How to Switch IT Providers Without Losing Your Mind

A Step-by-Step Checklist

Everything you need to know before, during, and after switching managed IT providers
— so nothing falls through the cracks.

Why This Guide Exists

Switching IT providers feels like defusing a bomb. One wrong move and your email goes down, your files vanish, or your entire team is locked out of everything on a Monday morning. No wonder most businesses stay with a bad provider way too long.

But here's the truth: a well-planned transition is straightforward. The horror stories happen when people wing it — or worse, when they let their outgoing provider control the timeline.

This checklist breaks the entire process into three phases: Before You Switch, During the Transition, and After Onboarding. Each phase has specific, actionable items you can check off as you go. We've also included a section on common pitfalls (because we've seen them all) and a timeline template to keep everything on track.

Whether you're actively looking for a new IT partner or just starting to think about it, this guide will make sure you don't lose your mind — or your data — in the process.

How to Use This Checklist

Work through each phase in order. Check off each item as you complete it.

Don't skip ahead — the order matters. Share this with your team so everyone's aligned.

01 PHASE 1: BEFORE YOU SWITCH

Get your house in order before you talk to anyone new.

☐ Review your current IT contract for termination clauses, notice periods, and data ownership terms

☐ Document all recurring charges and what you're actually paying for (licenses, support, hardware leases)

☐ Request a full inventory of your IT assets from your current provider (devices, servers, cloud subscriptions)

☐ Verify who owns your domain name(s) and confirm you have registrar login credentials

☐ Confirm you have admin access to your DNS records (or know who does)

☐ Verify ownership and admin access to all Microsoft 365 / Google Workspace accounts

☐ Collect all credentials, passwords, and MFA recovery codes your current provider manages for you

☐ Identify all third-party vendor relationships your IT provider manages on your behalf

☐ Document any custom applications, scripts, or integrations your provider built or maintains

☐ Back up all critical data independently — don't rely on your outgoing provider's backups

☐ Identify your "don't break" systems: what absolutely cannot go down during the transition?

☐ Set a realistic transition timeline (plan for 30–60 days minimum)

02 PHASE 2: DURING THE TRANSITION

Execute the handoff cleanly. Communication is everything.

- [ ] Give written notice to your current provider per your contract terms

- [ ] Introduce your new provider to your outgoing provider (yes, they need to talk to each other)

- [ ] Transfer domain registrar access to your new provider or to your direct control

- [ ] Transfer DNS management and verify all records are correct before and after

- [ ] Migrate email systems with zero downtime — verify mail flow before cutting over

- [ ] Transfer admin access for Microsoft 365 / Google Workspace to your new provider

- [ ] Hand over firewall, VPN, and network equipment credentials and configurations

- [ ] Transfer all server access, cloud hosting credentials, and remote management tools

- [ ] Migrate backup systems and verify at least one successful backup under the new provider

- [ ] Update all third-party vendor contacts to point to your new IT provider

- [ ] Remove your outgoing provider's remote access tools and accounts from all devices

- [ ] Change all shared passwords, admin credentials, and service account passwords

- [ ] Test every critical system before signing off on the transition

03 PHASE 3: AFTER ONBOARDING

Make sure the new relationship starts on solid ground.

☐ Confirm your new provider has documented your entire network environment

☐ Verify that monitoring and alerting is active on all critical systems

☐ Confirm backup schedules are running and tested under the new provider

☐ Ensure MFA is enabled across all critical business accounts

☐ Schedule a 30-day check-in to review how the transition went

☐ Verify your old provider no longer has access to any of your systems

☐ Request a technology roadmap or strategic plan from your new provider

☐ Confirm you have a clear escalation path and SLA in writing

☐ Set up regular quarterly business reviews with your new provider

☐ Collect feedback from your team — are response times and communication better?

Common Pitfalls to Avoid

Letting your old provider control the timeline

They have zero incentive to make this easy for you. Set firm deadlines, put them in writing, and hold them to it. If they drag their feet, escalate.

Not verifying domain and DNS ownership first

This is the #1 thing that goes wrong. If your old provider registered your domain under their account, you could lose access to your website and email. Verify this before you do anything else.

Skipping the credential audit

If your outgoing provider has passwords you don't, you're at their mercy. Get every credential documented and transferred before the relationship ends.

Rushing the transition

A 30–60 day transition window is standard. Trying to switch in a week is how things break. Give your new provider time to do it right.

Forgetting to remove old remote access tools

Your old provider likely has remote management software on every device. If you don't remove it, they still have access to your network. That's a security risk you can't afford.

Not changing shared passwords after the switch

Every password your old provider knew needs to change. Every one. This includes Wi-Fi passwords, admin accounts, vendor portals, and service accounts.

Assuming your old backups will just keep working

Backup systems managed by your old provider will stop working when they revoke access. Your new provider needs to set up and verify backups independently before the old ones go away.

Transition Timeline Template

Use this as a starting point. Every transition is different, but this gives you a realistic framework. Fill in your actual dates and adjust as needed.

WEEK 1–2   Planning & Preparation

- ☐ Review current contract and give written notice   Date: _____
- ☐ Audit all credentials, domains, DNS, and vendor relationships   Date: _____
- ☐ Select and sign with your new IT provider   Date: _____
- ☐ Back up all critical data independently   Date: _____

WEEK 3–4   Handoff & Migration

- ☐ Introduce old and new providers; begin credential transfer   Date: _____
- ☐ Migrate email, domain, DNS, and cloud services   Date: _____
- ☐ Transfer network equipment access and configurations   Date: _____
- ☐ Begin removing old remote access tools   Date: _____

WEEK 5–6   Verification & Cutover

- ☐ Test all critical systems under new provider management   Date: _____
- ☐ Verify backups, monitoring, and alerting are active   Date: _____
- ☐ Change all shared and admin passwords   Date: _____
- ☐ Update third-party vendor contacts   Date: _____

WEEK 7–8   Stabilization & Review

- ☐ Confirm old provider access is fully revoked   Date: _____
- ☐ Conduct 30-day check-in with new provider   Date: _____
- ☐ Collect team feedback on response times and communication   Date: _____
- ☐ Request technology roadmap and strategic plan   Date: _____

Ready to Make the Switch?

Switching IT providers doesn't have to be painful. We've helped dozens of businesses in Toledo make the transition smoothly — and we'd be happy to walk you through what your specific switch would look like.

We'll review your current setup, identify potential landmines, and give you an honest assessment — no pressure, no obligations. Just clarity.

SCHEDULE A FREE CONSULTATION

flyght.support/contact

(419) 670-7100

support@flyght.support

7430 W Central Ave., Toledo, OH 43617