

CIOs 30 Day DR Checklist

The 30-Day DR Checklist serves as a critical accelerator for new CIOs to rapidly evaluate and fortify their organization's IT Disaster Recovery (DR) capabilities, ensuring resilience against outages, ransomware, and other catastrophes that could cost thousands per minute in downtime. Its purpose is to compress a comprehensive DR overhaul into a tight timeline—long enough to uncover deep-seated gaps but short enough to implement fixes before the next crisis hits—transforming potential vulnerabilities into robust defenses and safeguarding your career from transition failures. In summary, the checklist breaks down into six phases: reviewing existing plans (Days 1-3), inventorying assets and dependencies (4-7), assessing risks (8-12), testing and validating (13-20), updating with training (21-27), and finalizing for go-live (28-30), drawing on Erwood Group's battle-tested strategies to achieve up to 40% faster recovery times and minimize multimillion-dollar risks.

1. REVIEW THE DR PLAN

- ☐ Does it exist? Is it in a binder, electronic, both? Is the documentation consistent across the org?
- ☐ Skim for basics What's the RTO (Recovery Time Objective)? RPO (Recovery Point Objective)? RTA?
- ☐ Cross-reference against real assets. Look for gaps. Are the RTOs Test and Achievable?
- ☐ Document findings Flag high-priority holes

2. INVENTORY ASSETS & DEPENDENCIES

- ☐ Map every critical system - Utilize CMDB if available - otherwise fire up Excel
- ☐ Find Dependencies Does your ERP rely on a third-party API that goes down during peak hours?
- ☐ Prioritize. More importantly, De-prioritize everything that is not Tier 1 or Tier 2.
- ☐ Map Data Flows, create visual maps and share findings

3. ASSESS RISKS & VULNERABILITIES

- ☐ Gather your top lieutenants and run a tabletop exercise. Assume everything breaks tomorrow.
- ☐ Cyber threats check your backups for immutability and that they're air-gapped.
- ☐ Natural disasters - What can impact you? Are you geo-redundant?
- ☐ Quantify Downtime Costs - Business case for protecting critical systems and applications.

4. TEST & VALIDATE THE PLAN

- ☐ Initiate DR Plan Validations - Look for gaps, failures, documentation. Who stands out?
- ☐ Failover drills - switch to backups. Time them. Are they documenting properly?
- ☐ Restore tests - Backup validity. Look for corrupted versus immutable backups.
- ☐ Vendor involvement. How dependent are you on vendors?

5. UPDATE, TRAIN & COMMUNICATE

- ☐ Update the plans. Tighten RTOs, add automation (e.g. scripts for auto-failover).
- ☐ Hold role-based sessions. Everyone participates, everyone gets trained.
- ☐ Drills for all: Make it mandatory. Emphasize buy-in, Training.
- ☐ Communication protocols. Create or update the playbook. Use templates.

6. FINAL REVIEW & GO-LIVE

- ☐ Circle back: Re-review the updated plan against original gaps.
- ☐ Get sign-offs from Owners and Managers.
- ☐ Include stakeholders - CFO for budget implications, CEO for alignment.
- ☐ Set recurring cadence: Quarterly tests, annual audits. DR Life-cycle.

Follow this checklist for deep insights into your company's DR in 30 days or less.

Ready to accelerate without the pitfalls? Erwood Group offers an exclusive 90-Day CIO Advisory Accelerator: Personalized guidance from our veteran strategists, including weekly check-ins, custom audits, and on-demand crisis simulations. Plus, extended support into year one for seamless scaling. Valued at \$50K, yours for \$25K if you book before year's end. No fluff, just results.