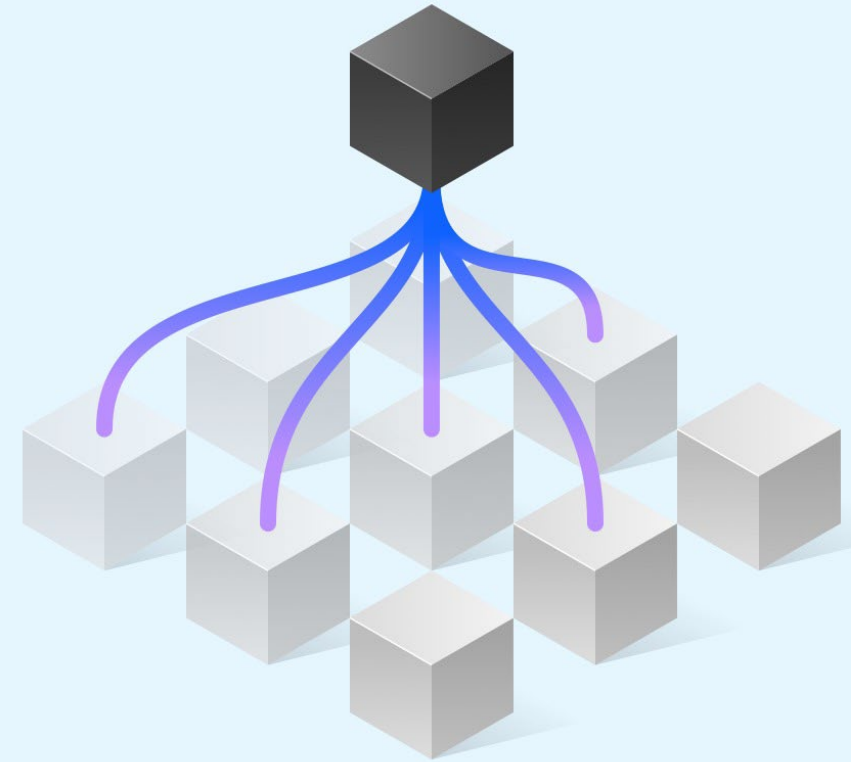


From Prompting Chaos to Consistency: The 6-Pillar Framework for Scalable AI Outputs

What is an LLM and how does it “Think”?

LLMs predicts what word is most likely to come next.

- Learned how people write by reading huge amounts of text and documents on various subjects over, and over, and over again.
- Memorized patterns, structure, and probabilities.
- Uses this knowledge to predict the most likely next word based on the input it receives.



Your Brain Predicts Patterns Too

See you later..... Alligator

How many times have you heard this expression in your lifetime?

It's fun to stay at the..... YMCA

Who hasn't heard this lyric?

Notice how you aren't thinking when generating these answers. You've just seen it so many times it is essentially a reflex. This is very similar to how LLMs work.

Example LLM Apps



Chat GPT



Claude



Gemini



DeepSeek

How your output is produced

- The LLM has its own “knowledge” based on the data it was exposed to.
- You ask it or prompt it to do some task

Output = LLM “knowledge” + Your input

You can't change what the LLM was trained on. You can only control the second part of the equation, what you give it.

Prompt Format: The 6-Pillars of Prompting

1. **Persona:** Who is the AI, what role is it taking on?
2. **Context:** What is the background, Situation, or Goal?
3. **Task:** What is the explicit job that needs to be done?
4. **Constraints:** What are the guardrails, what tone should be used
Tone?
5. **Examples:** An Example, or structure of an example.
6. **Format:** How should it look? What structure should it have?

Lab Portion

Restrictions & Best Practices

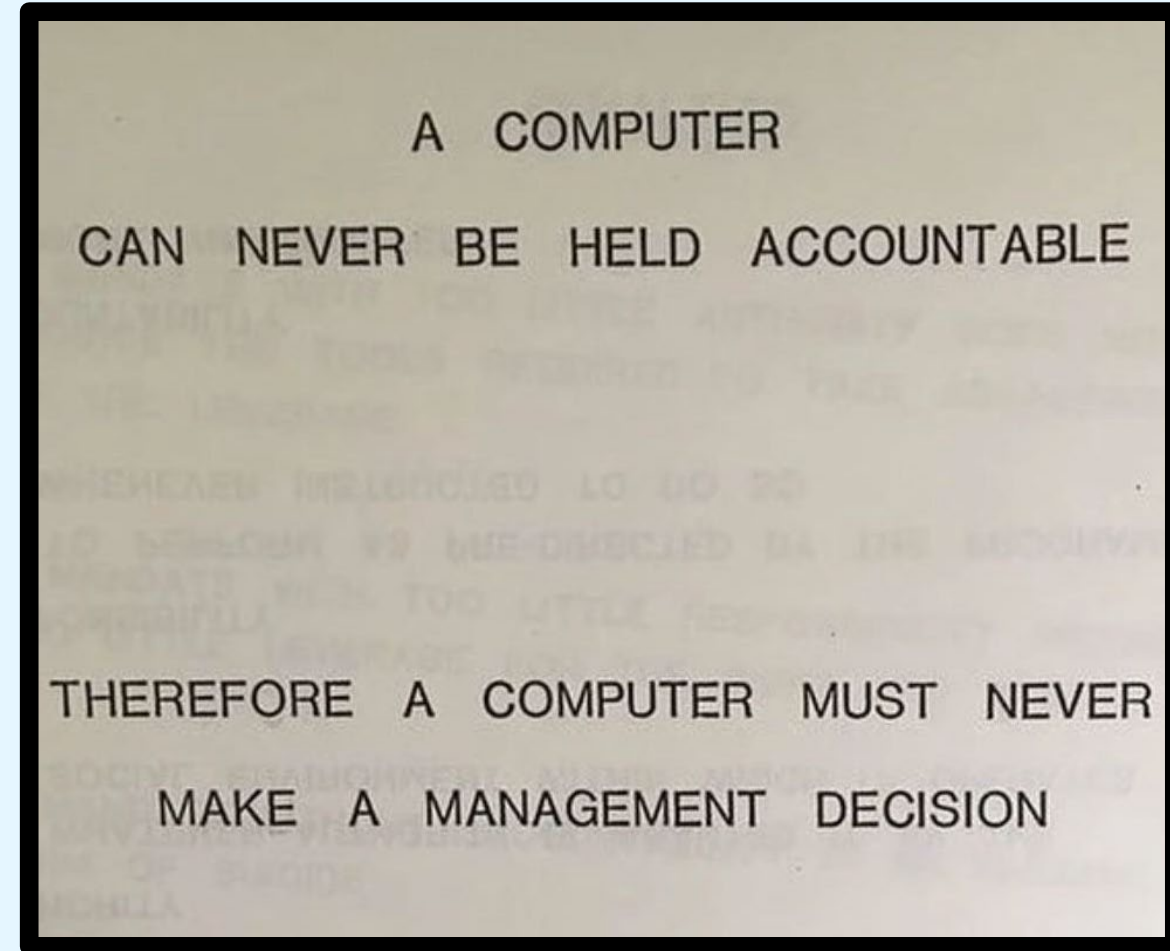
Keep Prompts Clear and Concise

- Aim for about **50–300 words**.
- Provide just enough context for clarity.
- Avoid unnecessary details that don't contribute to the task.
- Focus on being clear, specific, and relevant.

Restrictions & Best Practices

Never Share Sensitive or Confidential Data

- Do not upload or include:
 - Customer or client information
 - Employee records
 - Financial data
 - Company documents, source code, or internal strategies
 - Passwords, API keys, or other sensitive credentials
- **Rule of thumb:** If you wouldn't post it publicly, don't include it in your prompt.



Restrictions & Best Practices

AI Can Make Mistakes

Large Language Models (LLMs):

- Can misunderstand instructions.
- May generate incorrect or misleading information with confidence.
- Predict likely words—they **do not think or reason like humans**.

Best Practice

- Verify important information before using it.
- Treat AI as a **helpful assistant**, not a guaranteed source of truth.
- Always double-check content that affects business decisions, customers, or compliance.

Must read: <https://bastai.substack.com/p/hey-boss-7-dead-giveaways-youre-treating?triedRedirect=true>