DivergeIT
IT's in our nature

Reactive vs Ready:

The Business Leader's Guide to Managed IT and Compliance Services

By DivergeIT

Key Takeaways

Reactive IT has a cost. You just don't see it on an invoice. The average small business experiences 14 hours of IT downtime per year. At $137–$427 per minute in combined lost revenue, idle payroll, and recovery costs, that exposure adds up fast. Add the longer-term impact of customer attrition and reputational damage, and the true cost of "waiting until something breaks" consistently exceeds what a proactive IT program would cost to run.

Downtime is largely preventable and the causes are well understood. Cybersecurity incidents, human error, outdated hardware, and inadequate backup systems account for the majority of IT outages. They result from systems that aren't being monitored, maintained, and tested on a disciplined basis.

Compliance obligations are expanding, enforcement is accelerating, and mid-sized companies are not exempt. HIPAA fines can reach $2.13 million per violation category. PCI non-compliance costs $5,000–$100,000 per month and can result in losing the ability to process payments. California's privacy regulators are actively fining companies of all sizes for CCPA violations. Treating compliance as a once-in-a-while exercise is a risk posture that's increasingly difficult to defend.

Compliance is not a project. It's an ongoing program. Regulations update. Staff turns over. New vendors are onboarded. Systems change. Any of these events can open compliance gaps in an environment that passed an audit six months ago. The companies that stay out of regulatory trouble maintain continuous documentation and monitoring - not just when an audit is on the calendar.

Mid-sized companies face a structural IT challenge. The combination of growing system complexity, expanding compliance obligations, an accelerating threat landscape, and a severe shortage of qualified cybersecurity talent creates a gap that internal generalist IT teams cannot close through effort alone. This is a capacity and specialization problem and recognizing it is the first step toward solving it.

For most mid-sized companies, partnering with a managed IT provider is the more practical and cost-effective path. Building genuine internal IT capability - with 24/7 monitoring, security depth, compliance expertise, and strategic planning - requires multiple specialized headcount and significant technology investment. Managed IT services deliver all of this at a predictable monthly cost that, for most companies, compares favorably to both the cost of building internally and the cost of a single significant incident.

Not all managed IT providers are equal. SOC 2 certification, demonstrated experience in your specific industry, and current Microsoft or Google partner credentials will eliminate the majority of the market and surface the providers genuinely qualified to serve you. From there, evaluate on scope of coverage, response time commitments, compliance capabilities, and the quality of their reporting and communication. Use the Evaluation Scorecard in Section 8 to compare candidates systematically.

Table of Contents

Executive Summary

The Hidden Cost of Reactive IT: What Downtime Is Really Costing You

The Compliance Stakes: What Happens When You Fall Short

Why Mid-Sized Companies Struggle to Keep Up

From Reactive to Proactive: What a Modern IT Program Looks Like

The Business Case for Outsourcing IT: Build vs. Partner

How to Evaluate and Choose the Right Managed IT Services Provider

MSP Evaluation Scorecard

Executive Summary

Most growing companies don't have an IT strategy. They have an IT history - a series of tools adopted under pressure, problems patched after the fact, and a team stretched too thin to do anything but respond to whatever broke most recently.

It works. Until it doesn't.

The moment a server goes down during your busiest week of the year, a ransomware attack locks your team out of critical systems, or a compliance audit reveals gaps that should have been addressed years ago, reactive IT stops being an inconvenience and becomes a genuine business crisis.

This guide is for CEOs, COOs, and senior business leaders at small and mid-sized businesses (SMBs) who are asking honest questions: Is our IT infrastructure keeping up with our business? Are we managing compliance risk responsibly? And is there a smarter, more cost-effective way to handle all of this than what we're doing today?

The answers carry more urgency than you might expect, but the path forward is also more practical than you might assume.

2980 Columbia St, Torrance, CA 90503 USA

(866)216-3778

sales@divergeit.com

www.DivergeIT.com

The Hidden Cost of Reactive IT: **What Downtime Is Really Costing You**

WWW.DIVERGEIT.COM

DivergeIT
IT Solution Partner

The Hidden Cost of Reactive IT: **What Downtime Is Really Costing You**

Every business experiences IT problems. The question is whether you find out about them before or after they affect your operations. For most mid-sized companies running on reactive IT support, the answer is after, and the impact and cost is consistently underestimated.

Downtime is Expensive, and It Happens More Than Most Companies Track.

The average small business experiences approximately **14 hours of IT downtime per year.**[1] That may not sound dramatic, but consider what those hours cost:

- For small businesses, downtime runs between **$137 and $427 per minute** in combined lost revenue, idle payroll, and recovery costs - meaning a single three-hour outage can cost between $25,000 and $77,000.[2]
- 78% of SMBs say a single hour of downtime costs them over $10,000.[3]
- **57% of small businesses with 20 to 100 employees report downtime costs exceeding $100,000 per hour** during critical outages.[4]

These aren't enterprise numbers. They're the reality for companies your size.

But the Visible Costs are Only Part of the Picture.

The direct financial hits - lost revenue, idle staff, emergency recovery - are the parts that are measurable. The hidden costs are harder to quantify but often more damaging over time:

- **Customer trust-** Research from Splunk found that 29% of companies have lost customers due to downtime, and that brand reputation can take up to 60 days to recover after a major incident.[5]
- **Employee morale and productivity-** When systems are unreliable, your team spends time working around technology rather than with it. That drag compounds across every affected employee, every week. In a competitive labor market, it creates job dissatisfaction and poor morale that can impact retention.
- **Compliance exposure-** In regulated industries, downtime that affects access to protected data doesn't just disrupt operations, it can trigger a mandatory breach notification and regulatory review.

DivergeIT
IT Solution Partner

The Hidden Cost of Reactive IT: **What Downtime Is Really Costing You**

What Causes Downtime in Most Mid-sized Companies?

The leading causes are predictable and, importantly, mostly preventable with the right systems in place:

- **Cybersecurity incidents -** ransomware, phishing, and credential compromise top the list, cited by 84% of firms as their primary downtime driver.[6]
- **Human error -** misconfigured systems, accidental deletions, and process failures account for nearly 40% of major outages.[7]
- **Outdated hardware and software** - unpatched systems and aging infrastructure compound over time, creating failure points that are invisible until they aren't.
- **Lack of backup and recovery planning -** the absence of tested, current backup systems turns a recoverable incident into a multi-day crisis.

14 hrs	$427/min	**$357K+**
avg. IT downtime per year for small businesses	average cost of IT downtime per minute	potential annual exposure — before compliance risk or customer attrition

"Most small businesses aren't tracking downtime as a financial risk. By the time they are, the exposure has already compounded."

Sources: [1] Datto, cited in The Network Installers, Cost of IT Downtime Statistics, 2026
[2] Standley Systems / Sherweb, The True Cost of IT Downtime for Small Businesses, 2025
[3] Datto, cited in The Network Installers, Cost of IT Downtime Statistics, 2026
[4] ITIC / Queue-It, Cost of Downtime Statistics, 2025
[5] Splunk, cited in The Network Installers, Cost of IT Downtime Statistics, 2026
[6] ITIC 2024 Hourly Cost of Downtime Report [7] Uptime Institute, 2025 Annual Outage Analysis Report

The Compliance Stakes: What's Required and **What Happens When You Fall Short**

WWW.DIVERGEIT.COM

DivergeIT
IT Solution Partner

The Compliance Stakes: What's Required and **What Happens When You Fall Short**

For growing companies in regulated industries, IT compliance isn't optional and it isn't static. The rules are expanding, enforcement is increasing, and the consequences of falling short are no longer limited to large enterprises that make the news.

What Compliance Means in Practice

Depending on your industry and the data your company handles, you may be subject to one or more of the following frameworks:

- **HIPAA -** Applies to healthcare providers, insurers, and any business handling Protected Health Information (PHI). Requires encryption, access controls, audit trails, and breach notification protocols.
- **PCI DSS -** Mandatory for any business accepting credit card payments. Requires network security controls, encryption of cardholder data, and regular vulnerability assessments.
- **SOC 2 -** Required by many enterprise clients and government agencies as a condition of doing business. Demonstrates that your systems meet standards for security, availability, and data confidentiality.
- **GDPR -** Applies to any company handling personal data of EU residents, regardless of where your business is located.
- **CCPA/CPRA -** California's consumer privacy laws apply to companies doing business with California residents, with expanded enforcement authority and rising penalty levels.
- **CMMC/NIST -** Required for government contractors and their supply chains. Compliance levels range from basic cyber hygiene to advanced threat protection.

DivergeIT
IT Solution Partner

The Compliance Stakes: What's Required and **What Happens When You Fall Short**

The Cost of Non-compliance is Rising - and Enforcement is Accelerating.

Regulatory bodies have become significantly more aggressive about enforcement, and the financial consequences are no longer reserved for large institutions:

- **HIPAA:** In 2025, the HHS Office for Civil Rights imposed over $8 million in fines across 19 settlements - the highest number of resolution agreements in a single year on record. Per-violation fines can reach **up to $2.13 million per violation category per year** for willful neglect.[8]
- **PCI DSS:** Non-compliance penalties typically run **$5,000 to $100,000 per month**, and payment processors can, and do, revoke a company's ability to accept credit cards.[9]
- **CCPA/CPRA:** California fined American Honda $632,500 in 2025 for making it unnecessarily difficult for consumers to exercise their privacy rights - a data point that signals how seriously California's Privacy Protection Agency is taking enforcement against businesses.[10]
- **GDPR:** Total cumulative fines have now exceeded €5.88 billion across thousands of cases. The average fine across all cases is €2.36 million.[11]

Cost of non-compliance

- Regulatory fines
- Legal fees
- Remediation costs
- Lost contracts
- Reputational damage

Unpredictable. Compounding. Avoidable.

Cost of a compliance program

A structured compliance program — policies, controls, and ongoing management — is a fixed, predictable investment with a defined scope.

"The cost of getting it right is almost always less than the cost of getting it wrong."

DivergeIT
IT Solution Partner

The Compliance Stakes: What's Required and **What Happens When You Fall Short**

Compliance is Not a One-time Project.

One of the most common and costly misconceptions about compliance is treating it as a one-time checkbox exercise. Regulations update. Systems change. Staff turns over. New vendors are onboarded. Any of these events can create new compliance gaps. The companies that stay out of trouble are the ones that monitor continuously, not the ones that passed an audit three years ago and haven't at it looked since.

To stay on top of it, compliance requires dedicated expertise, continuous monitoring, and documentation that's maintained and current - not scrambled together when an audit appears on the horizon.

Industry	Framework(s)	Key Requirements
Healthcare	HIPAA	Protection of patient health information (PHI), breach notification within 60 days, access controls and audit trails
Financial Services	SOX, GLBA, FINRA	Financial data integrity, customer data protection, cybersecurity incident reporting to regulators
Professional Services	SOC 2, GDPR	Trust and security controls for client data, EU data privacy rights and cross-border data transfer rules
Retail	PCI DSS	Secure handling of cardholder data, network segmentation, encryption, and annual compliance validation
Government Contractors	CMMC, NIST	DoD contract eligibility requires certified cybersecurity maturity levels and NIST 800-171 control implementation

Sources:
[8] HHS OCR Enforcement Data; Secureframe Non-Compliance Fines Report, 2025
[9] Help Net Security, Weak Enforcement Keeps PCI DSS Compliance Low, 2025
[10] California Privacy Protection Agency; Compliance Hub, Compliance Fines 2025
[11] GDPR Enforcement Tracker; Compliance Hub, Compliance Fines 2025

Why Mid-Sized Companies **Struggle to Keep Up**

WWW.DIVERGEIT.COM

DivergeIT
IT Solution Partner

Why Mid-Sized Companies **Struggle to Keep Up**

There's a specific and well-documented challenge that companies in the 50–500 employee range face with IT: they've grown complex enough that the demands are real, but they haven't yet built the infrastructure to manage the demands systematically. Understanding why this happens is the first step toward solving it.

The IT Generalist Problem

Most mid-sized companies rely on one or a small number of IT staff who manage everything: help desk tickets, network infrastructure, software deployments, security monitoring, patch management, backup systems, and compliance documentation - often simultaneously. These are fundamentally different disciplines. Asking a generalist team to stay current across all of them while responding to daily operational demands creates inevitable gaps. Not because the people aren't capable, but because no finite team can do all these things well without dedicated resources and specialized depth.

Reactive Habits are Hard to Break

When most IT capacity is consumed responding to problems, there's nothing left over for prevention. Scheduled maintenance gets deferred. Patch cycles slip. Security reviews don't happen. Backup testing gets skipped. Each individual deferral feels reasonable in the moment; the accumulation of them over time creates an environment where the next incident isn't a question of if, but when.

DivergeIT
IT Solution Partner

Why Mid-Sized Companies **Struggle to Keep Up**

Technology Complexity is Accelerating

The IT environment of a 200-person company in 2025 looks nothing like it did five years ago. Cloud infrastructure, SaaS applications, remote and hybrid workforces, Microsoft 365 environments, AI tools, mobile devices, and third-party integrations have all expanded the attack surface and the compliance footprint simultaneously. The rate at which new complexity is being added consistently outpaces the rate at which internal teams can learn to manage it efficiently or securely.

Budget Pressure Creates False Economies

It's easy to defer IT investment when nothing is visibly broken. The cost of reactive IT - lost productivity, emergency service calls, downtime, compliance penalties - is distributed and often invisible until a significant event forces it into the open. Proactive IT investment, by contrast, shows up as a line item on the budget every month. This asymmetry consistently leads companies to underinvest in prevention relative to the risk they're carrying.

1 in 5
SMBS

report being unable to survive a network or data breach that costs them as little as $10,000.

VikingCloud, 2025 SMB Threat Landscape Report

From Reactive to Proactive: What a **Modern IT Program Looks Like**

WWW.DIVERGEIT.COM

DivergeIT
IT Solution Partner

From Reactive to Proactive: What a **Modern IT Program Looks Like**

Proactive IT isn't a philosophy - it's a set of specific, measurable capabilities. Understanding what a well-run IT program includes helps business leaders evaluate whether their current environment has meaningful gaps.

The Core Components of a Proactive IT Program

Continuous monitoring: Your network, servers, endpoints, and cloud environment should be monitored in real time - not checked periodically or only after something breaks. Monitoring tools detect anomalies, performance degradation, and security indicators before they become outages or incidents.

Automated patch and update management: Unpatched software is one of the most common entry points for attackers and causes of system instability. A proactive program applies security patches and updates on a defined cycle - not when someone has time to get to it.

Backup and disaster recovery - tested, not assumed: Most companies have some form of backup. Far fewer have regularly tested whether those backups restore correctly. A mature program includes documented recovery procedures, defined recovery time objectives, and regular testing that confirms recovery works when it's needed.

Endpoint security and device compliance: Every device accessing your corporate systems - whether company-issued or personal - is a potential entry point. Modern endpoint protection goes beyond antivirus. It includes behavioral detection, device compliance enforcement, and the ability to remotely isolate or wipe compromised devices.

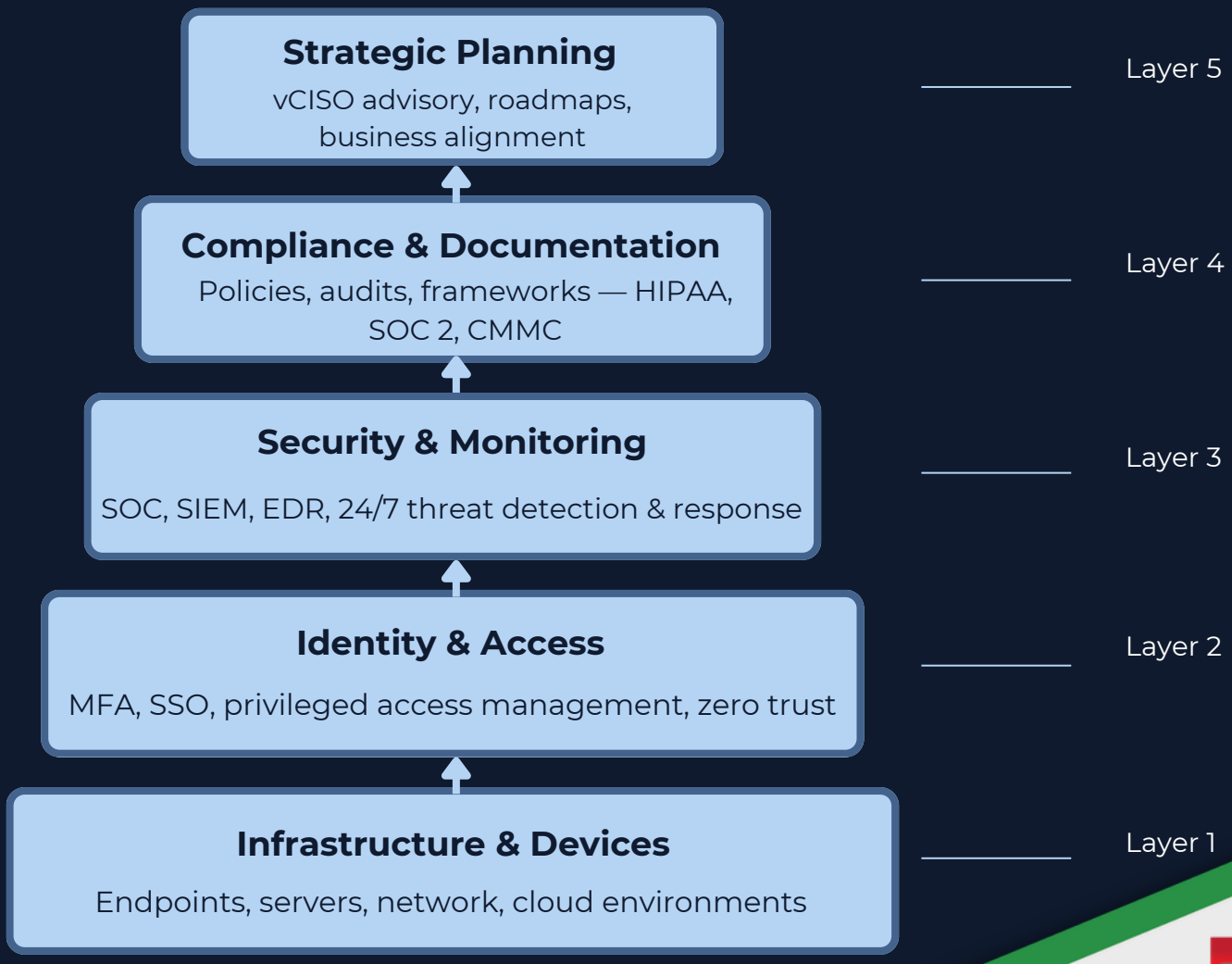
Identity and access management: Who has access to what, and why? Many companies have accumulated access permissions over time without auditing or rationalizing them. Proper identity management, including multi-factor authentication, least-privilege access principles, and regular access reviews, significantly reduces the scope and impact of any compromise.

DivergeIT
IT Solution Partner

From Reactive to Proactive: What a **Modern IT Program Looks Like**

Compliance documentation and audit readiness: Compliance isn't just about having the right controls in place, it's also about being able to prove it. A mature program maintains continuous documentation, maps controls to applicable frameworks, and keeps the organization audit-ready year-round rather than scrambling every audit cycle.

Strategic IT planning: Technology decisions made today have consequences for years. A proactive program includes regular strategic reviews that align your IT roadmap with your business objectives, ensuring your infrastructure supports growth rather than constraining it.



The Business Case for Outsourcing IT: **Build vs. Partner**

WWW.DIVERGEIT.COM

DivergeIT
IT Solution Partner

The Business Case for Outsourcing IT: **Build vs. Partner**

The question isn't whether you need a mature IT program (you do), it's whether building one internally or partnering with a managed IT provider is the right approach to get you and keep you there - faster, better, and at lower total cost.

What Building a Great IT Support Program Internally Requires

A proper internal IT capability that covers proactive monitoring, security, patch management, backup and recovery, compliance, and strategic planning requires:

- Multiple headcount with distinct specializations (security, infrastructure, compliance, help desk), which is rarely achievable with fewer than 3–5 dedicated IT staff
- Significant technology investment in monitoring platforms, endpoint protection tools, backup systems, and compliance software
- Continuous training to stay current in an environment where the threat and regulatory landscape changes meaningfully every 6–12 months
- 24/7 coverage - which means either overtime, on-call arrangements, or staffing for multiple shifts

The fully loaded annual cost of this capability - including salaries, benefits, tooling, and training - runs well into six figures for even a basic program and requires consistent management attention to sustain.

DivergeIT
IT Solution Partner

The Business Case for Outsourcing IT: **Build vs. Partner**

What a Trusted Managed Services Provider Should Deliver

The right managed IT service provider (MSP) operates as an extension of your business, taking on the day-to-day responsibility for your technology environment while you focus on running and growing your company. The right provider brings:

- **Immediate expertise across multiple disciplines -** security specialists, cloud architects, compliance experts, and help desk support, without the hiring, training, or retention burden
- **Enterprise-grade tooling -** monitoring platforms, security tools, and compliance software that would be cost-prohibitive for a single small or mid-sized company to license and operate independently
- **Predictable, flat-rate pricing** - turning unpredictable IT emergencies into a known monthly cost that doesn't spike when something goes wrong
- **24/7 coverage -** most mid-sized companies cannot staff 24/7 IT support coverage; managed providers operate at scale across many clients, making continuous coverage economically viable
- **Faster time to maturity -** building a proactive IT program from scratch internally can take 12–18 months or longer; an experienced MSP can assess, prioritize, and close gaps in a fraction of that time

The Economics in Practice

For most small and mid-sized businesses, managed IT services are priced between **$100 and $250 per user per month**, depending on scope and service level.[1][2] For a 50-person company, that's a range of $5,000 to $12,500 per month - or $60,000 to $150,000 per year.

Compare that against a single significant downtime event ($25,000–$100,000+), a compliance penalty ($5,000 to $2 million+ depending on the framework), or the cost of hiring and retaining even two dedicated IT specialists ($200,000+ per year in fully loaded costs). The math consistently favors partnership.

DivergeIT
IT Solution Partner

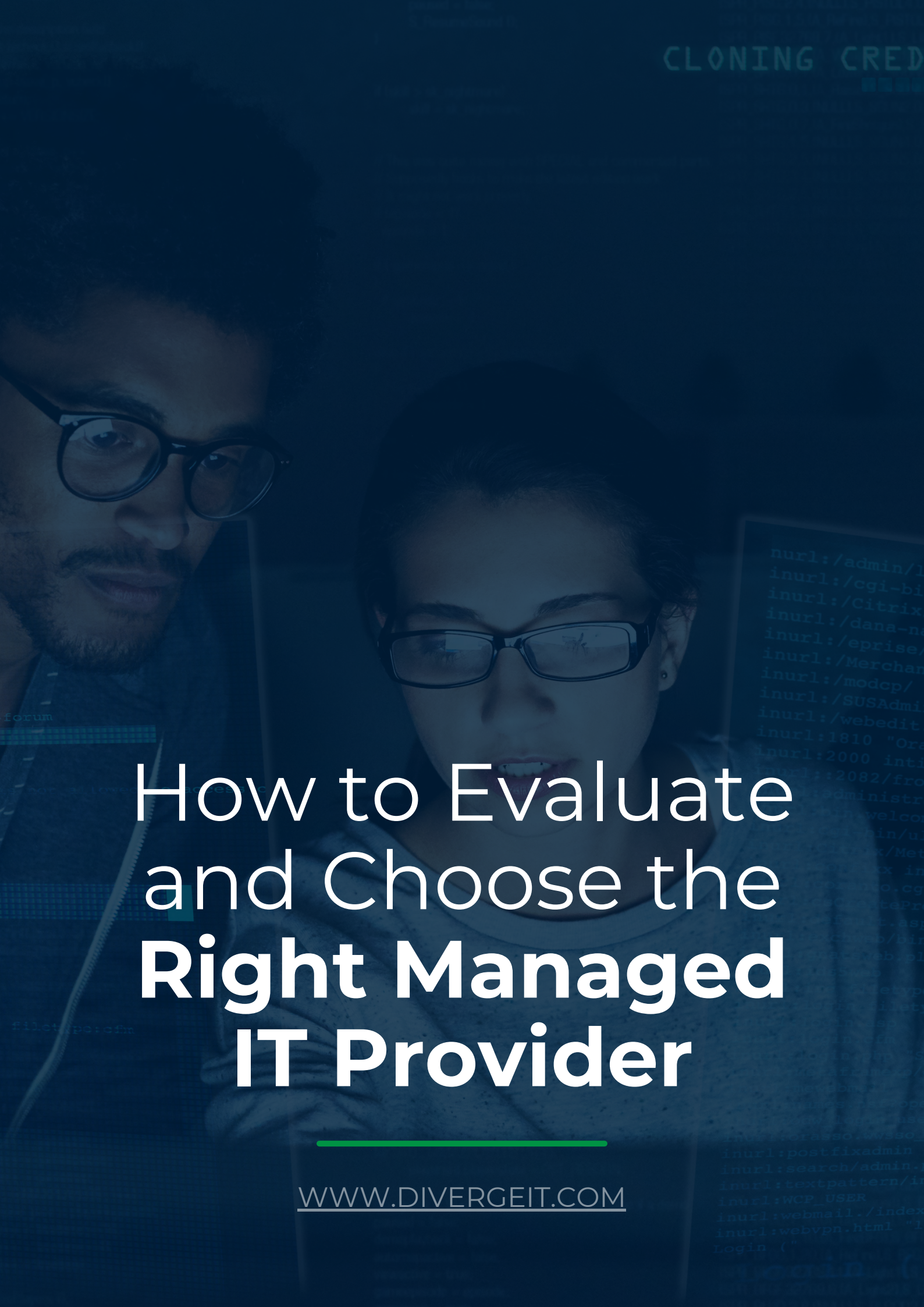
The Business Case for Outsourcing IT: **Build vs. Partner**

What an MSP Cannot Replace

It is important to highlight that outsourcing IT to a managed provider is not a decision that removes all responsibility from company leadership. The most effective MSP relationships work because the business leadership is engaged - approving security investments, enforcing policies with employees, and treating IT as a strategic function rather than an afterthought. An MSP is a force multiplier, not a substitute for organizational commitment.

IT Management Model Comparison	Managing Internally **In-House IT Team**	Partnering with an MSP **DivergeIT**
Cost Structure	Variable — salaries, benefits, tooling, and surprise costs compound unpredictably	Fixed monthly fee — fully budgetable with no surprise infrastructure costs
Expertise Available	One or two generalists — limited depth across networking, security, cloud, and compliance	Full team of specialists — engineers, analysts, and vCISO-level advisory on demand
Coverage Hours	Business hours only — nights, weekends, and holidays leave systems unmonitored	24/7/365 monitoring — coverage never stops, regardless of time or day
Response Time	Reactive — issues often discovered hours or days after impact has begun	Proactive detection — SLA-backed response times measured in minutes, not hours
Compliance Support	Ad hoc — frameworks like HIPAA and SOC 2 require costly outside consulting engagements	Built-in compliance alignment — HIPAA, SOC 2, CMMC, and NIST mapped to your program
Speed to Maturity	Slow — hiring, onboarding, and building a program from scratch takes 12–24+ months	Fast — fully operational from day one, leveraging proven toolsets and processes
Predictability	Low — staff turnover, tool sprawl, and evolving threats create ongoing uncertainty	High — consistent delivery, defined SLAs, and a single accountable partner

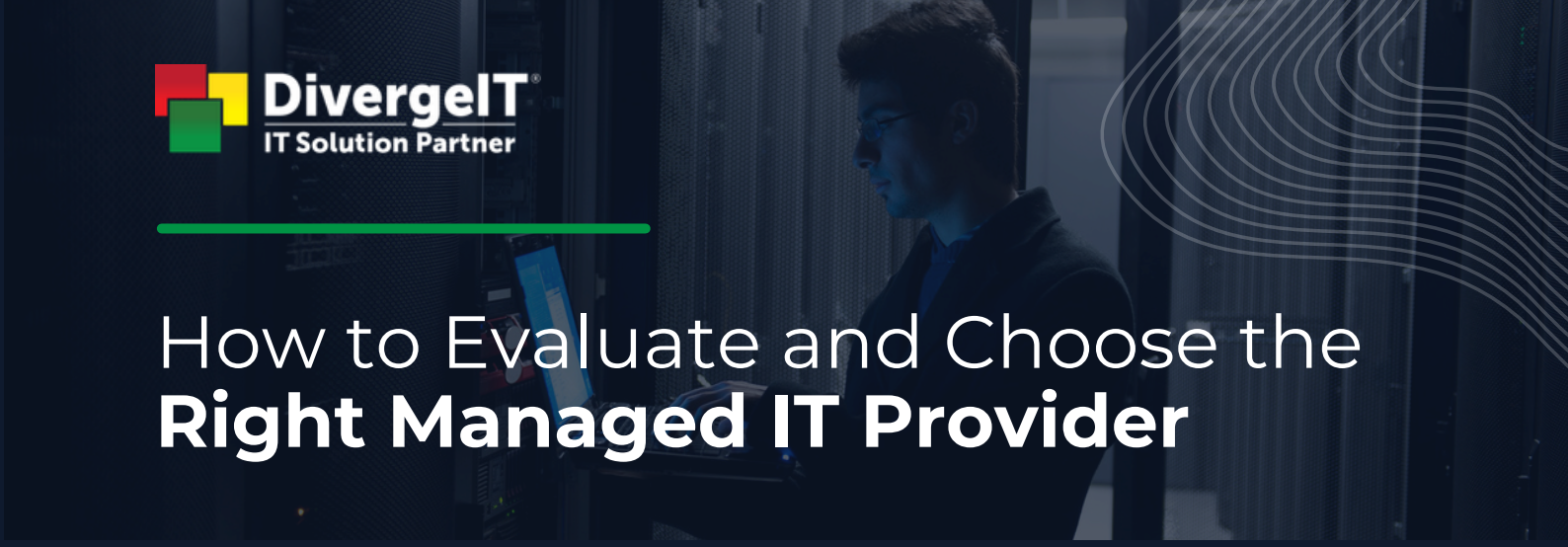
Sources:
[12] DivergeIT / industry MSP pricing benchmarks



How to Evaluate and Choose the **Right Managed IT Provider**

WWW.DIVERGEIT.COM

DivergeIT
IT Solution Partner



How to Evaluate and Choose the **Right Managed IT Provider**

The MSP market is large and uneven in quality. The right partner can genuinely transform your IT environment; the wrong one creates a false sense of security while problems accumulate. Here's how to evaluate your options with confidence.

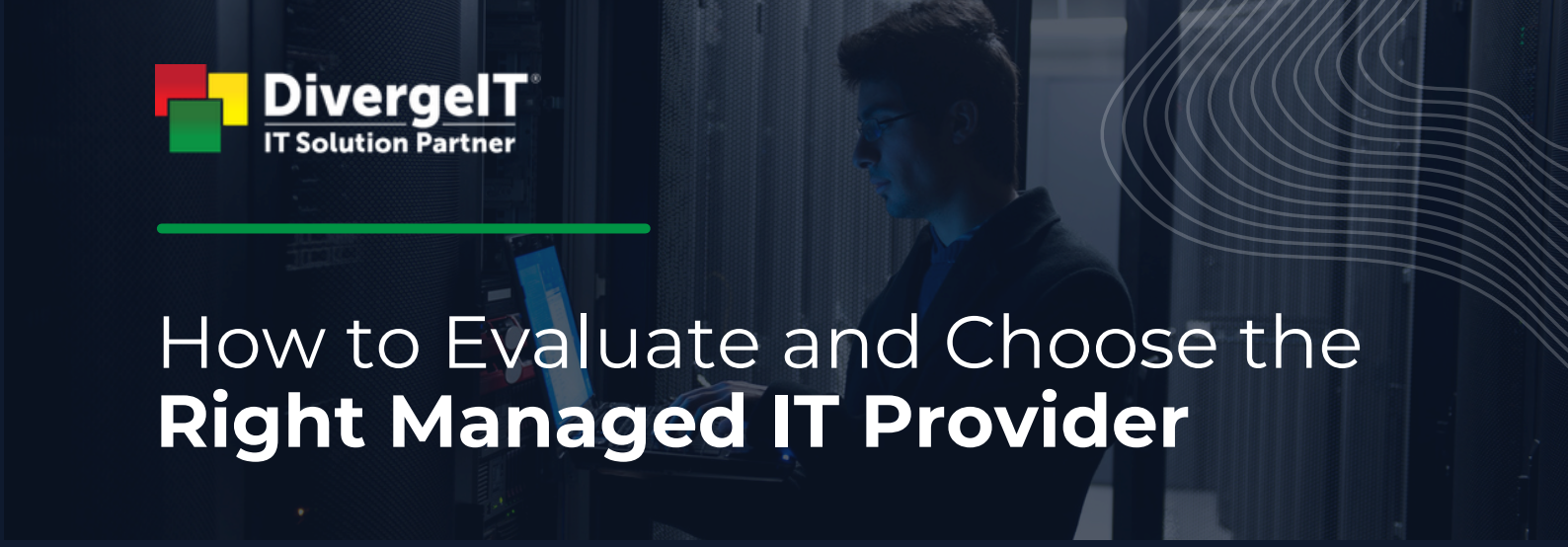
Three Qualification Filters that Narrow the Field Quickly

1. Do they have demonstrated expertise in your industry? Healthcare, financial services, legal, manufacturing, and government contracting each carry distinct compliance requirements and operational contexts. An MSP that serves your industry understands your specific regulatory obligations, speaks your language, and has experience building programs that meet those requirements. Ask for specific examples and references.

2. Are they SOC 2 certified or equivalent? This is a critical signal of operational maturity that's easy to verify and quickly narrows the field. An MSP willing to hold itself to a formal compliance standard is demonstrating the same discipline it will bring to your environment. Remarkably, a significant share of managed IT providers - even experienced ones - do not hold active SOC 2 certification.

3. Do they hold current vendor certifications for your environment? If you operate in Microsoft 365 - as the vast majority of mid-sized businesses do - your provider should hold an active Microsoft partnership credential. This isn't just a badge; it reflects that the team is trained, certified, and recognized by Microsoft on the platform managing your identity, email, collaboration, and data. Ask for documentation.

DivergeIT
IT Solution Partner



How to Evaluate and Choose the **Right Managed IT Provider**

Beyond Qualifications, Evaluate On:

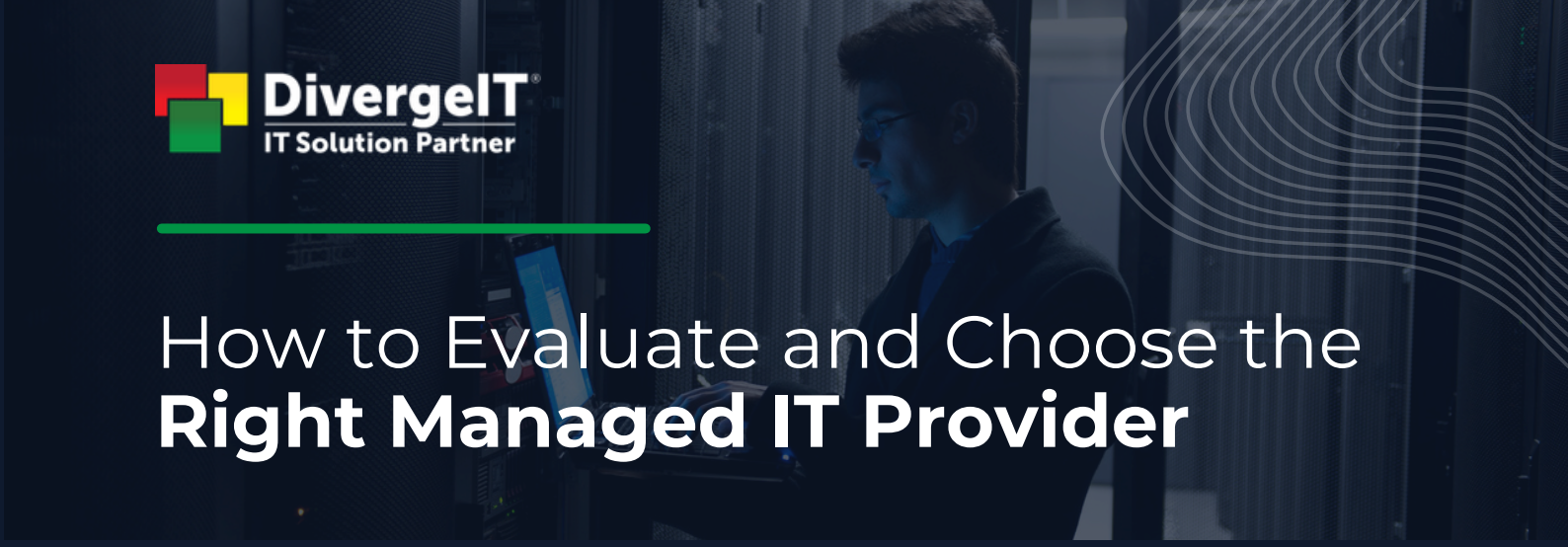
Scope of services - A credible managed IT provider covers the full stack: endpoints, identity, network, cloud, email, backup and recovery, and compliance. A provider strong in help desk support but light on security and compliance is not positioned to manage the risk environment your business faces today.

Response time commitments - There's a meaningful difference between an MSP that monitors your environment and one that responds when something goes wrong. Get specific SLA commitments in writing. How quickly is a critical alert escalated to a human? How long does initial response take? What are the escalation paths? A reputable provider will document these clearly. Vague answers here are a weak signal.

Proactive vs. reactive orientation - Ask a prospective provider: how do you identify and address issues before they become outages? Providers oriented toward proactive management will have clear answers about monitoring protocols, patch management schedules, and regular maintenance reviews. Providers operating primarily in break-fix mode will give you vague generalities.

Compliance capabilities specific to your needs - If your business carries compliance obligations - HIPAA, PCI DSS, SOC 2, CMMC, or others - ask directly: what does your support for this framework include? Can you provide documentation and audit support? Do you have a compliance platform? Have you supported clients through audits under this framework?

DivergeIT
IT Solution Partner



How to Evaluate and Choose the **Right Managed IT Provider**

Transparency and reporting - You should receive regular, readable reporting on the health of your IT environment: what's been monitored, what's been patched, what incidents occurred and how they were resolved, and where your compliance posture stands. Ask to see a sample report before signing anything. If the reporting is opaque, the relationship will be too.

Client references - Ask for references from companies similar to yours in size and industry and call them. Ask not just whether they're satisfied, but specifically: How has the provider handled an incident? How do they communicate during problems? Would you sign with them again? The answers to these questions reveal more than any sales conversation.

Red Flags to Watch For:

- No SOC 2 or equivalent compliance certification
- Inability to clearly describe what's included vs. billed separately
- Vague or missing SLA commitments on response times
- No demonstrated industry-specific experience
- Unable or unwilling to provide client references
- No Microsoft or Google partner credential when you operate in those environments
- A "we handle everything" answer to every question, with no specificity on how

DivergeIT
IT Solution Partner

MSP Evaluation **Scorecard**

Use this scorecard when evaluating managed IT service providers. Rate each provider on a scale of 1–5 for each criterion. The provider with the highest total score in the categories most relevant to your business, who also feels like a good fit with your company culture and team, is likely your strongest candidate.

SECTION A: Qualifications & Credentials

Evaluation Criterion	Notes	Score (1–5)
Active SOC 2 certification or equivalent	Request the current certificate	_____
Microsoft / Google / other platform partnership credentials	Verify at certified partner level	_____
Demonstrated experience in your specific industry	Ask for named client examples or case studies	_____
Years in business (5+ years preferred)	Track record of stability matters	_____
Dedicated managed IT practice (not break-fix with an "MSP label")	Ask how the team is structured	_____

SECTION B: Scope of IT Services

Evaluation Criterion	Notes	Score (1–5)
24/7 proactive monitoring (network, servers, endpoints, cloud)	Active monitoring, not reactive ticketing	_____
Automated patch and update management	Defined patch cycle with documented SLA	_____
Endpoint protection and device compliance enforcement	Covers all device types, including BYOD	_____
Identity and access management (MFA, access reviews)	Not just deployed - actively managed	_____
Backup and disaster recovery - with tested restoration	Ask when they last tested recovery for a client	_____
Cloud and Microsoft 365 / Google Workspace management	Covers your primary productivity environment	_____
Help desk support - response time and staffing hours	U.S.-based? Hours of availability? SLA?	_____

DivergeIT
IT Solution Partner

MSP Evaluation **Scorecard**

SECTION C: Compliance Capabilities

Evaluation Criterion	Notes	Score (1–5)
Support for your specific compliance frameworks (HIPAA, PCI, SOC 2, CMMC, CCPA)	Ask for specific experience, not just awareness	_____
Compliance gap assessment capability	Can they assess where you stand today?	_____
Ongoing compliance monitoring and documentation	Continuous, not just at audit time	_____
Audit preparation and support	Have they supported audits under your framework?	_____
Proprietary or integrated compliance platform	Automated evidence collection and reporting?	_____

SECTION D: Operations & Service Delivery

Evaluation Criterion	Notes	Score (1–5)
Documented response time SLAs by incident severity	Get this in writing before signing	_____
U.S.-based support team available during your business hours	Confirm staffing model and locations	_____
Defined escalation process for critical incidents	Who do you call? What happens next?	_____
Proactive maintenance schedule and cadence	Scheduled reviews, not just reactive response	_____
Business continuity and disaster recovery planning support	Ownership of the plan, not just backup tools	_____

DivergeIT
IT Solution Partner

MSP Evaluation **Scorecard**

SECTION E: Transparency & Partnership

Evaluation Criterion	Notes	Score (1–5)
Regular, readable IT environment reporting	Review a sample report before deciding	_____
Client portal or real-time visibility into environment status	Can you see what's happening without asking?	_____
Referenceable clients in your industry	Ask for 2–3 and contact them	_____
Clarity on pricing - what's included vs. billed separately	No surprises after onboarding	_____
Strategic IT planning as part of the engagement	Are they an advisor, or just a vendor?	_____
Responsiveness and communication quality during the sales process	How they sell is how they'll serve	_____

Scoring Summary

Section	Max Score	Provider A	Provider B	Provider C
A: Qualifications & Credentials	25			
B: Scope of IT Services	35			
C: Compliance & Capabilities	25			
D: Operations & Service Delivery	25			
E: Transparency & Partnership	30			
TOTAL	**140**			

For businesses with significant compliance obligations - Healthcare, Financial services, Legal, Government Contracting - consider weighing Section C scores at 1.5x when calculating totals

About **DivergeIT**

DivergeIT is a managed IT and security services provider with more than 20 years of experience supporting mid-sized companies across the United States. Ranked among the top managed service providers in the country - including #24 nationally and #2 in Los Angeles - DivergeIT brings enterprise-grade IT management, compliance expertise, and security capabilities to companies that need them most: growing organizations that have outpaced their current IT infrastructure and need a partner who can close the gap.

DivergeIT holds active SOC 2 certification, top 1% Microsoft Partner status in the United States, and a proprietary compliance platform that automates evidence collection and audit preparation across HIPAA, SOX, FINRA, FDIC, NIST, and other key frameworks. Our commitment is backed by real service guarantees - including $100 credits for missed response times, no-cost ransomware recovery, and live engineers available in under five minutes.

Ready to See Where Your IT Environment Stands?

Contact DivergeIT for a no-obligation IT assessment.

Sales@divergeit.com | www.DivergeIT.com | 866-216-3837