



— MANAGED IT & WHITE-GLOVE SUPPORT

The San Diego Managed IT Buyer's Guide

How to compare managed IT providers, read a proposal and plan a clean switch

- A readiness worksheet to complete before you speak to any provider
- A proposal review table with the red flags worth catching early
- A weighted scorecard for comparing providers on more than price
- A switching plan and 90-day checklist for a clean handover

Why this guide, and how to use it.

Most businesses choose a managed IT provider after a bad week: a ransomware scare, a departing IT person, or one outage too many. That is exactly when it is hardest to compare options calmly. This guide gives you a structured way to do it, written from the provider side of the table by people who know which questions are hard to answer well.

Use it in order. Fill in the readiness worksheet first, so every provider quotes against the same facts. Take the questions and scorecard into each meeting, then use the checklist and 90-day plan once you have chosen. Nothing here assumes you will pick Alpiba; it works for any provider you are considering.

What's inside

- A readiness worksheet to complete before you speak to any provider
- A proposal review table with the red flags worth catching early
- A weighted scorecard for comparing providers on more than price
- A switching plan and 90-day checklist for a clean handover

Contents

- 01 Step 1: know what you have before anyone quotes
- 02 Step 2: read the proposal for what it leaves out
- 03 Step 3: score providers on evidence, not charm
- 04 Step 4: switch providers without losing access
- 05 San Diego considerations
- 06 Your 24-point checklist
- 07 Questions to ask any IT provider
- 08 Your 30/60/90-day plan
- 09 Plain-English glossary
- 10 About Alpiba

How to use it: read Part 1 together with the person who owns IT decisions, then work through the checklist in one sitting. Anything you can't tick becomes the first line of your 30-day plan.

● PART 1

Step 1: know what you have before anyone quotes

Providers can only quote accurately against accurate facts. Spend an hour gathering the items below before the first meeting, and send the same summary to every provider you talk to. Gaps are fine: write “unknown” and treat each one as a question the provider should help you answer.

Readiness worksheet		
WHAT TO GATHER	WHERE TO FIND IT	WHY IT MATTERS
Number of users, including part-timers and contractors	Payroll, or your Microsoft 365 or Google Workspace admin console	Most managed IT is priced per user
Devices: laptops, desktops, servers, network gear	Your current provider, purchase records or a walk-through	Every device needs monitoring and patching
Locations and remote staff	Office leases and HR records	Drives on-site visits and network scope
Key business apps and who supports them	Ask each department what they can't work without	Line-of-business software is where outages hurt most
Vendors, contracts and renewal dates	Accounts payable and searches for renewal emails	Someone has to own these after the switch
Admin credentials and domain registrar access	Current provider, internal IT or the original setup emails	Whoever holds these controls your business
Compliance or insurance obligations	Client contracts, insurer questionnaires, regulators	HIPAA, SOC 2 or PCI DSS change the scope



Find your domain registrar first

If nobody knows who controls your domain name, fix that before anything else. Your email, website and many logins depend on it, and recovering a domain held in a former employee's personal account is slow and painful.

● PART 2

Step 2: read the proposal for what it leaves out

Most proposals list similar services. The differences hide in definitions, exclusions and the topics that are not mentioned at all. Read each proposal against this table and write down every question it raises.

Proposal review: what good looks like, and what to question

AREA	WHAT GOOD LOOKS LIKE	QUESTION IT IF YOU SEE
Scope	Every user, device, site and cloud service you listed is named	Phrases like “standard support” with no definition
Response	Average first response stated, with hours of coverage spelled out	Response promises with no definition of business hours
Security	MFA, endpoint detection and response, email security and 24/7 alert monitoring included	Security offered only as an optional extra
Backups	Immutable, off-site copies with scheduled restore tests and reports	“Backups included” with no mention of testing
Onboarding	A dated plan with named deliverables	An onboarding fee with no description of the work
Pricing	A clear per-user rate and a list of what triggers a project quote	Hourly charges for routine work
Exit	Documentation, credentials and data returned on request	Silence about what happens when you leave

● PART 3

Step 3: score providers on evidence, not charm

Score each provider from 1 to 5 on every row, multiply by the weight (count High as 3, Medium as 2 and Low as 1) and compare totals. The weights below suit a business that handles sensitive data; adjust them to match your priorities before the first meeting, not after.

Provider scorecard

CRITERION	SUGGESTED WEIGHT	EVIDENCE TO ASK FOR
Responsiveness	High	Average first response, how it is measured and who answers after hours
Security operations	High	Who reviews alerts overnight, and a redacted incident summary
Backup and recovery	High	The date and outcome of a recent restore test for a similar business
Documentation	Medium	A redacted runbook and network diagram

CRITERION	SUGGESTED WEIGHT	EVIDENCE TO ASK FOR
Onboarding plan	Medium	A written 90-day plan with deliverables
On-site coverage	Medium	The areas they serve on-site, and how planned and urgent visits are booked
Pricing clarity	Medium	A one-page list of inclusions, exclusions and project triggers
Exit terms	Medium	What you receive if you leave, in writing
Strategic reviews	Low	A sample quarterly business review

- Did they ask about your business before talking about tools?
- Did an engineer join the conversation, or only sales?
- Were the answers in plain English, without hiding behind acronyms?
- Did they tell you anything you didn't want to hear?

● PART 4

Step 4: switch providers without losing access

The riskiest part of changing providers is the handover window, when two parties have partial access and neither feels fully responsible. Treat it as a small project with an owner, a date and a written record.

- 1 Secure ownership first**
 Confirm that your company, not a person or a provider, owns the domain registrar, the Microsoft 365 or Google Workspace admin accounts, the firewall and the backup service.
- 2 Agree an overlap**
 Keep the outgoing provider engaged until the new one has monitoring on every device and has verified that backups restore.
- 3 Transfer and verify**
 Collect documentation, passwords, license details and open tickets, then test each credential rather than trusting the list.
- 4 Rotate and remove**
 Change every shared and admin password, remove the old provider's accounts and remote tools, and get written confirmation that they are gone.

5

Close the loop

Cancel old contracts on their notice dates and file the handover record with your documentation.

**Remote access tools left behind**

Old remote support agents left on devices are a known way in for attackers. Ask the new provider to list every remote access tool it finds and remove anything it didn't install.

● **PART 5**

San Diego considerations

- **On-site reach.** Ask exactly which areas a provider visits. Coverage from Chula Vista to Oceanside is a different promise from coverage of one neighborhood.
- **Power and fire season.** Ask how they prepare clients for SDG&E Public Safety Power Shutoffs: battery backup for network gear, cloud access to files and a remote work plan.
- **Earthquake and off-site recovery.** Backups should be immutable and stored off-site, with a documented way to restore if your office is unreachable.
- **Hybrid teams.** Laptops should be managed and patched wherever people work, not only when they connect to the office network.
- **Industry rules.** Dental practices, law firms, biotech labs and defense suppliers each carry specific obligations. A good provider asks about yours in the first conversation.

● **CHECKLIST**

Your 24-point checklist

Tick each item you can confirm today, with evidence. Anything left blank is a gap worth a conversation.

Service and response

- ☐ Response commitments, and how they are measured, written into the proposal
- ☐ Hours of coverage and the after-hours process in writing
- ☐ Named point of contact assigned
- ☐ Engineers reachable directly, not only through a queue
- ☐ On-site coverage confirmed for each of your locations
- ☐ Ticket priorities defined by business impact

Security and backups

- ☐ MFA enforced for every user and admin account
- ☐ Endpoint detection and response on every laptop and server
- ☐ Overnight and weekend security alerts triaged by a human analyst
- ☐ Immutable, off-site backups in place
- ☐ A restore test completed and documented
- ☐ Old remote access tools removed after the switch

Documentation and ownership

- ☐ Domain registrar held in the company's name
- ☐ Admin accounts owned by the company, not by individuals
- ☐ Network diagram and asset inventory delivered
- ☐ Runbooks written for recurring tasks
- ☐ Onboarding and offboarding checklists agreed
- ☐ Vendor list with contacts and renewal dates handed over

Commercials and exit

- ☐ Inclusions and exclusions listed on one page
- ☐ Project triggers defined before signing
- ☐ Process for adding and removing users understood
- ☐ Exit terms covering documentation, credentials and data
- ☐ Old provider's contract cancelled on its notice date
- ☐ First quarterly business review scheduled

● QUESTIONS

Questions to ask any IT provider

Use these in any proposal meeting, including with us. A good partner answers specifically, in writing, without hedging.

1 What is your average first response time, how do you measure it, and does it change after hours?

Notes:

2 Who reviews security alerts at 2am on a Sunday, and what can they do without calling us first?

Notes:

3 Can you show us a redacted runbook, network diagram and quarterly business review?

Notes:

4 What will the first 90 days look like week by week, and what do you need from us?

Notes:

5 When did you last run a restore test for a business like ours, and what did it show?

Notes:

6 What exactly triggers a project quote instead of being covered by the monthly fee?

Notes:

7 How do you handle a problem that keeps coming back?

Notes:

8 Which parts of San Diego County do you cover on-site, and how are visits scheduled?

Notes:

9 Who owns the admin accounts, documentation and domain if we part ways?

Notes:

10 What is one thing about our setup you would push back on?

Notes:

● ACTION PLAN

Your 30/60/90-day plan

A realistic sequence for a busy team. Assign an owner to each line and review progress every two weeks.

1 First 30 days

- ☐ Send the same readiness worksheet to every provider on your shortlist
- ☐ Meet each provider with an engineer in the room and ask the questions in this guide
- ☐ Score proposals with the weighted scorecard, using evidence rather than adjectives
- ☐ Confirm your company controls the domain registrar and every admin account

2 Days 31–60

- ☐ Sign with your chosen provider and agree a dated onboarding plan
- ☐ Run an overlap period with the outgoing provider
- ☐ Get monitoring onto every device and verify backups with a test restore
- ☐ Rotate shared and admin passwords once the handover is complete

3 Days 61–90

- ☐ Review the full inventory, documentation and runbooks
- ☐ Test the onboarding and offboarding checklists on a real hire or departure
- ☐ Close out the old provider: final invoice, contract end and access removal confirmed
- ☐ Hold the first quarterly business review and agree next year's priorities

● GLOSSARY

Plain-English glossary

Managed service provider (MSP)

A company that runs IT for other businesses for a recurring fee, usually including helpdesk, monitoring, security and vendor management.

First response time

How long it takes a person to acknowledge a request and start working on it. It is not the same as the time to fix.

RMM

Remote monitoring and management: the software a provider uses to watch device health, push patches and fix problems remotely.

Quarterly business review (QBR)

A meeting each quarter where provider and client look back at tickets, incidents, risk and spend, and agree what comes next.

EDR

Endpoint detection and response: security software that watches laptops and servers for malicious behavior and can isolate a device.

Offboarding

The steps that remove a departing person's access, recover their devices and hand their data to the right owner.

Immutable backup

A backup copy that can't be altered or deleted for a set period, even by an administrator, so ransomware can't destroy it.



Enterprise-grade IT. Human-sized service.

Alpiba is a San Diego-based managed IT and cybersecurity provider for growing businesses. One accountable team runs your helpdesk, security, cloud, network and backups for a flat per-user monthly price, with the discipline of a Fortune 500 technology program and the responsiveness of a boutique firm.

<15 min

average first response from a human-staffed
24/7 SOC

<1 hr

to trigger a documented ransomware
containment playbook

Quarterly

restore drills on immutable, off-site backups

25+ years

of technology leadership, Fortune 500 and
public sector

Book your free 30-minute assessment

We map your top risks, quick wins and a right-sized roadmap. No obligation and no sales pressure. Callers reach a senior engineer, not a call queue.

858-399-4225 info@alpiba.com alpiba.com/free-assessment

This guide is general information for small and mid-sized businesses. It is not legal, compliance or insurance advice; requirements vary by organization, regulator, insurer and contract. Framework references describe readiness support, not certification of Alpiba. © 2026 Alpiba, San Diego, California. You are welcome to share this guide unchanged.