Professional Computer Concepts

PEOPLE | SOLUTIONS | A SMARTER TOMORROW

The Small Business Guide to AI Governance

How to approve tools, protect data, assign accountability, and use AI without unnecessary bureaucracy

Professional Computer Concepts

calpcc.com

TECHNOLOGY
PEOPLE
POSSIBILITIES

How to Use This Guide

AI governance is not a ban on AI. It is the operating system for deciding which tools are allowed, what information may be used, who is accountable, and how the business responds when something goes wrong.

Best for	Owners, executives, managers, and technology decision-makers at small and midsized businesses.
Use it to	Ask better questions, identify gaps, and decide what deserves deeper technical review or managed support.

Important
A policy alone is not governance. Governance requires inventory, ownership, controls, review, and an exception process.

1. Start With the Business, Not the Tool

The first governance question is not “Which AI should we buy?” It is “What business outcomes are we trying to improve, and what risk are we willing to accept?” AI can accelerate drafting, research, analysis, customer communication, coding, and internal knowledge work. It can also amplify oversharing, bad decisions, weak permissions, and unapproved software use.

- Identify the business processes where AI is already being used, including free consumer accounts.
- Separate low-risk uses, such as brainstorming public information, from higher-risk uses involving customer, employee, financial, legal, security, or confidential data.
- Decide which outcomes require human approval before they leave the business.
- Assign one executive owner for the governance program, even if IT performs much of the technical work.

2. Build a Simple AI Inventory

You cannot govern what you do not know exists. Start with a practical inventory rather than a months-long discovery project.

Minimum AI Inventory

Check	Question / Action

☐	Which AI tools are employees using today?
☐	Are accounts personal, individually paid, team, or enterprise-managed?
☐	What business data is being entered, uploaded, connected, or synchronized?
☐	Which AI tools connect to Microsoft 365, Google Workspace, CRM, ticketing, accounting, code repositories, or other systems?
☐	Who owns each tool internally?
☐	Is there an approved business purpose?
☐	Can administrators review access, usage, or audit information?
☐	What happens to company data when an employee leaves?

3. Define Approved, Restricted, and Prohibited Use

- Approved: business use in company-managed AI platforms and approved integrations.
- Restricted: use involving sensitive or regulated information, external publishing, consequential decisions, or high-impact automation. Require defined safeguards and review.
- Prohibited: credentials, secrets, unapproved customer data, illegal activity, bypassing security controls, autonomous high-impact decisions without oversight, and unapproved AI accounts on company devices when policy forbids them.

A practical rule
If an employee would hesitate to send the information to an outside vendor by email, they should not place it into an unmanaged AI system.

4. Assign Accountability

Recommended Roles

Check	Question / Action

☐	Executive owner: sets risk tolerance and approves major exceptions.
☐	Technology owner: manages identity, access, vendor configuration, integrations, logging, and technical controls.
☐	Business process owner: decides whether AI output is appropriate for a specific workflow.
☐	Employee/user: follows approved-use rules and remains responsible for work submitted under their name.
☐	Legal/compliance advisor: consulted when the use case touches contractual, regulatory, employment, privacy, or sector-specific obligations.

5. Evaluate AI Vendors Before Approval

Vendor Review Questions

Check	Question / Action
☐	Does the business control the account and administrative roles?
☐	Does the platform support SSO, MFA, domain controls, or centralized provisioning?
☐	Are prompts, files, and outputs used to train vendor models?
☐	What are the retention and deletion options?
☐	What audit, reporting, or compliance capabilities are available?
☐	Can integrations be restricted and reviewed?
☐	How are subprocessors, data residency, and

	incident notifications handled?
☐	Can the organization export its data and remove access cleanly at offboarding?

6. Protect Data Before Expanding AI

- Review permissions before connecting AI to business repositories.
- Reduce stale or unnecessary access.
- Classify highly sensitive information and establish handling rules.
- Avoid connecting AI to entire repositories simply because the integration exists.
- Use least privilege for both people and AI-enabled applications.
- Monitor new integrations and OAuth/app consent.

7. Require Human Review Where Consequences Matter

- Require review before customer-facing, legal, financial, HR, security, or regulatory content is acted upon.
- Verify factual claims and source material.
- Do not allow AI to make final hiring, firing, credit, safety, or other consequential decisions without appropriate human and legal oversight.
- Document where AI may draft versus where a person must approve.

8. Create an Exception Process

1. User explains the business need and data involved.
2. Manager confirms the use case is legitimate.
3. Technology/security reviews the platform and access.
4. Leadership approves or rejects the exception when risk is material.
5. Exception has an owner, scope, and review date.

9. Review Governance Quarterly

- New tools or accounts discovered.
- New integrations or permissions.
- Usage trends and incidents.
- Vendor feature or contract changes.
- Employee feedback and recurring policy confusion.
- Open exceptions and whether they should be retired or formalized.
- Whether approved tools still match business needs.

The goal
Create enough structure that employees can use AI confidently, while leadership can explain

what is approved, where company data goes, and who is accountable.

30-Day AI Governance Starter Plan

6. Week 1: inventory tools and identify business owners.
7. Week 2: classify use cases and publish a short interim acceptable-use standard.
8. Week 3: review top vendors, identity controls, integrations, and data handling.
9. Week 4: approve the initial tool list, remediate obvious gaps, and schedule the first quarterly review.

SOURCES

Sources & Further Reading

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

1. NIST AI Risk Management Framework (nist.gov)
2. NIST Generative AI Profile (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