

Technology Planning Guide for **Professional Services Firms**

A practical framework for secure, reliable IT
where productivity, client trust, and information
are the business



Professional Computer Concepts

calpcc.com

TECHNOLOGY
PEOPLE
POSSIBILITIES

How to Use This Guide

Professional services firms depend heavily on people, communication, documents, scheduling, client information, and reputation. Technology problems quickly become client-service problems. The goal is not more technology; it is a dependable environment that lets professionals work efficiently while protecting client and business information.

Best for	Consulting, accounting, architecture, engineering, legal-adjacent, advisory, and other professional services organizations.
Use it to	Ask better questions, identify gaps, and decide what deserves deeper technical review or managed support.

Important

Industry and contractual obligations vary. This guide is a planning framework, not legal or regulatory advice.

1. Identify What Cannot Stop

- Client communication and email.
- Document and file access.
- Scheduling and collaboration.
- Billing, timekeeping, or practice-management systems.
- Remote access for professionals.
- Critical line-of-business applications.
- Secure access to client portals and third-party systems.

2. Protect Client and Firm Information

Information Protection Questions

Check	Question / Action
☐	Where is client information stored?
☐	Who can access each client workspace?
☐	Are former employees and guests removed promptly?
☐	Are sensitive documents shared through

	managed channels rather than personal email or consumer file-sharing?
☐	Are laptops encrypted and centrally managed?
☐	Are backups available independently of primary cloud services?
☐	Are retention and destruction requirements understood?

3. Design for Hybrid and Mobile Work

- Use managed laptops with encryption and endpoint protection.
- Use MFA and identity-based access controls.
- Avoid unmanaged remote-access tools.
- Provide secure collaboration and file access without forcing users into workarounds.
- Define expectations for public Wi-Fi, personal devices, printing, and local file storage.

4. Standardize Client Collaboration

- Use repeatable client workspace structures.
- Define where drafts, final deliverables, and client-provided documents belong.
- Use consistent external-sharing practices.
- Review guest access at project close.
- Avoid creating a new technology exception for every client unless contractual requirements demand it.

5. Reduce Dependency on Individual Employees

Continuity of Knowledge

Check	Question / Action
☐	Business credentials are stored in an approved password manager.
☐	Shared client processes are documented.
☐	Critical vendor accounts are company-owned.
☐	Key files live in managed shared locations.
☐	Administrative access is not dependent on one person.

☐	Offboarding includes transfer of files, ownership, and client responsibilities.
--------------------------	---

6. Cybersecurity Is Part of Client Trust

- Protect identity and email from impersonation and account takeover.
- Use endpoint monitoring and response.
- Train users to recognize phishing and fake support.
- Monitor cloud security events.
- Control privileged access.
- Prepare a response plan before an incident.

7. Govern AI Use With Client Work

AI Questions for Professional Services

Check	Question / Action
☐	May client information be entered into AI tools?
☐	Which AI platforms are approved?
☐	Are personal or free AI accounts prohibited for business data?
☐	Which work products require human verification?
☐	Must clients be informed about AI-assisted work in any circumstance?
☐	How are AI-generated factual claims, citations, calculations, and recommendations verified?
☐	Who approves new AI integrations or data connectors?

Professional judgment remains the product

AI can accelerate professional work, but the firm remains accountable for what it delivers under its name. Treat AI output as work product that requires the same level of professional review appropriate to the consequence.

8. Plan Capacity and Lifecycle

- Replace aging devices before failure becomes urgent.
- Review licenses and cloud costs annually.
- Plan for office moves, growth, and remote staff.
- Retire legacy servers and applications deliberately.
- Budget for security and modernization projects separately from normal support.
- Schedule regular technology strategy reviews with leadership.

Professional Services Technology Scorecard

Leadership Review

Check	Question / Action
☐	Client data locations are known and governed.
☐	Identity and MFA are standardized.
☐	All supported devices are centrally managed and encrypted.
☐	Critical systems have recovery plans.
☐	Client collaboration and external sharing are controlled.
☐	AI use is governed.
☐	Administrative credentials are centrally controlled.
☐	Onboarding and offboarding is repeatable.
☐	Technology lifecycle and budget are reviewed at least annually.

Questions to Ask a Technology Partner

Provider Evaluation

Check	Question / Action
☐	How do you manage identity, devices, security, cloud services, and lifecycle as one system?

☐	Who is accountable for security alerts and vendor escalations?
☐	How do you document the environment?
☐	How do you handle onboarding and offboarding?
☐	How do you plan projects and budgets with leadership?
☐	How do you approach AI governance and approved AI deployment?
☐	How do you test backups and recovery?
☐	What is excluded from the service, and who owns those gaps?

SOURCES

Sources & Further Reading

Product features and vendor controls change. Verify current capabilities, licensing, and contract terms before making implementation decisions.

1. NIST Cybersecurity Framework 2.0 (nist.gov)
2. NIST AI Risk Management Framework (nist.gov)

PROFESSIONAL COMPUTER CONCEPTS

Ready for a Change?

Professional Computer Concepts helps Bay Area businesses manage AI, IT, and cybersecurity through one accountable technology relationship. Contact PCC if you want practical guidance, clearer standards, or a more dependable technology environment.

Website: www.calpcc.com | Call: 415-897-0078

Address: 1565 South Novato Blvd, Suite 3, Novato, CA 94947

Services: Managed IT Services | Cybersecurity Services | Cloud Solutions | Virtual CIO