7 critical red flags to watch out for when choosing an MSP

For many small and midsize businesses (SMBs), partnering with a managed service provider (MSP) is essential to maintaining security, uptime and operational continuity.

A capable MSP reduces risk, strengthens resilience and supports business growth. But the wrong provider can quietly introduce vulnerabilities — both operational and financial — that aren't immediately visible.

If you already know what you need from an MSP, the next step is recognizing early warning signals that indicate a provider may introduce risk rather than reduce it. Some risks may be minor operational issues, while others can have significant business impact.

Red flags should focus first on critical indicators such as missing essential protections and signs of limited operational maturity.

Critical red flags (deal-breaker risks)

These signals indicate structural gaps that directly affect security, recovery and control:

1. Security positioned as optional rather than foundational

The red flag:

The MSP presents cybersecurity capabilities as add-ons instead of capabilities embedded into the core service model.

Why it's risky:

Providers that separate monitoring, protection and response often rely on fragmented toolsets, which limits unified threat visibility.

What strong providers demonstrate instead:

Integrated security operations spanning monitoring, patching, identity protection and incident response as standard service layers.

2. Incident response confidence without operational proof

The red flag:

The MSP claims incident response capability but cannot clearly demonstrate how detection, escalation and containment processes operate in practice.

Why it's risky:

During ransomware or breach scenarios, response speed and coordination determine business impact. Undefined workflows increase the likelihood of extended downtime and unnecessary data exposure.

What strong providers demonstrate instead:

Documented response frameworks, defined escalation paths and real operational readiness, not theoretical capability.

3. Backup assurances without recovery validation

The red flag:

Backups are confirmed, but recovery timelines, testing frequency or restoration scope remain unclear.

Why it's risky:

Backups that are not regularly tested often fail to perform as expected during real incidents.

What strong providers demonstrate instead:

Regular recovery testing, scenario-based restoration exercises and clearly communicated recovery expectations.

4. Administrative control retained by the provider

The red flag:

The MSP maintains exclusive ownership of privileged access, credentials or environment administration.

Why it's risky:

This creates operational dependency and increases vendor lock-in risk, particularly during contract transitions or incident disputes.

What strong providers demonstrate instead:

Customer-retained ownership of administrative access, credential transparency and auditable governance controls.

5. Human availability remains unclear

The red flag:

Support appears comprehensive, but guaranteed human response during critical incidents is undefined.

Why it's risky:

Automated ticketing alone cannot resolve outages or contain security incidents. Delayed human availability amplifies operational and financial impact.

What strong providers demonstrate instead:

Contracted response expectations, live escalation coverage and clearly defined incident prioritization.

Operational red flags (service delivery risks)

These indicators affect day-to-day reliability and operational experience:

6. Reactive service model (“break-fix” delivery)

The red flag:

The MSP primarily engages after issues occur rather than preventing them proactively.

Why it’s risky:

Reactive providers often emphasize ticket closure over risk reduction, which can lead to recurring issues, degraded performance and avoidable downtime.

What strong providers demonstrate instead:

Preventative maintenance, continuous monitoring, risk reporting and environment health management.

7. Operational knowledge concentrated within the provider

The red flag:

Documentation, network visibility, asset inventories and environment knowledge are not transparently shared with the customer.

Why it’s risky:

When operational knowledge is concentrated within the provider, transitions become more difficult, recovery slows and vendor dependency increases.

What strong providers demonstrate instead:

Shared documentation, accessible environment mapping and collaborative operational transparency.

Moving from warning signs to structured evaluation

These red flags align with the key risk domains SMBs should evaluate when selecting an MSP, including security readiness, incident response capability, recovery resilience and operational control.

If any of these signals emerge during provider discussions, treat them as prompts to investigate further, request operational evidence and validate governance safeguards.

Make risk-aware, not assumption-based, decisions

Choosing an MSP is ultimately an assessment of risk, not just a comparison of service offerings.

A mature provider reduces exposure across cyberthreats, downtime and compliance obligations. The wrong provider can introduce structural risks that only become visible during

Let Acronis help you find an MSP

The Acronis Partner Locator helps you identify qualified MSPs, explore service offerings and find the right fit for your business.

Find a Partner