Gnotek
Think before you automate

Seven governance failures appearing repeatedly in organizations experimenting with AI.

1. No AI policy at all

Most companies currently allow employees to use AI tools without any formal guidance.

Typical reality:

- Employees using ChatGPT, Claude, or Gemini on their own.
- No written rules regarding data usage.
- No definition of acceptable or prohibited AI applications.

Risk

Sensitive company information may be pasted into public models.

Examples seen in real incidents:

- internal financial forecasts
- customer data
- proprietary product details

Governance fix

*Create an **AI Acceptable Use Policy** that defines:*

- what tools may be used
- what data cannot be shared
- human review requirements

2. No Ownership of AI Decisions

Organizations deploy AI tools but *no one formally owns the outputs.*

Typical scenario:

A marketing team generates content with AI.

Who is accountable if:

- the content is wrong?
- it violates copyright?
- it contains hallucinated facts?

Without governance, responsibility becomes ambiguous.

Governance fix

Assign **clear AI accountability roles**:

Role	Responsibility
Executive sponsor	strategic oversight
AI system owner	operational responsibility
Human reviewer	approval before use

This aligns directly with **Gnotek Ai**'s constitutional principle that **human agency remains central**.

3. AI Is Implemented Before the Problem Is Understood

This is extremely common.

Companies begin with the question:

"Where can we use AI?"

Instead of:

"What problem are we solving?"

The result:

- unnecessary automation
- fragile workflows
- unclear ROI

The **Gnotek Ai** manifesto explicitly warns about this pattern.

Governance fix

Require a *use-case definition step* before any AI deployment.

Typical review questions:

- What decision is AI supporting?
- What data does it require?
- What error tolerance is acceptable?

4. No Model Transparency

Organizations adopt AI tools but *do not understand how they work*.

For example:

- which model is being used
- how data is stored
- whether prompts are logged
- whether outputs are retained for training

This creates both **security and compliance risks**.

Governance fix

*Maintain an **AI inventory registry** listing:*

- model provider

- data inputs
- system purpose
- risk level

This is a standard requirement in most governance frameworks.

5. No Monitoring of AI Performance

AI systems change behavior over time.

Reasons include:

- model updates
- prompt drift
- changing business data
- evolving workflows

Organizations often deploy AI once and assume it will perform consistently.

Risk

Outputs gradually degrade.

Example scenarios:

- customer support AI giving outdated information
- analytics GPTs producing incorrect insights

Governance fix

*Implement periodic **AI review cycles**:*

- quarterly performance review
- error tracking
- output sampling

6. Over-Automation

Another governance failure occurs when organizations automate too aggressively.

Common pattern:

1. AI generates analysis
2. AI makes decisions
3. Humans removed from the loop

This is dangerous because **AI systems are probabilistic**, not deterministic.

In sensitive areas like:

- hiring
- finance
- legal analysis

human oversight remains essential.

Governance fix

Define **human-in-the-loop thresholds**.

Example:

Task	Human Review Required
Internal brainstorming	optional
Client communication	recommended
Financial or legal decisions	mandatory

7. No AI Risk Classification

Many companies treat all AI uses the same.

But risk varies dramatically.

Example comparison:

AI Use	Risk
Brainstorming marketing ideas	low
Generating financial projections	moderate
Evaluating job candidates	high

Without classification, companies apply the wrong level of oversight.

Governance fix

Create a **risk tier system** similar to what regulators are moving toward.

Example structure:

Risk Tier	Governance Level
Low	minimal oversight
Moderate	human review
High	formal governance review