



FREE BUSINESS RESOURCE • 2026 EDITION

The Silicon Valley Managed IT Buyer's Guide

How to compare IT providers, evaluate proposals, reduce risk, and plan a smooth transition.



01 A readiness worksheet before you request quotes	02 A proposal review table to spot gaps and red flags
03 A weighted scorecard to compare providers fairly	04 A 30/60/90-day plan for a controlled handover

CMIT Solutions Silicon Valley • Local expertise, backed by national resources
cmitsolutions.com/siliconvalley-ca-1019/ • (408) 872-1577

How to use this guide

Choosing an IT partner is easier when every provider is responding to the same facts and the same questions. Use this guide to structure the process before a contract is signed—not after a problem occurs.

A practical sequence

1. Prepare

Gather a current inventory of users, devices, locations, key applications, contracts, and business risks.

2. Compare

Give each provider the same requirements. Ask for written scope, response definitions, security details, backup evidence, and exit terms.

3. Verify

Score providers against evidence and references, not just presentation quality or the lowest monthly price.

4. Transition

Assign an owner, confirm account ownership, maintain overlap, test recovery, and document access removal.

A useful rule

If a provider cannot explain an important commitment in plain English and put it in writing, treat it as unresolved—not as an assumed inclusion.

Inside the guide

SECTION	WHAT YOU'LL FIND
01	Readiness worksheet
02	Proposal review: what to verify
03	Provider scorecard
04	Switching providers safely
05	Silicon Valley and Bay Area considerations
06	24-point IT partner checklist
07	Questions to ask providers
08	Your 30/60/90-day plan
09	Plain-English glossary
10	About CMIT Solutions Silicon Valley

Step 1 | Know what you have before anyone quotes

Providers can only scope accurately against accurate information. Spend time gathering the items below and share the same summary with every provider. If something is unknown, write “unknown” and ask how the provider will help establish it.

WHAT TO GATHER	WHERE TO LOOK	WHY IT MATTERS
Users and contractors	HR roster; Microsoft 365 or Google Workspace admin	Drives per-user licensing and support scope
Devices and network gear	Asset list, invoices, current IT provider	Every endpoint and network device needs ownership, patching and monitoring
Sites and remote work	Office list, remote-work policy, staff locations	Affects on-site coverage, connectivity and access controls
Business-critical apps	Department leads; vendor contracts	Identifies where downtime would stop revenue or service
Cloud and email	Microsoft 365, Google Workspace, cloud consoles	Clarifies identity, data storage, licensing and security responsibilities
Backups and recovery	Backup console, provider reports, restore-test records	A backup is only useful if data can be restored in time
Contracts and renewals	Accounts payable, vendor emails, renewal calendar	Prevents surprise costs and missed notice dates
Admin access and domain	Domain registrar, identity platform, firewall, DNS	Your organization should control its critical accounts
Compliance and insurance	Customer contracts, insurer questionnaires, legal/compliance lead	May affect security controls, retention and evidence requirements

First priority: confirm ownership

Make sure your organization controls its domain registrar, business email tenant, cloud accounts, firewall, backup console, and administrator identities. Keep recovery methods current and protected.

Business snapshot to complete

YOUR NOTES	YOUR NOTES
Number of users: _____	Number of locations: _____
Critical applications: _____	Current IT model: _____
Top 3 business risks: _____	Contract renewal date: _____

Step 2 | Read the proposal for what it leaves out

Proposals may use similar service names while defining them very differently. Review the detail behind each promise and ask for written clarification before signing.

AREA	WHAT GOOD LOOKS LIKE	RED FLAGS TO QUESTION
Scope	Users, devices, sites, cloud services and responsibilities are explicitly listed.	"Standard support" without a definition; devices or sites left out
Response & coverage	Priority levels, first-response targets, support hours and after-hours process are defined.	A promise to be "fast" with no measurement or coverage window
Security operations	MFA, endpoint protection, email security, alert handling and escalation are described.	Security tools sold as optional extras without a risk discussion
Backups & recovery	Backup scope, retention, off-site/isolated copies, restore tests and recovery objectives are stated.	"Backups included" with no restore evidence or recovery target
Onboarding	A dated plan, named deliverables, dependencies and accountable owners are included.	A setup fee with no list of tasks or completion criteria
Pricing	Monthly inclusions, exclusions, project triggers, license costs and annual adjustments are clear.	Routine work billed separately or uncapped charges that are hard to forecast
Compliance	The provider explains what it supports and what remains the client's responsibility.	A broad claim of "compliance" with no controls, evidence or boundaries
Exit & ownership	Data, credentials, documentation, configurations and transition assistance are addressed.	No exit process or unclear ownership of accounts and documentation

Ask for a scope schedule

Request a one-page schedule showing what is included, excluded, monitored, patched, backed up, reviewed, and billed as a separate project. Have the provider explain any exceptions.

Step 3 | Compare providers on evidence

Use a consistent scorecard for every provider. Suggested weights below are a starting point for businesses handling important customer, financial, employee, or regulated data. Adjust weights before meetings, not after seeing the proposals.

CRITERION	SUGGESTED WEIGHT	EVIDENCE TO REQUEST
Security monitoring and response	3 – High	Describe alert triage, escalation, after-hours coverage; provide a redacted example report.
Backup and recovery	3 – High	Show a recent restore-test result and explain recovery time and recovery point targets.
Service responsiveness	3 – High	Define first response, severity levels, measurement method and support hours.
Scope clarity	3 – High	Provide written inclusions, exclusions and responsibilities by system/site.
Onboarding plan	2 – Medium	Share a dated plan, discovery deliverables, risks and dependencies.
Documentation and ownership	2 – Medium	Confirm company ownership of tenant, domain, credentials, diagrams and runbooks.
Pricing transparency	2 – Medium	Explain user/device pricing, license costs, annual changes and project triggers.
Local/on-site coverage	2 – Medium	Confirm service area, scheduling process and urgent on-site options.
Strategic guidance	1 – Low	Provide a sample quarterly review or technology roadmap.
Exit terms	2 – Medium	Explain how data, credentials and documentation are returned and access is removed.

Scoring method

Score each provider from 1 (weak) to 5 (excellent) for every criterion. Multiply the score by its weight (High = 3, Medium = 2, Low = 1). Add the weighted points, then discuss any high-risk gap regardless of total score.

PROVIDER	SECURITY / RECOVERY	SERVICE / SCOPE	WEIGHTED TOTAL
Provider A	_____	_____	_____
Provider B	_____	_____	_____
Provider C	_____	_____	_____

Step 4 | Switch providers without losing access

A provider change is a controlled project. The riskiest period is the handover, when responsibilities overlap and access may be incomplete. Assign one internal owner and agree the sequence in writing.

01 Secure ownership first

Confirm your organization controls the domain registrar, business email/cloud tenant, identity platform, firewall, backup service, DNS, and administrator accounts.

02 Agree on an overlap

Keep the outgoing provider engaged until the incoming team has discovered the environment, monitoring is active, and backups have been verified.

03 Transfer and test

Collect the asset inventory, network diagrams, licenses, vendor contacts, open tickets, recovery procedures and credentials. Test access rather than trusting a handover spreadsheet.

04 Rotate and remove

After the transfer is validated, rotate shared and privileged credentials, review MFA/recovery methods, remove unneeded accounts and remote tools, and record completion.

05 Close the loop

Confirm contract notice dates, final invoices, license ownership, data return, and a written transition record. Keep evidence in your internal documentation.

Remote-access cleanup matters

Ask the new provider to inventory remote support agents, VPNs, service accounts, and management tools. Remove anything no longer authorized, and document what remains.

Handover sign-off

HANDOVER ITEM	HANDOVER ITEM
Internal owner: _____	Target cutover date: _____
Outgoing provider contact: _____	Incoming provider contact: _____
Backup restore verified: ☐ Yes ☐ No	Privileged access reviewed: ☐ Yes ☐ No
Documentation received: ☐ Yes ☐ No	Old access removed: ☐ Yes ☐ No

Silicon Valley & Bay Area considerations

A provider should understand how your team works—not just where your office is. Use these prompts to test whether a proposed service model fits your local operations and risk profile.

TOPIC	QUESTIONS TO ASK
Hybrid and distributed teams	Are laptops, identity controls and security policies managed consistently outside the office? How are remote employees supported?
Cloud collaboration	Who administers Microsoft 365 or Google Workspace, email security, Teams/SharePoint/OneDrive, access policies and licensing?
High-value intellectual property	How are engineering files, source code, designs, customer data and sensitive business documents protected from unauthorized access or exfiltration?
Regulated and customer-driven requirements	Can the provider help map controls and collect evidence for requirements relevant to your business, such as HIPAA, PCI DSS, SOC 2 or CMMC? Who owns formal compliance decisions?
Business continuity	What happens if your office, internet connection, cloud tenant or a key application is unavailable? When was recovery last tested?
On-site service reach	Which Bay Area locations are covered, how are visits scheduled, and what happens when an issue cannot be resolved remotely?
Growth and change	Can the service scale with acquisitions, new locations, more users, AI tools, or new line-of-business applications?
Vendor ecosystem	Who coordinates with internet providers, SaaS vendors, phone providers, hardware suppliers and application support teams?

Industry-specific prompts

BUSINESS TYPE	EXAMPLES TO DISCUSS
Healthcare / dental	EHR availability, PHI access, MFA, backup restoration and HIPAA-related safeguards.
Finance / wealth management	Payment and wire-fraud controls, identity security, records, and applicable SEC/FINRA/GLBA obligations.
Engineering / manufacturing	CAD/BIM performance, large-file collaboration, production uptime, IP protection and customer security requirements.
Professional services / nonprofits	Secure client and donor information, staff/volunteer access, continuity and cost predictability.

These are discussion prompts, not a determination that any specific regulation applies to your organization.

Your 24-point IT partner checklist

Tick each item you can verify today. Leave an item blank if the answer is unknown or only verbal. Use the gaps to guide your next provider conversation.

Service and response

- Response commitments and measurement are written into the proposal
- Support hours and after-hours escalation are defined
- Named account/contact owner is identified
- Ticket priorities reflect business impact
- On-site coverage is confirmed for each location
- Internal responsibilities and customer dependencies are clear

Security and recovery

- MFA is required for users and administrators where appropriate
- Endpoint protection covers company-managed laptops and servers
- Security alerts have a documented triage and escalation process
- Backups are protected from routine compromise or deletion
- A restore test is documented with results and follow-up actions
- Incident response roles and communications are agreed

Documentation and ownership

- Domain registrar and business cloud tenants are company-controlled
- Administrator accounts and recovery methods are documented
- Asset inventory and network diagram are maintained
- Recurring tasks have documented procedures
- Joiner/mover/leaver processes are defined
- Vendor contacts, contracts and renewal dates are recorded

Commercials and exit

- Inclusions and exclusions are listed in plain English
- Project triggers and out-of-scope rates are defined
- Adding/removing users and devices is straightforward
- Exit terms cover data, credentials and documentation
- Old provider access removal is included in transition steps
- A regular service and roadmap review is scheduled

How to use your results

Any unchecked item related to security, recovery, account ownership, or contract exit deserves a clear owner and due date. Prioritize risk—not the number of boxes checked.

Questions to ask every IT provider

Ask the same questions in every meeting. Strong answers are specific, measurable and documented. Use the notes area to compare what each provider says.

01. What is your first-response commitment, how is it measured, and what changes after hours?

Notes: _____

02. Who reviews security alerts overnight or on weekends, and how are urgent incidents escalated?

Notes: _____

03. Can you show a redacted service report, network diagram, runbook or quarterly review?

Notes: _____

04. What will onboarding look like week by week, and what do you need from us?

Notes: _____

05. When was a restore test last performed, what was restored, and what did the test reveal?

Notes: _____

06. What work triggers a separate project quote instead of being covered by the monthly fee?

Notes: _____

07. How do you investigate recurring issues and prevent them from happening again?

Notes: _____

08. Which Bay Area locations do you cover on-site, and how are urgent visits arranged?

Notes: _____

09. Who owns the administrator accounts, domain, documentation and data if we part ways?

Notes: _____

10. What is one risk or weakness you would challenge us to address first?

Notes: _____

Listen for specifics

Ask for examples and evidence. A provider should be comfortable describing limitations, assumptions, dependencies, and what they would do if a control or recovery test failed.

Your 30/60/90-day plan

A realistic sequence for a busy team. Assign an owner to each action and review progress every two weeks. Adjust timing to your environment, contract terms and business calendar.

DAYS 1–30 | Prepare and select

- Complete the readiness worksheet and share it with shortlisted providers.
- Meet each provider with a technical lead present; ask the questions in this guide.
- Score proposals using evidence, written scope and transparent pricing.
- Confirm company control of domain, cloud tenants and privileged accounts.
- Agree decision criteria, stakeholders, budget range and target transition date.

DAYS 31–60 | Onboard and validate

- Sign a defined scope and dated onboarding plan with named owners.
- Run an overlap period with the outgoing provider where possible.
- Inventory assets, identities, applications, vendors and known risks.
- Enable agreed monitoring and security controls across in-scope systems.
- Perform and document a backup restore test; remediate failures.

DAYS 61–90 | Stabilize and improve

- Review inventory, documentation, runbooks and unresolved risks.
- Test onboarding/offboarding steps and privileged-access review.
- Confirm old contracts, licenses, accounts and remote tools are closed out.
- Hold a service review and agree the next quarter's priorities.
- Create a 6–12 month roadmap tied to business goals and risk.

Track the handover

For each action, record an owner, due date, status, evidence/link, and blocker. Do not mark a task complete until the control or deliverable has been verified.

Plain-English IT glossary

TERM	PLAIN-ENGLISH MEANING
Managed service provider (MSP)	A company that manages some or all of an organization's IT for an ongoing fee.
MFA	Multi-factor authentication: requiring more than one form of proof to sign in.
Endpoint detection and response (EDR)	Security technology that monitors computers and servers for suspicious activity and can help contain threats.
RMM	Remote monitoring and management tools used to monitor device health, deploy updates and support systems remotely.
Immutable backup	A backup copy protected against alteration or deletion for a defined period.
Recovery time objective (RTO)	The target time to restore a system or service after disruption.
Recovery point objective (RPO)	The maximum acceptable amount of data loss measured in time.
First-response time	How long it takes a provider to acknowledge a request and begin handling it; it is not necessarily the time to resolve it.
Quarterly business review (QBR)	A scheduled review of service, incidents, risks, spend and upcoming priorities.
Zero trust	A security approach that verifies users, devices and access requests rather than automatically trusting them because of network location.
vcIO / vcISO	Virtual technology or security leadership that helps plan priorities, governance and risk management.
Offboarding	Removing a departing user's access, recovering company devices and transferring their business data appropriately.

Useful evidence to keep

Current asset inventory • access and ownership register • backup/restore test reports • incident escalation plan • vendor and renewal list • network diagram • documented policies • service reports • risk register • transition sign-off.



Local expertise. National resources. A practical IT partner.

CMIT Solutions Silicon Valley supports growing Bay Area organizations with managed IT services, cybersecurity, cloud and Microsoft 365 solutions, IT support, network management, data backup, compliance support and strategic technology guidance.

The local team serves businesses across San Jose, Campbell, Palo Alto, Stanford, Menlo Park, Redwood City, Pleasanton and surrounding Bay Area communities, backed by CMIT's nationwide network.

LET'S TALK ABOUT YOUR IT

CMIT Solutions Silicon Valley

900 East Hamilton, Suite 100
Campbell, CA 95008

Phone: (408) 872-1577

Email: sales@cmitswsv.com

Website: cmitsolutions.com/siliconvalley-ca-1019/

Start with a conversation about your priorities.

Discuss IT operations, cybersecurity, cloud, backup and recovery, compliance needs, or a potential provider transition.

Important note

This guide is for general educational purposes and is not legal, compliance, insurance, or security advice for a specific organization. Requirements depend on your business, contracts, data, regulators and risk profile. Mention of a framework does not guarantee compliance or certification. Verify technical and contractual details with qualified advisors before making decisions.

Prepared for Silicon Valley and Bay Area business owners • 2026