A PRACTICAL GUIDE FOR BUSINESS LEADERS

How to Switch Managed IT Providers Without Disrupting Your Business

Changing IT partners can feel risky. With the right planning, clear ownership, and a structured handoff, you can reduce disruption while setting your organization up for more dependable support.

THE GOAL	Maintain business continuity, protect access and data, and make the new provider accountable for a well-documented transition.

01 Define what needs to change

Document recurring service issues, unmet expectations, security concerns, response times, and business priorities. Decide what success should look like with your next MSP.

02 Review your current agreement

Confirm notice periods, renewal dates, termination provisions, service ownership, and any fees. Involve your legal or procurement team as needed.

03 Inventory systems and access

Create a working inventory of devices, cloud services, applications, licenses, domains, backups, network equipment, vendor contacts, and privileged accounts.

04 Build a joint transition plan

Agree on milestones, responsibilities, communication channels, support coverage, escalation paths, and a realistic cutover schedule before making changes.

05 Transfer knowledge and validate

Securely transfer documentation and credentials, test backups and restore procedures, verify monitoring and security controls, and confirm critical services function.

06 Stabilize and measure

Run a post-transition review, resolve outstanding tickets, verify access changes, and measure service against agreed expectations.

YOUR TRANSITION READINESS CHECKLIST

Before You Make the Switch

Use these checkpoints to guide conversations with your current provider and prospective MSP.

Contracts and timing	Notice requirements, contract end date, termination fees, and vendor dependencies are understood.
Ownership and access	Administrative access, domain ownership, cloud tenants, licenses, and key accounts are documented.
Documentation	Network diagrams, asset inventory, vendor contacts, configurations, and open issues are available.
Security and recovery	MFA, endpoint protection, backup status, recovery testing, and security responsibilities are reviewed.
Cutover and communication	A named transition lead, escalation plan, staff communications, and rollback options are established.
Acceptance criteria	The new provider will validate service desk access, monitoring, backups, critical apps, and security controls.

Questions to ask a prospective MSP

Who owns the transition plan? How will you prevent downtime? What access and documentation will you need? How will security and backups be verified? What does support look like in the first 30 days?

READY TO DISCUSS YOUR OPTIONS?

CCS can help you assess your current IT challenges and plan a thoughtful transition.
customonline.com/switching-managed-it-providers/

Planning note: Timing and responsibilities vary by environment and contract. Avoid canceling critical services until replacement coverage and access are confirmed.