor, an insurer or a board. Score yourself out of ten and read the bands below the table.

Question	Yes	No
1. Backups run daily and successfully across all critical systems.	☐	☐
2. Backups include all servers, endpoints, and Microsoft 365 / cloud data.	☐	☐
3. At least one backup copy is stored offsite or in a separate cloud region.	☐	☐
4. At least one backup copy is immutable (cannot be deleted or encrypted by ransomware).	☐	☐
5. Backup data is encrypted in transit and at rest.	☐	☐
6. Documented Recovery Time Objective (RTO) exists for every critical system.	☐	☐
7. Documented Recovery Point Objective (RPO) exists for every critical system.	☐	☐
8. A real restore test has been performed in the last 90 days.	☐	☐
9. A full disaster recovery simulation has been performed in the last 12 months.	☐	☐
10. A documented DR plan exists, with named owners and current contact details.	☐	☐

Important: this scorecard reveals exposure, not the exact remediation path. A low score can be addressed quickly and cost-effectively if approached in the right order. The fastest single uplift is almost always achieved by implementing third-party Microsoft 365 backup and running a real restore test against existing on-premises systems. From there, the priorities depend on what specifically is missing.

Score interpretation

Score	Band	What it means
0 – 3	CRITICAL EXPOSURE	Material risk of business-ending data loss. Address as a board-level priority this quarter.
4 – 6	AT RISK	Backups exist, but recovery is unreliable. Specific gaps need to be closed before the next incident.
7 – 8	ADEQUATE	Reasonable foundation. Refinement needed on testing, documentation or coverage.
9 – 10	STRONG	Mature recovery posture. Maintain through regular testing, drills and reviews.

HOW SYSTEM FORCE IT CAN HELP

Backup and disaster recovery are not products you buy once. It is a discipline maintained continuously backups that actually run, restores that actually work, plans that actually reflect today's environment. Most internal IT teams are stretched too thin to maintain it properly, and most generic IT providers focus on the install and forget the testing.

System Force IT delivers:

- Backup audits honest assessment of your current backup posture against this checklist, with a remediation plan.
- Backup validation tests real restore tests against your existing systems, with documented results.
- Microsoft 365 backup third-party backup deployed across Exchange, SharePoint, OneDrive, Teams and Groups.
- On-premises and hybrid backup, Veeam, Datto, and similar enterprise-grade products with immutable storage.
- Disaster recovery planning, workshops, documentation, tabletop exercises, full simulations.
- Managed backup services fully outsourced backup operation with monitoring, alerting and tested restore.

Book a Backup & Disaster Recovery Review
One of our senior engineers will assess your current backup and DR posture against the 10 scorecard questions, identify the most material gaps, and provide a clear remediation plan with realistic timelines and costs. Free of charge, completed within five working days. The report is yours to keep, whether or not you choose to work with us.

- Book your free DR review at systemforce.co.uk

Or call us directly: 01452 701355 We're based in Gloucestershire and protect UK SMEs across professional services, manufacturing, healthcare and digital sectors.

Authoritative sources and further reading

- NCSC Backup Guidance: ncsc.gov.uk/guidance/backing-your-data
- NCSC Mitigating Malware and Ransomware: ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks
- ICO Guide to Data Security and Backups: ico.org.uk
- Microsoft Shared Responsibility for Microsoft 365: learn.microsoft.com
- ISO 22301 Business Continuity Management: bsigroup.com

This document is provided for general guidance only. RTO/RPO targets, cost figures, and recovery time estimates are typical industry ranges based on UK SME data; actual figures vary significantly by business, sector, and incident type.

The scorecard is a planning tool, not a formal certification mechanism. Always seek tailored advice for material business continuity decisions.

System Force I.T.
Secure IT Simplified

Want a free backup and disaster recovery review with System Force IT?

We run free, no-obligation reviews for UK SMEs.
Written report in 7 working days.
No sales pitch, no follow-up unless you ask for one.

Book at systemforce.co.uk
Or call us directly: 01452 701355

System Force IT | supporting UK businesses since 2006.

UKAS ISO/IEC 27001: 2022 Certified | Microsoft Solutions Partner | Certified 3CX Partner | Cyber Essentials Practitioners | RIPE NCC Member

Next Step:

Book your free BACKUP & Disaster Recovery.

01452701355

www.systemforce.co.uk

sales@systemforce.co.uk