ninjaOne

The MSP M&A Playbook

A framework for evaluating, consolidating, and integrating acquired environments

The mergers and acquisitions landscape

According to Omdia's MSP Trends and Predictions report, approximately three-quarters of MSP-related deals tracked in 2025 were funded by private equity investors, and mergers and acquisitions (M&A) activity is expected to grow another 16 percent in 2026.

As deal volume grows, so does integration complexity. The MSPs widening their margins are the ones with platforms built to absorb acquired environments at the same pace that they close deals. The ones carrying operational debt are the ones that signed without a clear integration plan.

Where acquisitions typically go wrong

Most acquisition problems originate in three areas that due diligence rarely covers in enough detail.

The inherited tech stack

Acquiring MSPs inherit a different RMM, a different patch policy, a different backup configuration, and a technical team that knows their tools and nobody else's. The new environments run on different tools, different policies, and different configurations. When a client of the acquired MSP has a problem, your team is navigating a foreign environment under pressure.

The assumed security posture

Most security failures in an acquired environment start with basics that were not transferred, such as a patch policy that was not migrated, a backup that was not verified, or an endpoint that fell off the radar during the transition.

The security posture of the acquired business becomes your responsibility the moment the deal closes. What you assumed was managed may not have been.

The accelerating operational debt

Tool sprawl accelerates post-acquisition. The average MSP already runs multiple vendors for RMM, patching, backup, and security, and every new company acquired increases this. For MSPs managing three or more acquired environments on disconnected platforms, that sprawl is not only a cost issue, but also starts constraining the business model. Fragmented execution, which is the same gap that costs single-environment MSPs time and margin, is repeated across every acquired environment simultaneously.

Platform readiness determines whether an acquisition accelerates or shrinks business revenue and efficiency.

How to use this playbook

This guide is written for two types of MSPs.

Currently in the middle of an acquisition

You are working with an inherited tool stack and a technical team navigating multiple consoles simultaneously

Actively acquiring

You have completed at least one deal and are planning more. Your concern is whether your platform can absorb new environments quickly enough to protect client retention and margins post-close.

Whether you are evaluating a target or stabilizing what you have already closed, this playbook gives you the questions to ask before, during, and after a deal.

Work through the checklist below and flag every statement that currently applies to the environment you are assessing. This may be a prospective acquisition target, or an environment you have already closed.

At the end of each category, note how many items you flagged.
At the end of the checklist, we will explain how to read your results.

The MSPs M&A evaluation checklist

SECTION 1: BEFORE YOU CLOSE AN ACQUISITION

Tech stack and toolset alignment

Why it matters: The tools that an acquired MSP uses are not always preferred. Understanding what is in the stack, and what it would take to retire or replace each component, is the starting point for any realistic integration timeline.

- ○ No clearly defined standard tech stack exists across core functions
- ○ Active vendor contracts limit consolidation or migration options
- ○ Platforms in active use are no longer strategically supported or actively sold
- ○ One or more tools are difficult to replace or migrate
- ○ Support knowledge for one or more platforms is concentrated in one or two individuals

Items flagged: /5

Security hygiene and operational security

Why it matters: Security controls that are locally managed rather than centrally enforced represent one of the highest-risk areas in any acquisition. What you cannot see becomes a liability when the deal closes.

- ○ Internal security policies are not consistently applied across systems and teams
- ○ Known security gaps have been accepted as risk rather than remediated
- ○ The MSP would not meet your minimum-security baseline today
- ○ Security practices depend on individual behavior rather than enforced systems
- ○ Client security requirements are stricter than the MSP's own internal practices

Items flagged: /5

Compliance obligations

Why it matters: Compliance requirements often do not transfer cleanly between organizations. Understanding which customers are subject to specific frameworks, and whether those requirements constrain your tooling or architecture decisions, matters before you finalize terms.

- ○ One or more customer accounts are subject to compliance frameworks (e.g., FedRAMP, HIPAA, SOC 2, ISO 27001)
- ○ Compliance controls are not formally documented or consistently enforced
- ○ Compliance oversight has no clear owner post-acquisition
- ○ Compliance-related costs are not reflected in customer pricing or margins
- ○ Current practices undermine auditability or regulatory requirements

Items flagged: /5

Technical currency and tech debt

Why it matters: Deferred upgrades and outdated platforms become a support burden and extend your integration timeline.

- Upgrades and modernization efforts are regularly deferred due to risk, capacity, or expertise constraints
- Customers are operating on end-of-life or unsupported systems
- Customers rely on legacy systems that actively increase support burden
- Technical debt is largely unacknowledged or unmapped
- Technical debt limits the ability to standardize across environments

Items flagged: /5

Tool supportability and legacy risk

Why it matters: Legacy platforms that require continued support are among the most difficult integration challenges to resolve quickly.

- Support knowledge for one or more platforms is concentrated in one or two individuals
- System configuration and operational knowledge is not formally documented
- Loss of key technical personnel would materially impact service continuity
- Support practices are learned informally rather than standardized
- Tools in active use are no longer sold, supported, or strategically aligned

Items flagged: /5

SECTION 2: PEOPLE AND OPERATIONS

Talent risk

Why it matters: Understanding which individuals carry critical knowledge, and whether that knowledge is documented, directly affects your integration timeline.

- Critical systems or processes depend on specific individuals to function
- Operational knowledge is not documented or transferable
- Staff retention strategies are not aligned with actual operational dependency
- Key roles could not be replaced within 90 days without significant disruption
- The business relies on individual heroics rather than repeatable systems

Items flagged: /5

Operational maturity

Why it matters: Documented, consistently followed processes are much easier to change than institutional memory.

- Operational variance across teams or locations introduces integration risk
- Documentation exists but is not current, accessible, or used in practice
- Escalations are handled ad hoc rather than through a predictable process
- Core processes break under growth or staff turnover
- Different operational entities run in meaningfully different ways

Items flagged: /5

Service delivery efficiency

Why it matters: Service delivery that varies by team or individual rather than by documented process is difficult to standardize at scale.

- Service delivery practices vary significantly across teams or locations
- Ticketing and service metrics do not provide clear visibility into throughput or bottlenecks (aging tickets, reopens, escalations)
- Ticket reopen rates or escalation frequency are trending upward
- Service levels are maintained through short-term workarounds rather than sustainable practices
- Reactive, incident-driven work consistently crowds out proactive or preventive activity

Items flagged: /5

SECTION 3: COMMERCIAL AND STRATEGIC FIT

Products, services and offering consolidation

Why it matters: Overlapping or redundant offerings create delivery complexity. Understanding which services you are acquiring, and which you would rather not own, matters before closing.

- Services are heavily customized on a per-customer basis rather than standardized
- Certain services create disproportionate delivery complexity relative to their revenue contribution
- Overlapping or redundant offerings exist with no consolidation plan post-acquisition
- One or more offerings are priced below their true delivery cost
- Services that would not be sold today are included in the active portfolio

Items flagged: /5

Commercial practices and customer profitability

Why it matters: Aggregate revenue figures do not tell you which customers are profitable. Understanding the composition of the customer base, including inherited pricing exceptions and accounts that constrain your decisions, can affect how you model a deal.

- Pricing exceptions are common and not formally governed
- Certain customers materially constrain operational or technology decisions
- Inherited contracts carry structurally poor margins
- Renewals are routinely renegotiated rather than renewed predictably
- Customer-level profitability is not tracked or understood

Items flagged: /5

Customer and account risk

Why it matters: Revenue concentration and customer satisfaction can materially change the value of what you are acquiring after close.

- Customer satisfaction outcomes vary significantly across accounts
- One or more customers would resist future standardization efforts
- One or more accounts would not be pursued under your current acquisition criteria
- Satisfaction levels depend on specific individuals rather than consistent service delivery
- SLAs are not consistently achievable across the account base

Items flagged: /5

Market and competitive landscape

Why it matters: Understanding the competitive dynamics of the market you are entering helps you assess whether the acquired revenue and customer base will remain stable through the transition.

- ○ The market is highly competitive with strong regional or vertical alternatives
- ○ Margins are under active pressure from competitive dynamics
- ○ Future growth is constrained by market maturity or saturation
- ○ Differentiation is based primarily on personal relationships rather than documented capability
- ○ The MSP's competitive differentiation is not clearly understood internally

Items flagged: /5

Sales and growth engine maturity

Why it matters: Revenue generated primarily by the owner or a small number of key individuals may not transfer with the business.

- ○ New business is primarily driven by the owner or a small number of individuals
- ○ Sales processes are not documented or consistently followed
- ○ No CRM system is actively used for pipeline management or forecasting
- ○ Growth depends primarily on referrals with no additional acquisition channels
- ○ Forecasting and pipeline practices are inconsistent or informal

Items flagged: /5

SECTION 4: INTEGRATION READINESS

M&A integration approach and operating model

Why it matters: Whether the acquiring MSP has a defined integration framework is one of the strongest predictors of how cleanly a deal will run.

- ○ No defined acquisition and integration framework exists
- ○ Decision rights for pre-close versus post-close actions are undefined
- ○ Previous integration failures have not been formally addressed or documented
- ○ No clear timeline or plan exists for establishing operational control post-close
- ○ Each deal is handled differently with no repeatable integration approach

Items flagged: /5

Hosting and infrastructure footprint

Why it matters: Hosted infrastructure can be a strategic revenue driver or an inherited operational liability.

- ○ The organization operates datacenters or hosted infrastructure with unclear strategic purpose
- ○ Hosting revenue represents a significant portion of total revenue with unclear margins
- ○ Responsibility for hosted environment maintenance is not clearly defined
- ○ Infrastructure changes would materially affect customer SLAs or contractual commitments
- ○ Hosting exists as a legacy carryover rather than a strategic revenue driver

Items flagged: /5

Interpreting your results and next steps

Congratulations on finishing the checklist. You should now have a score for each of the 15 categories.

HERE'S HOW TO INTERPRET YOUR RESULTS:

Scoring

Fewer than a third of items flagged = low risk.
Document your findings and continue diligence or integration planning.

A third to half of items flagged = moderate risk.
Plan remediation steps before closing any acquisitions, or factor them into your integration sequence post-close.

More than half the items flagged = high risk.
Being in this category warrants a dedicated conversation, either before you sign any acquisitions or as an immediate integration priority.

Red flags: Categories that carry disproportionate deal risk

Three categories require attention regardless of their raw score.

1. **Security hygiene and operational security**
   Any flag in shared credentials, absent MFA, or unverified backups is a remediation priority. These are active liabilities that you own from day one.
2. **Talent risk**
   Key-person dependency concentrated in one or two individuals is a huge risk. Factor retention requirements into deal structure before you sign or proceed further.
3. **Technical currency and tech debt**
   Customers on end-of-life systems and routinely deferred upgrades will add directly to your support burden. Quantify this before you finalize acquisition terms, as it's easier to price in pre-close than to absorb post-close.

Practical next steps

Pre-close : Use your highest-scoring categories to structure your remaining diligence conversations. Any category where more than half the items applied is a candidate for deal term adjustments, phased integration requirements, or additional scrutiny before you proceed.

Post-close : Start with your highest-scoring categories. These represent the greatest pressure on client retention and operational stability. Work through them in sequence, with the highest concentration first.

How NinjaOne helps MSPs with M&A

From the moment a deal closes, the NinjaOne platform standardizes policies, deploys automation, and brings acquired endpoints under unified management. Ninety-two percent of MSPs are fully operational on NinjaOne in under 30 days, backed by free, unlimited onboarding, training, and migration support. New technicians are productive in hours, with eighty-nine percent of MSPs reporting it takes under 6 hours to onboard new technicians.

Partners typically replace 4 or more tools with the NinjaOne platform. A centralized hierarchical policy engine applies monitoring, patching, backup, and security configurations across acquired environments simultaneously. The platform supports 100,000+ endpoints per tenant without console sprawl, ensuring growth without limits.

MSPs using NinjaOne grow 3 times faster than the industry average. Your platform is ready when you are.

MSP success stories

Techvera | 23,500+ endpoints

Consolidated tool sprawl from years of acquisition-driven growth into a single platform. Saved over $1 million in hard costs across platforms, time spent, and capacity expansion.

> "It's more than an RMM. NinjaOne is an innovation-driven platform where we can confidently centralize IT ops as we scale."
>
> **Bill Tyndall, CEO, Techvera**

ERGOS Technology Partners | 40,000+ endpoints

Consolidated five legacy RMMs into one platform and migrated 40,000+ endpoints with zero downtime. Patching time reduced from several hours to under one hour.

> "We couldn't just solve for 30 or 40,000 endpoints. We had to solve for 100,000 as we kept growing."
>
> **Chris Amalfi, VP of Operations, ERGOS Technology Partners**

Babble

Retired five legacy tools at once and now onboards acquired companies directly into a unified toolset. Improved security and compliance for regulated clients.

> "When we started acquiring companies it became obvious that NinjaOne was the platform we wanted everyone on."
>
> **Chris Baker, Infrastructure and Systems Lead, Babble**