Acronis

GUIDE

How to choose an MSP: A guide for SMBs

A practical checklist to help SMBs evaluate service providers, assess risk and capabilities and make informed decisions.

Table of contents

Built on Decades of Real-World MSP Experience

More than 20,000 managed service providers (MSPs) worldwide trust Acronis to provide an integrated technology platform they use to serve their clients. Acronis has decades of experience working with MSPs and direct visibility into how they operate.

Across industries, regions and delivery models, Acronis closely observes which MSP practices ensure strong security and stability, and which gaps can lead to security incidents, downtime, failed transitions or vendor lock in.

This guide translates those real-world insights into a practical evaluation framework that helps SMBs make risk-aware decisions and avoid common pitfalls.

Why choosing an MSP is a critical decision

For SMBs, an MSP is more than just a provider of IT services. Your MSP should be a trusted partner and your first line of defense against cyberthreats and operational disruption. Consider the risks small businesses face:

- 46% of small businesses have experienced a cyberattack.[1]
- Nearly 20% of businesses that suffered an attack filed for bankruptcy or closed.[2]
- 200% year-over-year growth in ransomware attacks (2024–2025).

Choosing the wrong MSP can lead to:

- Data loss and security incidents.
- Compliance failures.
- Prolonged downtime.
- Unexpected costs.
- Frequent and risky service provider transitions.

What an MSP should deliver

A qualified MSP helps your business:

Strengthen cybersecurity: Protect against ransomware, phishing and data breaches.

Reduce operational costs: Improve operations without needing a full internal IT team.

Improve productivity: Achieve faster issue resolution and decrease downtime.

Scale safely: Grow your business with targeted IT services.

Meet compliance requirements: Comply with GDPR and industry-specific regulations.

Optional expert guidance:

If you would like help finding the right MSP, you can schedule a free consultation with an Acronis expert to clarify key risk areas, understand tradeoffs and ensure you know how to find service gaps — all with no obligation and no sales pressure.

Book a Consultation

[1] Gerber, Johan and Prokop, Jane. “Small business cybersecurity study.” Mastercard, March 27, 2025. https://www.mastercard.com/global/en/news-and-trends/stories/2025/small-business-cybersecurity-study.html

[2] Ibid.

Structured MSP interview

Structured MSP interview

Questions about real operational maturity

Use the interview sections below to guide structured conversations.

Each section focuses on a specific risk domain and helps you understand not just what an MSP offers, but how the MSP delivers it.

Best practice:

Interview at least three MSPs (ideally five).

Differences in transparency, maturity and accountability become obvious quickly.

1 Scope and service fit

Do the MSP's services actually match your needs and expectations?

? Which services do you provide specifically for SMBs?

Look for: Clearly defined services such as security, backup, disaster recovery, endpoint management and user support.

Why this matters: Claims of 'we do everything' often indicate unclear scope and potential future cost disputes.

? What is included in your standard fee, and what is considered extra?

Look for: A clear breakdown of included services, optional add ons and billable activities.

Why this matters: Unclear scope is one of the most common sources of conflict and surprise invoices.

? Do you support our current tools, systems and environment?

Look for: Explicit confirmation of supported platforms and known limitations.

Why this matters: Unsupported tools often lead to exclusions, delays or forced migrations later.

2 People and operations

Who will actually support you, and how stable is the operation?

? How is your delivery team structured, and who supports us day to day?

Look for: Named roles, clear escalation paths and transparency beyond sales.

Why this matters: You should know who will handle incidents — tnot only who manages the sales process.

? What is the average tenure of your technical staff?

Look for: Clear, confident answers rather than vague or evasive responses.

Why this matters: High staff turnover leads to slower response times and repeated mistakes.

? Do you have onboarding standards or minimum requirements for new clients?

Look for: Defined technical, security and documentation standards.

Why this matters: MSPs without standards are often overloaded and constantly firefighting.

? How long have you been operating as an MSP, and what is your team size?

Look for: Evidence of longevity and sufficient staffing coverage.

Why this matters: Longevity and adequate staffing indicate operational resilience.

3 Security operations and incident readiness

How prepared is the MSP for real incidents, not just prevention on paper?

How do you protect our business from cyberthreats?

Look for: 24/7 monitoring, MFA, patch management and proactive threat detection.

Why this matters: Basic controls prevent the most common attacks.

How do you handle security incidents and breaches?

Look for: A documented incident response process, defined roles and clear communication steps.

Why this matters: Tools alone do not stop incidents; response time and response quality determine the impact of an attack.

What is your guaranteed human response time?

Look for: A contractual commitment to human review, not just automated ticket acknowledgements.

Why this matters: Issues escalate when there is no human to review them quickly.

How do you manage access and credentials?

Look for: Individual accounts, role-based access and audit logs.

Why this matters: Shared credentials remove accountability and increase risk.

4 Data protection and incident recovery

What happens when systems fail or data is lost?

How do you back up our data and test recovery?

Look for: Automated, encrypted backups with regular recovery testing.

Why this matters: Untested backups often fail when needed most.

Which recovery scenarios do you regularly test?

Look for: Testing beyond simple file restores, including system and environment recovery.

Why this matters: Limited testing does not prepare you for real incidents.

What documentation will we receive and retain?

Look for: Network diagrams, backup procedures, incident response plans and access documentation.

Why this matters: Without documentation, recovery and transitions become slow and costly.

5 Governance, compliance and ownership

Who owns risk, responsibility and control?

Do you have experience with our industry and compliance requirements?

Look for: Demonstrated experience with relevant regulations and audits.

Why this matters: Compliance gaps often surface only after incidents or audits.

Do you provide ongoing compliance support or only one-time assessments?

Look for: Continuous monitoring, updates and guidance.

Why this matters: Compliance is ongoing, not a checkbox.

Which certifications, licenses and insurance do you carry?

Look for: Relevant certifications and professional liability or cyber insurance.

Why this matters: Without insurance, risk shifts back to your business.

Who owns administrative access and documentation?

Look for: Ownership clearly retained by the customer.

Why this matters: Lack of ownership leads to lock-in and loss of control.

6 Co-managed responsibilities

If you share IT responsibility with the MSP, are boundaries clearly defined?

Who is responsible for what in a co-managed setup?

Look for: A written responsibility matrix.

Why this matters: Undefined ownership leads to gaps and finger pointing.

❓ How are changes outside scope handled?

Look for: Clear approval workflows and escalation rules.

Why this matters: Informal changes often cause outages and disputes.

❓ How do you coordinate with our internal IT team?

Look for: Defined communication and collaboration processes.

Why this matters: Poor coordination creates delays and duplicated work.

7 Support coverage and escalation

When and how can you actually reach the MSP?

❓ What are your support hours?

Look for: Clearly defined business and non-business hour coverage.

Why this matters: Many incidents occur outside standard hours.

❓ How do you handle after-hours and emergency requests?

Look for: Transparent rules and pricing.

Why this matters: Emergency support without rules is often expensive or unavailable.

❓ What qualifies as an emergency?

Look for: Clear definitions aligned with response priorities.

Why this matters: Different interpretations delay response during critical incidents.

8 Commercial terms, SLAs, exit plan

How do you pay and how do you safely part ways if needed?

❓ Which pricing model do you use, and how does cost scale as we grow?

Look for: Transparency around pricing and total cost of ownership.

Why this matters: Some models look affordable initially but scale poorly.

❓ Can we review a draft contract, including SLAs?

Look for: Scope, service-level agreements (SLAs) and responsibilities clearly documented.

Why this matters: Contracts, not conversations, define accountability.

❓ What happens if we terminate the contract?

Look for: Guaranteed return of credentials, licenses and documented handover.

Why this matters: Inadequate exit terms can lead to downtime and vendor lock in.

Risk-based selection checklist

(Yes / No)

This checklist helps you assess risk.

How to score risk (what Yes / No really means)

Yes: The MSP meets the requirement.

No: This is a gap that introduces risk.

Assessment:

0 gaps: Acceptable risk.

1 gap: Proceed only with mitigation.

2+ gaps: High likelihood of failure.

A gap may lead to:

Security incidents.

Downtime or slow recovery.

Contractual disputes.

Loss of control or vendor lock in.

Tier 1 — Nonnegotiables (high-impact risks)

These factors directly affect security, availability and control:

- 24/7 monitoring and security coverage.
- Defined incident response process.
- Automated and regularly tested backups.
- Guaranteed human response time.
- Clear access and credential ownership.
- Clear pricing and scope boundaries.
- Documented exit and handover process.

Tier 2 — Operational reliability signals

These factors affect service quality and daily experience:

- Stable technical team.
- Clear team structure and escalation.
- Defined onboarding standards.
- Experience with similar SMB environments.
- Clear co-managed responsibilities.

Tier 3 — Governance, compliance and liability

These element are critical for regulated SMBs:

- Industry compliance experience.
- Ongoing compliance support.
- Relevant certifications.
- Professional liability and cyber insurance.
- Clear documentation ownership.

Tier 4 — Accessibility and responsiveness

These elements are critical for real-world availability:

- Defined support hours.
- Transparent after-hours rules.
- Clear emergency definitions.
- Predictable response expectations.

Tier 5 — Differentiators (value add)

Use these deciders to choose between strong candidates.

- Proactive security and IT reviews.
- Industry-specific templates or tooling.
- Peer references.
- Scalable service tiers.
- Strategic technology guidance.

Decision rule

How to choose

1. Start with Tier 1. Eliminate unacceptable risk.
2. Review Tier 2. Understand operational effort.
3. Evaluate Tier 3 based on regulatory exposure.
4. Consider availability in Tier 4.
5. Use Tier 5 to choose between viable options.

The goal:

A conscious, risk-aware decision, not necessarily a perfect checklist score.

Finding the right MSP is critical for your business

Choosing a managed service provider is one of the most important operational and security decisions an SMB can make. The right MSP strengthens your cybersecurity, improves resilience, supports compliance and helps your business scale with confidence. The wrong choice can expose you to security incidents, downtime, hidden costs and vendor lock in.

The goal is to select an MSP that reduces risk, protects your business and operates as a true long-term partner.

Let Acronis help you find an MSP

Let Acronis help you find the right MSP. Talk to an expert about key risk areas, tradeoffs and service gaps — all with no obligation and no sales pressure.

Book a Consultation

Acronis

Learn more at
acronis.com