FREE RESOURCE

Shadow AI Discovery Kit

A checklist of where unsanctioned AI hides, plus a 30-day plan to find and triage it.

For CROs, CISOs, and Heads of Model Risk

SYNOPRA
AI AGENT GOVERNANCE & CONTROLS

5
places to look

30
day discovery plan

4
triage outcomes

What counts as shadow AI

If nobody inventoried it, nobody governs it. Four common forms:

1 **Personal accounts on public tools**

Staff paste work data into free chatbots using personal logins.

2 **AI features switched on inside approved SaaS**

A vendor adds an assistant or agent to a tool you already bought.

3 **Unapproved AI tools and extensions**

Transcription bots, browser add-ons, and code assistants adopted by teams.

4 **Homegrown agents and scripts**

Workflows built on personal API keys, with no review or logging.

Five places shadow AI hides

Work through them in order. Each gets its own checklist.

1	**SaaS and network logs**	Traffic to AI domains, OAuth grants
2	**Browser extensions and endpoints**	Add-ons and desktop apps
3	**Expense reports and procurement**	Cards, small contracts, renewals
4	**API keys, code, and cloud**	Keys, repos, agent frameworks
5	**Approved vendors and people**	Embedded features, survey, amnesty

1. SaaS and network logs

Start where the data already exists.

- [ ] **Pull DNS and proxy logs** for known AI domains (chatbots, copilots, transcription, image tools).
- [ ] **Review CASB or SWG reports** for new AI apps and top upload destinations.
- [ ] **List OAuth grants** in Google, Microsoft, and Slack, then flag AI apps with broad scopes.
- [ ] **Check SSO and identity logs** for sign-ins to AI tools you did not provision.
- [ ] **Look for file uploads** of customer or internal documents to AI services.
- [ ] **Rank the results** by user count and data volume, not by app name.

Tip: a short list of 20 to 30 AI domains is enough to start.

2. Browser extensions and endpoints

What runs on laptops often never touches a server log.

- [ ] **Export installed extensions** from managed Chrome, Edge, and Firefox fleets.
- [ ] **Flag AI extensions** that read page content, email, or documents.
- [ ] **Inventory desktop apps** with AI assistants, meeting recorders, and note takers.
- [ ] **Check local model runners** and developer tools on engineering machines.
- [ ] **Review MDM and EDR data** for software outside the approved catalog.
- [ ] **Note unmanaged devices** that reach company data, since they bypass every list above.

3. Expense reports and procurement

Money leaves a trail even when logs do not.

- [ ] **Search card and expense data** for AI vendor names and small recurring subscriptions.
- [ ] **Review purchase requests** under the formal procurement threshold.
- [ ] **Check free trials** that quietly converted to paid plans.
- [ ] **List contracts** with AI clauses on data use, training, or retention.
- [ ] **Ask finance** for the ten largest new software line items this year.
- [ ] **Match each vendor** to a named business owner, or mark it unowned.

4. API keys, code, and cloud

Where agents are built, and where they quietly act.

- [ ] **Scan code repositories** for AI provider keys and SDK imports.
- [ ] **Check cloud billing** for AI and model-serving services nobody announced.
- [ ] **List agent and workflow tools** such as n8n, Zapier, and custom scripts, with their owners.
- [ ] **Review service accounts** used by agents, and what each one can reach.
- [ ] **Rotate exposed keys** and move the keys you keep into a managed secrets store.
- [ ] **Ask what each agent can do** read only, write, or take actions with money or customers.

Agents that act matter most. Prioritize them over tools that only summarize.

5. Approved vendors and your people

The AI you already bought, and what employees will tell you.

- [ ] **Ask top vendors in writing** which AI features are on, what data they use, and who processes it.
- [ ] **Review recent release notes** for new assistants or agents added to approved tools.
- [ ] **Run a short, blame-free survey** asking which AI tools people use and why.
- [ ] **Offer a 30-day amnesty** so teams can declare tools without penalty.
- [ ] **Interview three power users** per function to learn real workflows.
- [ ] **Publish a simple request path** so approved use is easier than hiding it.

Triage each finding in minutes

Score three questions, then pick one of four outcomes.

What data does it touch?

Public, internal, customer, regulated

Can it take actions?

Reads only, writes, or acts on its own

Who is affected?

Staff, customers, regulators

STOP

Regulated data or autonomous action, no controls. Disable now.

CONTAIN

Real value, real risk. Restrict data and add logging.

GOVERN

Move into the inventory with an owner, tier, and controls.

ALLOW

Low risk and documented. Record it and move on.

The 30-day plan

Four weeks from first look to a governed inventory.

1 Week 1

Scope and sweep

Name an owner. Pull logs, billing, and extension data. Send the amnesty notice.

2 Week 2

Verify and add

Run the survey and vendor questions. Interview power users. Merge every source into one list.

3 Week 3

Triage

Score each finding. Decide Stop, Contain, Govern, or Allow. Stop the worst first.

4 Week 4

Govern and report

Assign owners and tiers. Log decisions. Brief leadership on what you found and fixed.

Record every finding the same way

These fields turn a discovery list into evidence an examiner can read.

- [ ] **Tool or agent name** and vendor
- [ ] **Business owner** a named person
- [ ] **How it was found** source and date
- [ ] **Data it touches** highest sensitivity
- [ ] **What it can do** read, write, or act
- [ ] **Risk tier** and triage outcome
- [ ] **Controls in place** logging, approval, masking
- [ ] **Next review date** who signs off

Next steps

1

Classify what you found

Use the free Risk Tier Classifier at synopra.com/classifier.html.

2

Score your governance readiness

Take the 3-minute check at synopra.com/assessment.html.

3

Want help running the 30 days?

Request a 30-minute governance briefing at synopra.com.

This kit provides general information to support internal discussion. It is not legal, regulatory, or compliance advice.