Macrium Software

It's our business to protect your data

Backup & Recovery Best Practices for IT/OT Environments

sales@macrium.com

www.macrium.com

Macrium Software
It's our business to protect your data



Contents

1 Why Backup & Recovery Matter in OT and IT 3

2 Why OT Environments Are at Risk 3

3 Understanding the 3-2-1-1-0 Backup Rule 4

4 Laying the Foundations for Resilience 5

- Foundation 1: Formalize Your Backup & Disaster Recovery Policy
- Foundation 2: Define Clear RPO & RTO Targets

5 Four-Step Approach to Backup & Recovery 5

- Step 1: Plan Your Backup & Recovery Strategy
- Step 2: Evaluate & Select Your Solution
- Step 3: Implement Your Backup & Recovery
- Step 4: Validate your Backups
- Step 5: Improve Your Strategy

6 What's Next for IT/OT Resilience 9

7 Turning Backup Strategy into Business Strength 9

Macrium Software

Why Backup & Recovery Matter in OT and IT

Operational technology (OT) systems were designed to be isolated, but the shift toward Industry 4.0, smart manufacturing and remote access has exposed them to the same cyber-threats that plague enterprise IT networks. Legacy equipment often lacks basic authentication or encryption and cannot be patched quickly, while IT and OT convergence opens new pathways for attackers, increasing exposure to ransomware and remote access.

In 2024, the number of industrial organizations listed on **ransomware leak sites reached 1,693, a year-over-year increase of 87%.** A quarter of these incidents resulted in a full OT shutdown, and three quarters caused partial outages. For example, **in late August 2025, a cyberattack forced Jaguar Land Rover** to proactively shut down IT systems across its global production plants, halting assembly lines that typically produce more than 1,000 vehicles per day and affecting a supply chain supporting more than 100,000 jobs. While malicious attacks dominate headlines, operational disruption can also come from accidental changes or untested software updates - such as the **infamous July 2024 CrowdStrike update** that triggered widespread organization-wide shutdowns.

The lesson is clear: **prevention alone does not guarantee continuity. A comprehensive backup and recovery strategy is the lifeline that determines whether you can restore operations quickly or face prolonged and damaging downtime.**

Why OT Environments Are at Risk

OT environments were once protected by isolation, but the shift toward connected, data-driven operations has changed that. Systems that previously ran on air-gapped PLCs and SCADA networks now depend on IT infrastructure for remote monitoring, cloud analytics, and proactive maintenance. Every new connection - a VPN tunnel, a wireless sensor, or an engineer's laptop - introduces another potential entry point. Attackers exploit these connections, often using stolen IT credentials to move laterally into OT environments where legacy devices lack modern security controls.

Ransomware groups have quickly adapted to these opportunities. They know that halting a production line or distribution center can cost millions in lost output and penalties, and they use that leverage to demand higher payments. Dragos also reported that of the increasing attacks 70% affect manufacturers and 25% cause a complete OT shutdown. This underlines how industrial operations have become a prime target for disruption.



2025 Paramount Software UK Limited. All rights reserved.

Macrium Software

Not all threats are intentional. Human error remains one of the most persistent risks, contributing to 95% of breaches according to industry studies. A single phishing email, weak password, or untested vendor update can open the door to a major outage. Even well-intentioned actions, such as remote maintenance or configuration changes, can trigger cascading failures across critical systems.

At the same time, regulatory expectations are tightening. Frameworks like **NIS2 and NIST SP 800-82** now emphasize operational resilience — not just prevention but demonstrable recovery capability. These standards require organizations to document, test, and prove their ability to restore essential services. Meeting them isn't just a compliance exercise; it's an opportunity to embed stronger, repeatable backup and recovery practices across both IT and OT.



Understanding the 3-2-1-1-0 Backup Rule

The 3-2-1-1-0 model is recognized as the gold standard for system protection, trusted by IT and OT environments alike for its reliability and resilience.

3 copies

Keep one production copy and at least two additional backups.

2 media

Store backups on two different media types (for example, local disk and tape or cloud).

1 off-site

Maintain at least one copy off-site to safeguard against fires, floods, or site-wide outages.

1 immutable or offline

Protect one copy using immutable storage or offline, air-gapped media to defend against ransomware.

0 errors

Regularly test and verify backups so there are no errors when recovery is needed.

The model sounds simple, but implementing it effectively can be complex. Air-gapped storage, off-site rotation, and regular validation add cost and coordination challenges — particularly in distributed OT environments with bandwidth constraints or remote facilities. Many industrial systems still run on older operating systems such as Windows XP or legacy Linux, which cannot easily connect to modern cloud solutions.

For many organizations, 3-2-1-1-0 serves as a North Star - a guiding standard to aim toward rather than a single project to complete. Start by creating multiple copies across different media, then build in off-site and immutable layers as budgets, infrastructure, and risk appetite evolve

Above all, keep validation front and center: a backup only proves its worth when it restores cleanly and completely.

2025 Paramount Software UK Limited. All rights reserved.

Macrium Software

Laying the Foundations for Resilience

While the 3-2-1-1-0 model sets out the technical principles of resilience, it's only effective when built on the right foundations. Before you can shape your backup and recovery strategy, you need to establish two key cornerstones: a clear policy and defined recovery objectives. These form the framework every technical decision will rely on.

Foundation 1: **Formalize Your Backup & Disaster Recovery Policy**

A well-defined backup and disaster recovery policy turns best practice into consistent execution. Document how often backups occur, what data is included, retention periods, off-site storage locations, and who is responsible for managing recovery. A clear policy reduces confusion during incidents, supports audit requirements, and ensures everyone understands their role in maintaining resilience.

Make sure you review both frequently to ensure your policies and targets stay aligned with your business's goals.

Foundation 2: **Define Clear RPO & RTO Targets**

Once your policy is in place, establish measurable recovery objectives that align with your business and compliance needs. Define your Recovery Point Objective (RPO) — how much data loss is acceptable — and your Recovery Time Objective (RTO) — how quickly systems must be restored. Set these targets based on operational impact and regulatory expectations. For example, mission-critical production systems may require near-zero downtime, while less essential workloads can tolerate longer recovery times. Frameworks such as NIS2 increasingly expect organizations to demonstrate their ability to restore essential services quickly

Four-Step Approach to Backup & Recovery

Step 1: Plan Your Backup & Recovery Strategy

Planning is where resilience begins. Map your environment: conduct a Business Impact Analysis to rank workloads by criticality and determine acceptable downtime and data loss. Engage stakeholders across IT and OT – engineers, operators and executives – to capture the nuances of industrial processes and ensure buy-in. Determine regulatory obligations and align them with your RPO/RTO targets.

When selecting storage media, weigh speed versus resilience. For high priority systems, locally attached storage typically provides faster recovery performance than NAS devices, while tape or rugged removable drives provide durability and isolation. Cloud or colocation services can serve as off-site targets but may incur bandwidth costs or slower recovery.

Step 1 Checklist

- ☐ **Conduct a Business Impact Analysis and define RPO/RTO targets.**
- ☐ **Involve IT and OT stakeholders to build a shared view of risk.**
- ☐ **Choose media that balance performance, cost and resilience.**
- ☐ **Create a documented backup and disaster recovery policy.**

2025 Paramount Software UK Limited. All rights reserved.

Macrium Software

Step 2: Evaluate & Select Your Solution

Armed with an understanding of what you need to protect and your RPO/RTO objectives, evaluate backup technologies. Start by deciding which level of backup is appropriate for each workload:

Application-level backups protect specific services such as databases. They allow quick recovery of critical workloads but may leave the underlying OS and configuration unprotected.

File-level backups safeguard user data and shared folders; they are simple and lightweight but require rebuilding systems manually after a failure

---

System imaging (recommended for most OT/IT infrastructure) captures a sector-level snapshot of entire disks and partitions. Images provide flexibility - you can recover the whole system to identical or dissimilar hardware, virtualize it or extract individual files —and typically enable faster recovery in a disaster.

Once you understand the level of protection needed, look at features such as full-system imaging, incremental/differential backups, synchronization, encryption and flexible scheduling. Image-based backups capture the entire OS, applications and configuration, making it easier to rebuild an infected machine or restore a “golden image” after a ransomware incident. Complement images with application-level protection where appropriate.

The goal is to identify solutions that meet your requirements and are easy to manage. Consider:

Environment fit

Does the solution protect the mix of virtual machines, physical servers, workstations and industrial PCs in your environment?

Scalability

Can it handle the number of devices and data volume you anticipate? Centralized management becomes important when protecting hundreds of endpoints or remote facilities.

Granularity

Does it allow both bare-metal recovery and granular file or application restores? Flexibility speeds up recovery

Vendor expertise

Look for a partner familiar with industrial requirements and regulatory nuances. Strong support can be more valuable than marginal feature differences.

Tip 1: Embrace Imaging & Full-System Backup Solutions

Image-level backups capture entire operating systems, configurations, and application data — not just files — allowing for faster, more reliable recovery. They also align with frameworks like NIST SP 800-34 and NIS2, making them ideal for critical IT/OT endpoints where downtime must be minimized.

Tip 2: Combine Full, Incremental, and Differential Backups

Use a mix of full, incremental, and differential backups to balance performance, storage efficiency, and recovery speed. Full backups provide complete protection but require more storage, while incremental and differential backups capture only changes — helping you meet RPO and RTO targets without unnecessary overhead.

2025 Paramount Software UK Limited. All rights reserved.

Macrium Software

Step 3: Implement Your Backup & Recovery System

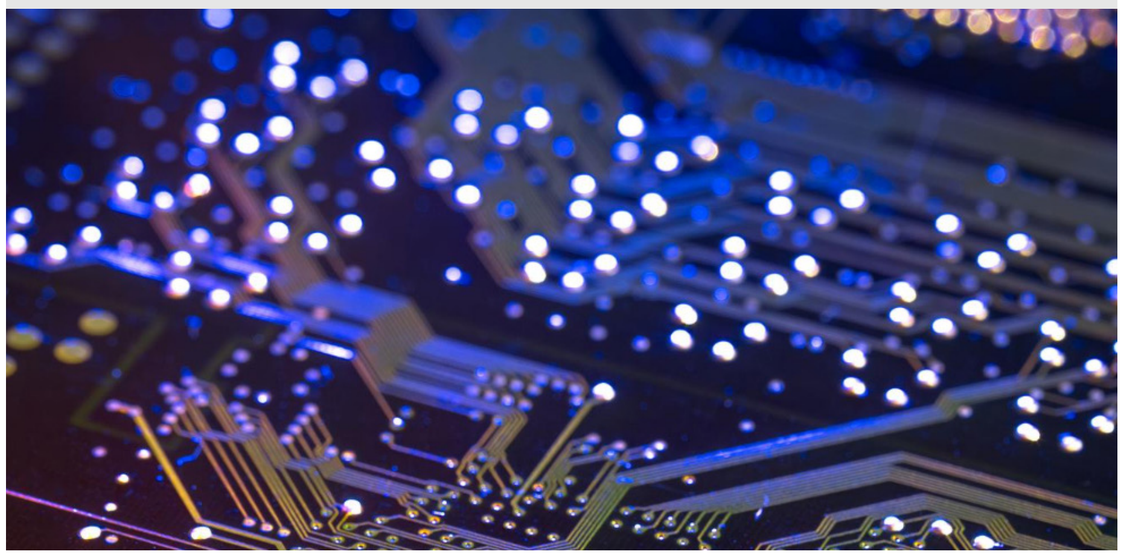
With a plan and a solution selected, translate the 3-2-1-1-0 principles into concrete actions. Diversify your copies: store one on a fast, local location for rapid restores; another on a separate medium such as a removable hard drive; and a third at an off-site location or secure cloud. For ransomware resilience, adopt immutable storage or air-gapped media that cannot be altered by malware.

Automate and orchestrate backup jobs to reduce human error. Schedule frequent incrementals for data that changes often and less frequent fulls for static systems. Deduplication and compression help control storage growth. For geographically dispersed sites, utilize storage close to the systems being backed up to avoid sending excess traffic over VPNs.

Finally, build a layered recovery strategy. Full-system images enable bare-metal restores when a workstation or server is compromised. Granular file-level backups allow you to recover specific datasets quickly. Replicate critical backups to a secondary site or disaster recovery environment so you can fail over if your primary location is lost.

Step 3 Checklist

- ☐ **Maintain ideally three copies of each backup on two media types.**
- ☐ **Ensure one copy is off-site and one is immutable/offline.**
- ☐ **Automate backup jobs and leverage deduplication.**
- ☐ **Layer full-image and file-level backups for flexibility.**
- ☐ **Train staff on how to perform restores and document procedures.**



Step 4: Validate

Testing brings the “0” in the 3-2-1-1-0 model to life.

Build regular validation into your process so you know recovery will work when it matters. Start small, then move toward full recovery drills.

Check integrity

Run simple hash checks to confirm that backup files are complete and unaltered.

Test virtual restores

Boot a backup in an isolated environment to make sure operating systems, drivers, and applications load as expected.

Try hardware restores

Apply an image to a physical machine of the same type used in production to confirm compatibility and reliability.

Run disaster recovery drills

Protect one copy using immutable storage or offline, air-gapped media to defend against ransomware.

Refine and repeat

After every test, document what worked and what didn’t, and update your procedures.

2025 Paramount Software UK Limited. All rights reserved.

Macrium Software

Prove Your Backups Work When It Counts

Integrate backup into your incident response plan

When responding to a ransomware attack or other disruption, staff should know which clean backups to use and how to isolate infected systems. Train your incident response team on restoration procedures so recovery becomes muscle memory

Integrity checks strengthen confidence

Use hash comparisons or checksum verification to confirm that backup data matches the source. Audit backup logs and retention schedules to confirm policies are being followed.

Build a Habit of Documentation

Throughout this process, document the configuration of your backup environment, the results of each test and any lessons learned. Documentation supports audits, accelerates onboarding of new staff and provides a repeatable baseline for future exercises. Each iteration should feed back into your plan, creating a cycle of continuous improvement

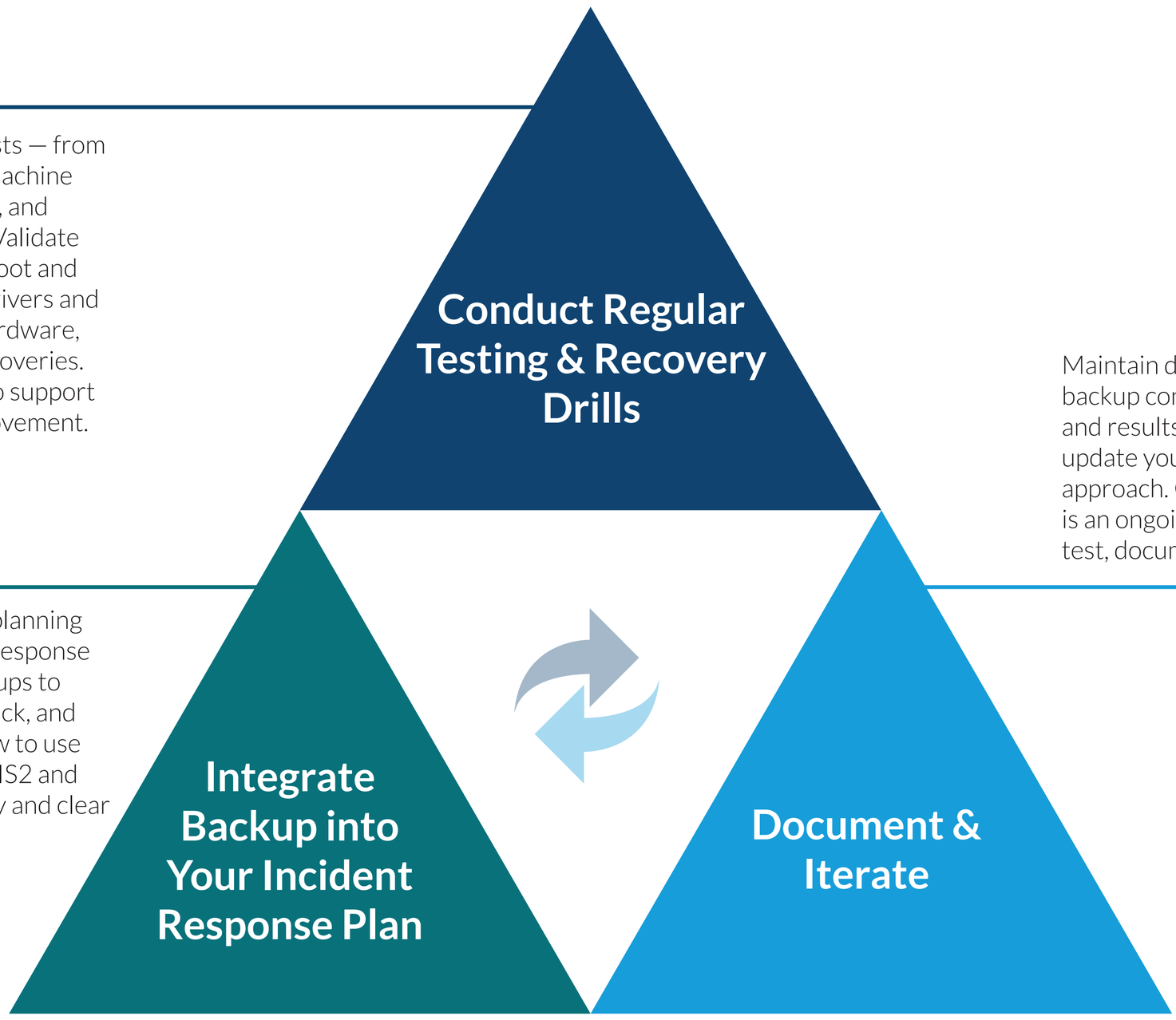
Step 5: Improve

Validation isn't the end of the process — it's where meaningful improvement begins. Use the insights from testing, audits, and real-world incidents to strengthen every part of your backup and recovery strategy. Review the results of each test and compare them against your RPO and RTO targets. Identify where recovery fell short or where automation could reduce time and human error. Feed these lessons into updates to your backup schedule, storage choices, and policies.

Encourage cross-team collaboration between IT, OT, and security teams to identify process gaps and coordinate improvements. Regular reviews of incident reports and new technologies help ensure your strategy evolves alongside your infrastructure and threat landscape.

Continuous improvement turns backup and recovery from a maintenance task into a living resilience capability — one that adapts as your organization grows and as new risks emerge.

Schedule routine restore tests — from hash verification to virtual machine restores, hardware restores, and full disaster recovery drills. Validate that image-based backups boot and function correctly, ensure drivers and applications work on real hardware, and rehearse large-scale recoveries. Record and review results to support audits and continuous improvement.



Maintain detailed documentation of backup configurations, test procedures, and results. After each test or incident, update your runbooks and refine your approach. Continuous improvement is an ongoing cycle — plan, implement, test, document, and repeat.

Make backup and recovery planning a core part of your incident response strategy. Identify clean backups to rebuild systems after an attack, and train teams on when and how to use them. Regulations such as NIS2 and HIPAA expect rapid recovery and clear evidence of preparedness.

2025 Paramount Software UK Limited. All rights reserved.

Macrium Software

What's Next for IT/OT Resilience

IT and OT environments are becoming more connected, bringing efficiency but also new exposure. Attackers are exploiting the overlap between systems, using stolen credentials, remote access and compromised software updates to move between networks. AI-driven malware and supply-chain compromises are now routine risks, which means recovery planning must extend beyond your own infrastructure. Suppliers, service providers and partners all play a role in resilience.

At the same time, OT networks are growing to support thousands of IoT and edge devices, each with their own vulnerabilities. Organizations are adapting by introducing zero-trust architectures, immutable backups and automated recovery testing to ensure systems can be restored quickly and safely.

Regulatory frameworks such as NIS2 and DORA continue to push the industry toward greater accountability. The organizations that succeed will be those that can demonstrate their readiness, not just claim it. Being able to test, measure and prove recovery capability will become a competitive advantage.

Resilience is moving from a compliance exercise to a core business discipline — one that protects operations, reputation and trust in an increasingly connected world.



Turning Backup Strategy into Business Strength

Backup and recovery underpin every aspect of operational resilience in IT and OT environments. A clear, well-tested strategy doesn't just protect data; it keeps critical systems running, safeguards productivity and strengthens stakeholder confidence. By understanding the risks specific to OT, adopting the 3-2-1-1-0 model, and following a structured approach to Plan, Evaluate, Implement, and Validate, and Improve, organizations can recover quickly from incidents and reduce downtime.

2025 Paramount Software UK Limited. All rights reserved.

Macrium Software

It’s our business to protect your data

If you´d like expert guidance on shaping your resilience strategy, Macrium´s specialists can help you assess your current setup, identify risks, and implement backup and recovery solution that fits your operations.

Speak to the team

sales@macrium.com

www.macrium.com