ELEVATE
SOLUTIONS

GUIDE · IT STRATEGY & OPERATIONS

MSP Transition: What to Expect

Switching without downtime

Everything to know before switching IT providers — timeline, documentation handoff, red flags, and how to run a clean transition.

01 — BEFORE YOU SIGN ANYTHING

Set the exit up before you announce it

Most painful provider switches fail before they start: the contract is read too late, the incumbent holds more than anyone realized, and the announcement lands before the firm controls its own accounts. Do these four things first, quietly, in order.

The stakes are not abstract. Your IT provider holds administrative control over the systems that hold client files, patient records, and financial data. Third-party involvement doubled to 30% of breaches. Verizon DBIR 2025 A provider change is exactly the kind of third-party event where access goes unaccounted for — unless you run it deliberately.

1. Read your current contract — three clauses decide everything

Pull the signed agreement, not the proposal. Look for:

CLAUSE	WHAT TO FIND AND WRITE DOWN
Termination notice	How many days' written notice, to whom, in what form (email vs. certified mail), and whether the contract auto-renews. Many agreements renew for a full year if notice misses a 60- or 90-day window. Calendar the deadline today.
Data return & cooperation	Does the contract obligate the provider to return documentation, credentials, configurations, and backups at exit? In what format and timeframe? If the contract is silent, plan extra time — you will be negotiating cooperation, not invoking it.
Offboarding fees	Some agreements bill hourly for "transition assistance" or charge per-device de-enrollment fees. Get the number in writing before you give notice, so a surprise invoice cannot be used as leverage mid-handoff.

2. Inventory what the incumbent actually holds

Before notice goes out, list every system where the incumbent — not your firm — is the administrator or account owner. The big four to confirm first: global admin on your Microsoft 365 or Google Workspace tenant, your domain registrar login, your backup platform, and your software license agreements. Section 02 is the full worksheet. If the registrar account or the tenant is registered in the provider's name rather than your firm's, fixing that is your first transition task — ownership disputes are far easier to resolve while the relationship is still commercial.

3. Don't announce until you're ready

Give notice only after you have: (a) the contract deadlines mapped, (b) the access inventory drafted, © a new provider selected with a written onboarding plan, and (d) at least one administrator credential per critical system held by someone on your own staff. Most outgoing providers behave professionally. You plan for the one that doesn't.

4. Budget for overlap

A clean transition usually means paying two providers for 30–60 days: the incumbent through the notice period, the new provider from onboarding day one. Treat the overlap as the cost of continuity, not waste — it buys you a working fallback while access transfers, and it removes the temptation to cut the handoff short. Build it into the year's budget before you sign the new agreement.

> **ONE RULE ABOVE ALL**
>
> Your firm — not any provider, old or new — should be the registered owner of your domain, your tenant, and your data. A transition is the moment to make that true if it isn't already.

02 — DOCUMENTATION TRANSFER

The handoff list: 24 items, verified one by one

This is the heart of the transition. For each item, record who currently holds it, then have someone — your staff or the new provider — log in or open the file and confirm it works before you mark it verified. "We sent the spreadsheet" is not verification. A successful login is.

A · IDENTITY & CONTROL OF RECORD

ITEM	CURRENT HOLDER	VERIFIED (DATE / INITIALS)
Tenant global admin — Microsoft 365 / Google Workspace, with break-glass account credentials		
Domain registrar account — login, registered owner shown as your firm, transfer lock status		
DNS zone control — where records are hosted; export of all current records (MX, SPF, DKIM, A, CNAME)		
SSL/TLS certificates — issuing accounts, expiry dates, private keys where applicable		
Credential vault / password manager — full export of accounts the provider manages on your behalf		
MFA recovery — recovery codes and registered devices for every admin account being handed over		

B · NETWORK & INFRASTRUCTURE

ITEM	CURRENT HOLDER	VERIFIED (DATE / INITIALS)
Firewall admin access — plus a current config backup and any vendor support contract		
Switches & Wi-Fi controllers — admin credentials, controller/cloud account ownership		
Server & hypervisor admin — local admin, domain admin, vCenter/Hyper-V, out-of-band (iLO/iDRAC)		
VPN & remote access — configurations, certificates, who currently has remote access and how		
Network documentation — diagram, IP scheme, VLANs, ISP handoff points, site-to-site links		

ISP & circuit accounts — account numbers, who is authorized to call in, contract end dates

C · DATA, ENDPOINTS & SECURITY TOOLING

ITEM	CURRENT HOLDER	VERIFIED (DATE / INITIALS)
Backup platform — console access, job history, retention settings, and the date of the last tested restore		
RMM / endpoint management — agent inventory; written plan and date for removing the incumbent's agents		
EDR / antivirus console — tenant ownership, exclusion lists, alert history export		
MDM / mobile management — enrolled device list, Apple Business Manager / Android Enterprise ownership		
Email security gateway — admin access, mail-flow rules, quarantine policies, allow/block lists		
File storage admin — file servers, SharePoint/Drive admin, external sharing settings, permission map		

D · RECORDS, LICENSES & VENDORS

ITEM	CURRENT HOLDER	VERIFIED (DATE / INITIALS)
Hardware asset inventory — make, model, serial, location, warranty status for every device		
Software licenses & agreements — keys, license counts, renewal dates, and whose name the agreements are in		
SaaS admin inventory — every application where the provider holds an admin or billing role		
Vendor contacts & account numbers — phone system, copier/print, line-of-business software, ISP, hosting		
Ticket history export — at minimum the last 12 months; recurring issues are your new provider's starting map		
Compliance evidence — security policies, audit logs, training records, prior assessments held by the provider		

SEQUENCE MATTERS

Transfer group A first. Once your firm controls identity, the registrar, and DNS, every other item can be recovered with patience. Until then, every other item depends on the incumbent's goodwill.

Handoff coordinator (your firm) _____

Target date — all 24 items verified _____

03 — TRANSITION TIMELINE

30 / 60 / 90 days, with a gate at each step

A realistic transition runs about ninety days from the new provider's start date. The work below is the buyer's checklist, not the provider's marketing plan — at each gate, you decide whether the milestone is actually met before the next phase starts.

WINDOW	CORE WORK	GATE — WHAT "GOOD" LOOKS LIKE
Days 1–30	Discovery and access transfer. The new provider inventories every system, completes the Section 02 handoff list, deploys its monitoring and management agents, and documents what it finds — including the gaps. Incumbent access is revoked item by item as each transfer is verified, with shared and service-account passwords rotated.	All 24 handoff items verified. Incumbent admin access fully revoked and credentials rotated. Monitoring live on every server and workstation. A written discovery report in your hands, including what could not be recovered.
Days 31–60	Standardization and security baseline. Patching brought current; MFA enforced on all admin and remote access; backups re-pointed, retention confirmed, and a test restore performed; endpoint protection consistent across the fleet; documentation rebuilt from the discovery findings rather than inherited as-is.	A dated test-restore record you can show an auditor or insurer. MFA coverage report. Patch status report with exceptions explained. Documentation your own staff can read — not locked in the provider's head.
Days 61–90	Steady state. Ticket flow settles into the agreed support process; recurring issues from the incumbent's ticket history are triaged into fix-now versus roadmap; the first quarterly business review is held with a 12-month plan covering refresh, security work, and compliance deadlines.	First QBR completed, with a written roadmap and budget figures attached. Open items from days 1–60 closed or scheduled with dates. You know exactly how to open a ticket, escalate one, and reach a human after hours.

What "without downtime" actually means

Switching providers does not require migrating your email, your files, or your line-of-business systems — those stay where they are. What changes hands is administration. The user-visible events are small and schedulable: an agent install, a password rotation, possibly a brief firewall maintenance window. Anything bigger than that should be a separate, scoped project with its own plan — not smuggled into the transition.

Hold the gates

The most common transition failure is soft gates: standardization begins while three handoff items are still "in progress," and ninety days later nobody can say who controls the registrar. Keep a one-page tracker. At each gate, the open items are either closed or escalated under Section 04 — never quietly carried forward.

New provider start date _____

Gate review dates (30 / 60 / 90) _____

04 — RED FLAGS & ESCALATION

Fourteen warning signs — and what to do about them

Both providers in a transition should be held to written, checkable standards. The first list protects you from a difficult exit. The second list is the test you should apply to anyone you hire next — including the firm whose logo is on this document.

Incumbent red flags

- [ ] **Credential withholding** 1
  Admin passwords arrive late, incomplete, or "after the final invoice clears." Access to your own systems is not a payment dispute lever — put the request in writing and start the escalation clock.
- [ ] **"You don't own that tenant"** 2
  The M365/Google tenant, domain, or software agreements turn out to be registered to the provider. Common, and recoverable — but it must be the first thing you fix, in writing.
- [ ] **Surprise offboarding fees** 3
  Charges that appear only after notice is given and were never in the signed agreement. Ask for the contract clause that authorizes each line item.
- [ ] **No documentation to hand over** 4
  Years of service and nothing written down. You cannot fix that now — but it changes the plan: budget more discovery time in days 1–30 and verify everything independently.
- [ ] **Stalling past the notice period** 5
  Meetings rescheduled, single points of contact on leave, items perpetually "next week." Escalate from technician to owner, in writing, with dates.
- [ ] **Backups go quiet** 6
  Backup jobs stop, retention is shortened, or console access is cut during the notice period. Treat this as urgent: verify backup status independently the week notice is given, and weekly after.
- [ ] **Lingering access after exit** 7
  Remote-access tools, admin accounts, or mail-forwarding rules still active after the handoff date. The day-30 gate includes a sweep for exactly this.

New-provider red flags

- [ ] **No documented onboarding plan** 8
  A provider that cannot show you a written transition plan — phases, owners, dates — before you sign will not produce one after. Ask for it during the sales process.
- [ ] **No security baseline commitment** 9
  No stated standard for MFA coverage, patching cadence, backup testing, and endpoint protection — or no date by which your environment will meet it.

- [ ] **All-verbal promises** 10
  Scope, response expectations, and deliverables discussed at length but absent from the agreement. If it mattered enough to say, it matters enough to write down.
- [ ] **Vague scope boundaries** 11
  No clear line between what the monthly fee covers and what is billed as a project. Ambiguity here is where invoice disputes are born.
- [ ] **No exit terms of their own** 12
  Their contract is silent on what they return to you — documentation, credentials, configurations — when this relationship someday ends. You are reading this guide because that clause matters.
- [ ] **Documentation they won't share** 13
  The provider rebuilds your network documentation, then treats it as proprietary. Your environment's documentation belongs to you; confirm that in writing before day one.
- [ ] **No visibility into your own tickets** 14
  You should be able to see open tickets, their status, and history at any time. A provider that won't show its work is asking for trust it hasn't earned.

Escalation paths, in order

STEP	WHAT TO DO
1. Contract	Send a written request citing the specific clause (data return, cooperation, termination assistance) with a response deadline of 5–10 business days. Most disputes end here once the obligation is quoted back.
2. Platform recovery	For tenant and domain disputes, the platforms have owner-recovery processes that do not require the incumbent's cooperation: Microsoft and Google both verify business ownership (domain control, billing records, business registration) to reassign tenant admin; ICANN's transfer dispute process and the registrar's own ownership-verification process cover domains. These take weeks — start them early, in parallel with step 1, if signals are bad.
3. Counsel	If credentials or data are still withheld, this stops being an IT problem. A demand letter from your attorney — referencing the contract and, where relevant, your regulatory obligations to control client or patient data — changes the conversation quickly. For regulated firms, document the timeline as you go; you may need to show a regulator you acted diligently.

> **KEEP PERSPECTIVE**
> Most transitions are uneventful. Professionals hand over cleanly, and the escalation table goes unused. The point of this guide is that you should never have to rely on that.

Elevate Solutions provides managed IT and cybersecurity for businesses that answer to regulators, clients, and courts.

Elevate Solutions

6230 Wilshire Blvd Suite 2120, Los Angeles CA 90048

(424) 400-6625 · support@elevatesolutions.io · elevatesolutions.io