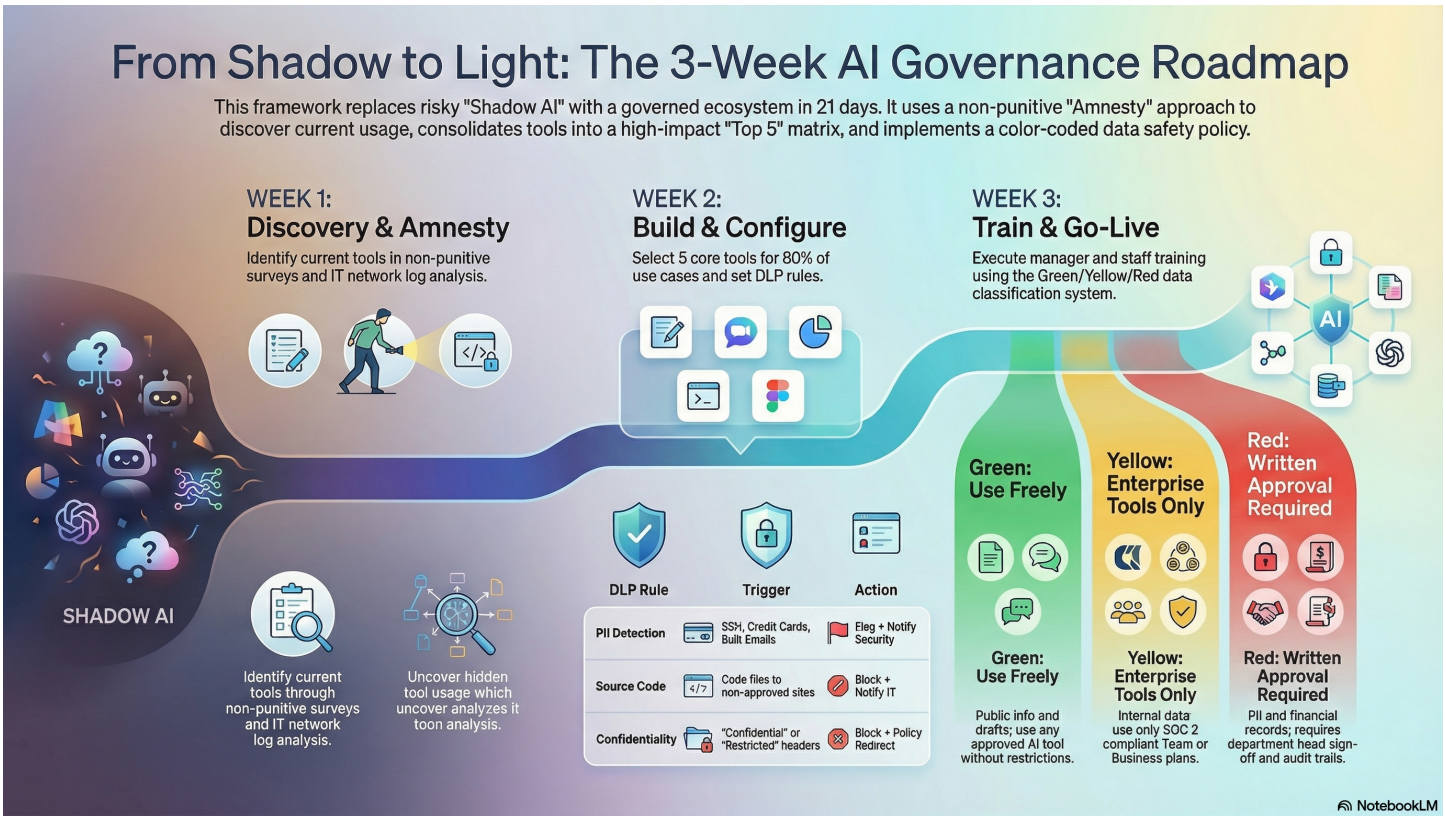
Shadow AI Governance Toolkit

The complete framework to map, manage, and govern shadow AI usage.
7 templates. 3-week deployment. Proven across organizations.



Scott Armbruster

AI Strategy & Systems Partner

23+ years in technology | 10+ years Fortune 500 consulting

scottarmbruster.com | linkedin.com/in/scottrarmbruster | info@scottarmbruster.com

What's Inside

1. Shadow AI Amnesty Audit Template
Employee disclosure form for Week 1

2. IT Discovery Checklist
Network log domains, extension audit, finance search terms

3. Approved AI Toolkit Matrix
5 use cases with ranked recommendations and evaluation checklists

4. Data Classification Policy
Green / Yellow / Red system for AI data handling

5. DLP Rules for AI Traffic
4 pre-configured rules for your DLP system

6. Training Session Outlines
Manager (2hr) and IC (1hr) agendas

7. Rollout Communication Scripts
Week 1/2/3 copy-paste announcements

+ 3-Week Deployment Timeline
Day-by-day implementation schedule

1

Shadow AI Amnesty Audit Template

Send this to all employees during Week 1. The amnesty framing is critical -- punitive language kills participation.

> *We're building an AI toolkit for the company. To make sure we choose the right tools, we need to understand what's already working. This is a no-penalty disclosure -- we want to learn from your experience, not restrict it.*

1. What AI tools do you currently use for work?

(List all tools (ChatGPT, Claude, Copilot, Midjourney, browser extensions, etc.))

2. What tasks do you use them for?

(Content writing, code review, data analysis, research, email drafting, meeting notes, etc.)

3. How often do you use each tool?

(Daily / Several times per week / Weekly / Occasionally)

4. Are you using a personal account or company account?

5. Roughly how much time does this save you per week?

6. What types of data do you typically share with AI tools?

(Public info / Internal docs / Customer data / Source code / Financial data)

7. What AI tool do you wish the company officially supported?

2

IT Discovery Checklist

Run this in parallel with the amnesty audit. Employees won't report everything -- network logs fill the gaps.

Proxy/Firewall Log Domains to Search:

```
*.openai.com -- ChatGPT, DALL-E, API
*.anthropic.com -- Claude
*.google.com/ai* -- Gemini
*.cohere.ai -- Cohere models
*.huggingface.co -- Open-source models
*.replicate.com -- Model hosting
*.midjourney.com -- Image generation
*.perplexity.ai -- AI search
*.jasper.ai -- AI writing
*.copy.ai -- AI copywriting
*.cursor.sh -- AI code editor
*.replit.com -- AI code assistant
*.otter.ai -- Meeting transcription
*.fireflies.ai -- Meeting transcription
```

Browser Extension Audit Keywords:

Search managed browser extension lists for: **AI, GPT, assistant, copilot, writer, summarize, transcribe**

Finance Audit:

Pull expense reports and corporate card transactions containing: **OpenAI, Anthropic, Jasper, Copy.ai, Midjourney, Otter, Fireflies, Cursor, Replit, Perplexity**

3

Approved AI Toolkit Matrix

The goal is to cover 80% of use cases with 5 or fewer tools. Consolidating tools reduces cost, simplifies security, and makes training easier.

General AI Assistant FOUNDATION TOOL

Recommended (in order): 1. Claude Team, 2. Gemini Business, 3. ChatGPT Team, 4. M365 Copilot, 5. Local open-source

SOC 2 compliant on Team/Business plans. No training on your data. This is your most important choice -- it will also serve as your document analysis and potentially image generation tool.

Every business is different. Your industry, existing tech stack, compliance requirements, and team size all affect which tool is the best fit. See the General AI Assistant Checklist to evaluate your options.

Code Assistant DEV TEAMS ONLY

Recommended (in order): 1. Claude Code, 2. Codex, 3. GitHub Copilot, 4. Cursor Team

Price is the biggest variable. Costs range from usage-based to $40+/user/month depending on tool and plan. No code sent to third parties on enterprise plans, local processing available on some.

Every business is different. Your language stack, repo size, security posture, and budget all matter. Pricing models vary significantly. See the Code Assistant Checklist to figure out which fits your team.

Document Analysis REUSE OPPORTUNITY

Recommended (in order): 1. Your General AI Assistant, 2. Perplexity Pro

Keep your tool count low. Whichever General AI Assistant you chose above likely handles document analysis well. Perplexity adds source citations for research-heavy workflows. Every new tool is another license, security review, and training session.

Every business is different. Your document types, compliance needs, and volume should drive this decision. See the Document Analysis Checklist to evaluate whether you need a dedicated tool.

Image Generation REUSE OPPORTUNITY

Recommended (in order): 1. Your General AI Assistant (ChatGPT or Gemini), 2. MidJourney, 3. Gemini

Reuse first. ChatGPT and Gemini both have image generation built in. If your team needs higher-fidelity creative output, MidJourney is the next step. Commercial usage rights on all recommended options.

Every business is different. Your creative volume, brand guidelines, and quality bar all affect this choice. See the Image Generation Checklist to decide if built-in is enough.

Meeting Transcription CHECK EXISTING TOOLS

Recommended (in order): 1. Your existing meeting platform, 2. Your General AI Assistant, 3. Otter.ai Business, 4. Fireflies.ai

Check what you already have first. Zoom, Teams, and Google Meet all have built-in AI transcription now. Only add a dedicated tool if your existing stack falls short. Critical: validate the Enterprise Data Protection policy of any transcription tool -- meetings often contain sensitive data.

Every business is different. Your meeting platform, recording policies, and data sensitivity should guide this choice. See the Meeting Transcription Checklist to audit what you already have.

The 80% rule: These 5 use cases cover the vast majority of what your team needs. There are hundreds of AI tools on the market, but every tool you add is another license, security review, and training burden. Start here, measure adoption, and expand deliberately. Review the Use Case Checklists if you want to dive deeper into any category.

Negotiation tip: Contact vendors directly and reference that you're consolidating from multiple individual accounts to one enterprise agreement. Most will offer annual discounts of 40-60%.

4

Data Classification Policy for AI Usage

Print this. Hang it in every team area. Three colors, three rules.

GREEN -- Use Freely

- Public information
- Marketing copy and blog drafts
- General research questions
- Code from open-source projects
- Meeting agenda planning
- Email drafting (non-sensitive)

Rule: Any approved tool. No restrictions.

YELLOW -- Business Tools Only

- Internal process documentation
- Non-sensitive business data
- Aggregated (anonymized) metrics
- Internal presentations
- Product feature brainstorming
- Competitive analysis

Rule: Enterprise-grade tools only (Team/Business plans). No personal accounts.

RED -- Approval Required

- Customer PII or data
- Financial records
- Strategic plans and roadmaps
- Proprietary source code
- Legal documents
- Employee records

Rule: Written approval from department head + IT. Full audit trail required.

5

DLP Rules for AI Traffic

Configure these in your existing DLP system (Microsoft Purview, Symantec, Forcepoint, etc.). Flag first, block later. Blocking on day one creates workarounds.

Rule 1: PII Detection on AI Domains

Trigger: SSN patterns (XXX-XX-XXXX), credit card numbers (16-digit), email addresses in bulk (10+)

Action: Flag + notify security team. Do not block.

Scope: All AI-related domains from the discovery checklist

Rule 2: Source Code Exfiltration

Trigger: Files with extensions .py, .js, .ts, .java, .go, .rb sent to non-approved AI domains

Action: Block + notify both user and IT

Scope: Exception: Approved code assistants (GitHub Copilot, Cursor Team)

Rule 3: Confidential Document Upload

Trigger: Documents containing "Confidential," "Internal Only," or "Restricted" in headers/footers

Action: Block + redirect to policy page explaining approved alternatives

Rule 4: Bulk Data Transfer

Trigger: CSV, XLSX, JSON files over 1MB sent to any AI endpoint

Action: Flag + require manager approval within 24 hours

6

Training Session Outlines

Two sessions cover the entire organization. Run the manager session first.

Manager Training -- 2 hours

1. Why shadow AI happens (15 min)

Employees trying to be productive, not malicious. Show the 75%/78% stats.

2. The real risks (20 min)

Data leaks, compliance fines, IP exposure. Use the $200K breach cost stat.

3. How to spot shadow AI (15 min)

Sudden productivity jumps, new expenses, unfamiliar browser extensions.

4. Response framework (20 min)

Educate, don't punish. Redirect to approved tools. Escalate only for Red data.

5. Approved toolkit walkthrough (30 min)

Live demo of each approved tool. Show managers how to use them first.

6. Q&A; + scenarios (20 min)

Walk through 5 real scenarios. "What do you do when..." format.

Individual Contributor Training -- 1 hour

1. Your approved tools (15 min)

Here's what you have access to. Here's how to get accounts set up.

2. Getting the most out of them (15 min)

Top 5 prompts per tool for your department. Live examples.

3. The Green/Yellow/Red system (10 min)

What data goes where. When in doubt, ask. No penalties for asking.

4. What NOT to do (10 min)

No customer data in personal accounts. No confidential docs. No shadow extensions.

5. Who to contact + Q&A; (10 min)

AI help desk contact. How to request new tools. Feedback channel.

7

Rollout Communication Scripts

Copy, customize, send. Tone matters -- these build buy-in, not compliance fear.

Week 1: Amnesty Announcement

"Team -- we're going all-in on AI. Not banning it. Embracing it."

"Over the next three weeks, we're building an official AI toolkit that gives everyone access to powerful, secure AI tools. To make sure we pick the right ones, I need your help."

"Starting today, we're running a two-week AI usage survey. This is a no-penalty disclosure. I don't care what you've been using -- I care about what's been working. Your input directly shapes which tools we officially support."

"Please fill out the survey by [DATE]. The more honest you are, the better your toolkit will be."

Week 2: Toolkit Announcement

"Thanks to everyone who participated in the AI survey. We heard you."

"Based on your feedback and our security review, here are the official AI tools now available to the entire team: [LIST TOOLS]. Accounts are being provisioned this week -- you'll get setup instructions by [DATE]."

"These tools cover the use cases you told us about. They're enterprise-grade, meaning your data stays private and we maintain compliance. If you need something not on the list, there's a request process -- we'll evaluate new tools quarterly."

Week 3: Training + Go-Live

"Your AI training sessions are scheduled for [DATES]. Attendance is required -- but I promise it's the most useful hour you'll spend this month."

"You'll learn exactly how to get the most out of your new tools, including specific prompts for your role. You'll also learn the simple Green/Yellow/Red system for knowing what data is safe to use with AI."

"After training, you're free to use approved tools without restrictions for Green and Yellow data. Questions? Reach out to [AI HELP DESK CONTACT]."

3-Week Deployment Timeline

Day-by-day implementation schedule. Run IT discovery and amnesty audit in parallel during Week 1.

Week 1: Discovery

Days 1-2

- IT/Security/HR alignment meeting
- Send amnesty audit to all employees
- IT begins network log analysis

Days 3-5

- Finance pulls AI-related expenses
- Collect and analyze survey responses
- Identify top shadow AI tools in use

Week 2: Build

Days 1-3

- Select and approve toolkit (use matrix above)
- Negotiate enterprise licenses
- Configure DLP rules (flag mode)

Days 4-5

- Provision accounts for all employees
- Create data classification poster
- Prepare training materials

Week 3: Deploy

Days 1-3

- Run manager training sessions
- Send toolkit announcement
- Run IC training sessions

Days 4-5

- Go live with approved tools
- Monitor DLP flags (first 48 hours critical)
- Establish AI help desk channel

Need Help Deploying This?

This framework has been implemented across organizations of all sizes -- from 50-person startups to 5,000-employee enterprises -- and consistently turns shadow AI from a risk into a competitive advantage. If you want hands-on help running the audit, selecting tools, or training your team, let's talk.

Scott Armbruster

AI Strategy & Systems Partner

Website: scottarmbruster.com

LinkedIn: linkedin.com/in/scottrarmbruster

Email: info@scottarmbruster.com

Services: scottarmbruster.com/agency