

SafeAI Zero Essentials

SafeAI™

Practical AI governance for real organizations

<https://safeaiengine.com>

A short starter kit with a one-page overview and three simple templates for basic AI governance.

Part 1 – One page overview

How to use this starter kit

Use the one-page overview and the three templates once for every AI use case. The goal is not perfection, but to ensure each use case has a clear owner, understood data, and simple guardrails before it goes live. Use this kit before you design, build, or put an AI system into production.

Who should fill this in?

- A **business owner** who is accountable for outcomes.
- A **technical owner** who understands how the system works.
- Optional but helpful: someone from **risk, security, or compliance** for higher risk use cases.

You can complete this in a 30-minute conversation.

Step 1. Capture the AI use case snapshot

Use **Template 1** to answer six basic questions:

who owns it, what it does, what decisions it supports, and what happens if it is wrong.

If you cannot describe the use case clearly here, it is not ready for design or build.

Step 2. Check data and risk at a basic level

Use **Template 2** to list the main data sources, flag personal or regulated data, and note any external AI or vendors.

- You do not need exact legal language. You do need an honest view of whether this use is low, medium, or high risk.

- If you answer "unsure" for data permission or mark the risk as "high", the use case should not go live without a deeper review.

Step 3. Agree simple controls and monitoring

Use **Template 3** to decide three things:

- when a human is involved, what you will watch, and what will cause you to pause or rollback the system.
- Keep it practical.
- Two or three metrics and one clear trigger to stop are enough at this stage.

Step 4. Store and review

- Keep this completed page with your AI inventory, project folder, or risk register.
- For active, higher risk or business critical use cases, review Templates 2 and 3 at least once a year or after major changes.
- If anything important changes (data, vendor, purpose), update this page.

If you consistently complete these three templates for every use case, you already have a basic AI governance layer in place.

Part 2 – Templates

Template 1 – AI use case snapshot

Use this to capture the basic facts about the AI use case.

Field	Your notes
Use case name	
Business owner	Person or role accountable for outcomes.
Technical owner	Person or team responsible for build and operation.
What it does	One sentence in plain language.
Decision type	Info only / Recommendation / Approve / deny / Automatic action.
Worst realistic impact if wrong	Low / Medium / High / Critical. Add a short explanation.

Template 2 – Data and risk essentials

Use this to check whether the use case is doing anything risky with data.

Field	Your notes
Main data sources	List key systems or datasets used.
Personal data used	Yes / No / Unsure.
Sensitive or regulated data	Yes / No / Unsure. Examples: banking, health, payment, other regulated data.
External AI or vendor involved	Yes / No. If yes, name the provider or product.
Are we allowed to use data this way	Yes / No / Unsure. High level view is enough here.
Overall risk level	Low / Medium / High. Add one line explaining why.

If "**Unsure**" appears often or the overall risk is "**High**", pause this use case and request a deeper review before it goes live.

Template 3 – Controls and monitoring mini plan

Use this to agree minimum guardrails and how you will keep an eye on the system.

Field	Your notes
Human in the loop	Who can review or override AI outputs and in which situations.
When we must not rely on the AI	Examples of cases where a human must decide instead of the AI.
How users know AI is involved	What, if anything, staff, or customers are told about AI involvement.
What we will watch	2–3 indicators. Examples: complaints, override rate, obvious errors, key performance metric shifts.
How often we will check	Daily / Weekly / Monthly. Include who is responsible.
When we pause or rollback	Clear trigger to stop or rollback. Example: spike in complaints, repeated bad decisions, data incident