

Chapter 2

Peeking Inside the AI Agent Mind

IN THIS CHAPTER

- » Fitting together the parts of Agentic AI
 - » Discovering how Agentic AI remembers and adapts
 - » Linking AI agents together
 - » Keeping yourself and others in the feedback loop
 - » Understanding how Agentic AI makes decisions
-

This chapter gives you an overview of how agentic artificial intelligence (AI) operates today. You can find out how both standalone agents and a larger system of interacting agents go about their tasks. You may need a while to fully grasp the implications of an AI mechanism that performs beyond the level of following static instructions from a prompt. For now, you need to understand that Agentic AI is a giant leap in the ongoing AI evolution. This jump is like moving from riding horses as the primary mode of transportation to space travel in a single leap.

AI developers and engineers create Agentic AI to act autonomously in its pursuit of goals, decision-making, and active adaptations on the fly. Its behavior is based on changing information and context. A single agent might handle a complex task from start to finish, while in a multi-agent system, several agents coordinate with one another, each specializing in parts of a broader workflow.

In this chapter, you can discover how these AI agents plan their actions, communicate with each other, and execute tasks. You can also get a comparison of the capabilities of Generative AI (GenAI) and Agentic AI,

and a better understanding of the mechanics behind this rapidly evolving technology.

Linking the Fundamental Building Blocks

AI developers and engineers construct Agentic AI systems from interconnected components that work together. But even with all this advanced automation, Agentic AI can't function alone. Human planning and oversight create the foundation not only in the developmental and task assignment phases, but throughout the Agentic AI's existence. Developers design and build agent workflows, define roles, create feedback loops, choose the right tools, and set safety boundaries. They also determine how agents access knowledge and when to involve humans in the loop.

Identifying Agentic AI building blocks

The Agentic AI system's core includes several key building blocks that collectively enable AI agents to operate with purpose and autonomy. These building blocks include

- » **A mission or objective:** Each agent receives a clear objective from a human or derived from a broader task. The objective guides the agents and the overall system's actions. Each agent uses planning and reasoning to achieve its objective by breaking the task into smaller steps, prioritizing them, and determining the best course of action based on available resources.

When the agent encounters complex challenges that require resolution to meet the objective, the agent uses a process called *task decomposition* to map out a series of simpler, more manageable subtasks. This process isn't unique to Agentic AI and commonly takes place in project management activities, software development, and robotics. People also use task decomposition in their personal productivity efforts.

» **Short-term memory and long-term memory:** The agent uses both memory types to recall information that's relevant to its current mission:

- *Short-term memory:* Helps the agent keep track of recent actions. *Short-term* typically refers to information held within the current conversation or task session.
- *Long-term memory:* Serves to improve performance, avoid repetition, and build contextual awareness over time. Long-term memory is essential for learning — for both humans and machines. *Long-term* refers to information stored persistently between sessions in mechanisms such as databases or vector stores.

» **Tool linkage and use:** Agentic AI can't and doesn't act in isolation. It must interact with software tools, application programming interfaces (APIs), databases, and even other AI models to gather information, execute actions, and generate outputs. Technologies such as LangChain, AutoGen, and OpenAI's function calling help to link agents with external tools:

- *LangChain* helps AI agents interact with external data by using chains of reasoning. In this context, “chains of reasoning” refers to the framework's core concept of chaining together multiple steps or components to accomplish complex tasks that require sequential processing and decision-making.
For example, in a use case, an agent can use LangChain to pull real-time stock prices from a financial API, process that information, analyze it, and summarize the results for human consumption.
- *AutoGen* allows multiple AI agents to collaborate and call tools or APIs, as needed. For example, when using AutoGen, one agent in the system can write computer code, while another runs it and returns with the output.
- *OpenAI's function calling* lets generative pre-trained transformer (GPT) AI models trigger external tools by

defining functions in the code. A weather chatbot can use function calling to access and retrieve live data from a weather API, for instance.

New protocols such as Model Context Protocol (MCP), Agent Network Protocol (ANP), Agent-to-Agent (A2A) protocol, and Agent Communication Protocol (ACP) also help agents interact with other AIs, data sources, and software. You can find out more about these protocols in [Chapter 3](#).



REMEMBER World modeling offers another way in which AI agents can connect and use resources in more sophisticated ways. World modeling gives an agent the ability to build an internal representation of the environment that it's working in. Think of this capability as the ultimate in providing context to aid AI's understanding of the many nuances, conditions, and restrictions inherent to any given environment. And the agent can get far more context from working in a digital workspace, a data ecosystem, or any scenario that exactly replicates its existence in the real world. I talk more about world models in [Chapter 3](#).

- » **Communication and coordination:** Agents need to share updates, delegate subtasks, resolve conflicts, and sync progress within themselves and with other agents in the system. Agentic AI systems achieve this sharing by using frameworks that enable messaging, state management, and collaborative decision-making, among other capabilities.

Enter the overseers

Without good planning and oversight, agentic systems can fail, suffer from model drift, or even create unsafe and disastrous events in the real world. After all, these systems aren't like yesterday's chatbots, prompted to perform on command and on task. These AI agents act largely on their own initiative.

Before you panic over AI agent autonomy, think about horses that are trained to perform tasks, from arena acts to tourist trail riding and field plowing. Horses typically do perform as expected, but when they don't, a rider or the horse itself can be seriously harmed. Additionally, if the horse doesn't have the right tools, such as a bridle, reins, or a plow, the horse either won't or can't perform to expectation.



REMEMBER Although Agentic AI can carry out tasks autonomously, it relies on human design and oversight — as well as interactions with the right technologies — to truly function effectively and responsibly.

Exploring Reasoning, Memory, and Goal Setting

In this section of the chapter, I talk about how Agentic AI systems think, remember, and plan. In essence, Agentic AI systems use three cognitive processes that mimic human intelligence:

- » Reasoning through problems
- » Remembering and applying past and present relevant information
- » Setting and pursuing goals

This mimicking of human thought processes is entirely new territory for machines. Make no mistake, this astounding technological achievement took longer than you may think to arrive. Agentic AI is the natural evolution of decades of work in autonomous and multi-agent systems. Specifically, the branch of AI focused on machines that can perceive their environment, make decisions, and act on their own. The *agentic* label (popularized by social scientist Albert Bandura in the 1980s) borrows from psychology's concept of *agency*, which means the ability to act intentionally rather than just react.



TIP Oversight of Agentic AI systems requires setting goals and guidelines for agents carefully and supervising the agents vigilantly. The agents don't think, *per se*, but rather mimic human thinking. Although human thinking is fallible, the processes that pass as machine thinking are sometimes even more so.

Understanding how these machine-thinking processes work can help you grasp both the power and limitations of current AI agents.

Assessing Agentic AI reasoning

Agentic AI reasoning refers to the system's ability to process information, analyze situations, draw conclusions, and determine appropriate actions. This complex computational process can produce remarkably sophisticated problem-solving behavior.

But the AI reasoning capability doesn't include other human abilities that people routinely use when solving a problem. These added and distinctively human superpowers include, but are not limited to

- » **Creative intelligence:** Generate new ideas and solutions to problems by combining originality, flexibility, and problem-solving skills across various domains.
- » **Intuitive intelligence:** Make decisions and solve problems instinctively, relying on gut feelings and subconscious processing.
- » **Moral intelligence:** Distinguish right from wrong and act based on ethical values such as integrity, responsibility, forgiveness, and compassion.
- » **Intrapersonal Intelligence:** Self-awareness and understanding one's own emotions, motivations, and goals.
- » **Naturalistic intelligence:** Recognize, categorize, and draw upon features of the environment.
- » **Emotional intelligence:** Recognize, understand, and manage one's own and others' emotions.

- » **Existential intelligence:** Ponder deep questions about existence, life, and death.
- » **Musical intelligence:** A sensitivity to sounds, rhythms, and music, which musicians, composers, and conductors typically have to produce the *it factor*.



TECHNICAL STUFF

The *it factor* is the elusive spark of emotional authenticity and creative intuition that makes a performance feel alive. By contrast, machine-made music often lacks that essence. It may be technically flawless, but it *lies flat*, meaning the music fails to stir emotion or truly resonate with human hearing.

Considering AI's limited intelligence

The type of intelligence that AI seeks to replicate is *analytical intelligence*, which is the ability to analyze, evaluate, and manipulate information to solve problems and make decisions. However, AI doesn't use the full breadth and scope of analytical intelligence components, which include critical thinking, logical reasoning, abstract thinking, and problem-solving.



REMEMBER Analytical intelligence doesn't perform at its fullest in a vacuum. When other forms of human intelligence (listed in the preceding section) are also in play — meaning combined and working with analytical intelligence, especially in the problem-solving and decision-making aspects — you get enhanced results derived from analytical intelligence.

Now, you may be thinking “Wait a minute! IBM’s AI won against expert players at the game of chess using only analytical thinking!” Yes, indeed — IBM’s Deep Blue did that. But that’s comparing apples to oranges. Deep Blue was initially built specifically as a chess engine and performed under precise conditions in a highly constrained environment.

Narrow AI successes — such as chess wins — don't provide proof that the AI can replicate the same level of success when solving general or disparate problems in varying conditions and without the benefit of a constrained environment. However, these successes do show that narrowly focused AIs are quite good at what they do. To this day, an AI specialized for a certain task can often outperform a general use model, but only within its intended scope.

Recognizing its intentional design

This idea of task specialization (see the preceding section) clarifies the design of Agentic AI systems that deploy multiple AIs; each agent is specialized to its part of the system's overall mission. Because of this design, many people and companies place more value on employing Agentic AI than on simply evolving GenAI models to higher performance standards.

The people using these technologies are betting that an orchestrated team of specialized AIs can outperform a general model with added capabilities for executing well-defined work processes. This may seem to be a safe bet, but Agentic AI is in its infancy, so the people and companies need to wait and see how well this team approach to autonomous specialized AI plays out before investing too heavily in it.

Evaluating Agentic AI memory

Agentic AI memory refers to its capability to store and recall past data and workflows that it can then use to inform present decisions and future predictions. People think of Agentic AI memory as working similarly to how a person remembers, which can help them understand the broader concept but doesn't tell the whole story.



REMEMBER In reality, AI doesn't remember in the human sense; instead, it functions as structured data retention and retrieval. Memory stores information that AI agents can retrieve to build continuity, maintain context, and behave in ways that appear intelligent and responsive over time.

In the absence of memory, every AI interaction would start from the beginning point with no awareness of what happened previously, and therefore, without benefit of the data gleaned from previous actions to draw upon. Consider how much you can enhance system performance just by making memory a capability. For example, agents can remember user preferences, refer back to earlier steps in a task, or adjust their behavior based on the outcome of a prior decision or a change in conditions. This is collectively referred to as the agent *learning over time*.

Adding memory to a system's design

Adding memory to an AI entails more than adding a device that has search functionality. Specialized technologies and tools support the Agentic AI memory by handling the storing, retrieving, and updating of information. (I talk about these types of tools in the section “[Identifying Agentic AI building blocks](#),” earlier in this chapter.)

In platforms such as LangChain, memory modules such as ConversationBufferMemory or VectorStoreRetrieverMemory help manage dialogue history and relevant knowledge. These tools allow an agent to access and reuse earlier conversations, a capability that’s especially important for long-form tasks such as writing, customer service, or complex decision-making.



TECHNICAL STUFF

In platforms that have memory modules, the AI model or the AI system often transforms the stored information into *vector embeddings* — which are mathematical representations of words or ideas — that the system can retrieve as related content, even if the prompt or the query wasn’t phrased exactly the same way each time. For example, retrieving information about *customer complaints* when your instructions ask about *user feedback* is important even when the exact words don’t match.

Agentic AI systems often pair vector databases, such as Pinecone or Facebook AI Similarity Search (FAISS), with memory modules to

manage larger volumes of information. Vector databases can help an agent search across documents, chat history, or contextual knowledge quickly and efficiently. For example, an agent might use Pinecone to retrieve previous customer support tickets that are similar to the current inquiry, which can help the agent provide better answers based on past outcomes.

Blending memory and reasoning in the design

More advanced agentic architectures use patterns such as *ReAct*, a term that's short for *Reason+Act*, which blends memory with real-time reasoning. In this approach, the agent remembers previous actions taken and the results those actions produced. The agent can then use that information to make assessments and decisions to guide its next steps. This type of design can really provide a big advantage in flexibility and responsiveness in dynamic environments — where change happens continually — such as when an agentic system troubleshoots software or performs research in which outcomes change based on each interaction.

Without question, including memory in Agentic AI provides substantial benefits in performance. Interactions between AI agents and humans feel more natural and less repetitive. If you ever encountered a system that requests the same information from you several times throughout the process, even though you gave it the same information every time it asked, you probably see this development as great news.

Similar to how Agentic AI can remember what it learned before, it can improve its own process for completing tasks because it doesn't have to repeat steps it has already taken or now understands.

The memory/reasoning blend also helps an agent complete complex tasks in which previous steps influence what happens much later. For example, if an agent is executing a marketing campaign, it must remember which assets are approved for public distribution and which are still in the draft stage.

Getting (too) personal with memory

Agentic AI can remember who you are and distinguish your personal habits, goals, or preferences from those of a zillion other people with

whom it may interact. This capability is called *personalization*, and because of memory and better context, Agentic AI can take personalization to a deeper level. Whether that extra insight makes the Agentic AI seem helpful, flattering, or creepy to you or your customers depends on how well the people who made the AI defined its mission and guardrails, as well as your or the end user's perceptions, and not usually on the AI's interpretation of its mission. But there are occasional exceptions.

And that potential creepiness factor brings us to the downsides of Agentic AI memory. Consider these factors:

- » **Systems that use only short-term memory reset after each session** — unless developers explicitly program them to retain information across time. System memory loss can upset or frustrate people who expect the agent to remember things it was never designed to recall.
- » **Long-term memory capabilities can exacerbate privacy and security concerns**, build biases in the AI, or even add confusion in the AI's decision-making processes. Data management, always a critical issue in AI, becomes increasingly important in Agentic AI because the AI memory may not include subsequent policy changes and data updates.

In short, memory transforms an agent from a reactive tool to a more sophisticated and context-aware assistant. Memory bridges the gap between a routine, repetitive automation and sustained, intelligent support.

Grasping Agentic AI goal setting

Agentic AI goal setting is the process that a developer or user uses to give the agent direction. Goals can be simple or complex. Instead of following explicit step-by-step instructions — like GenAI models do when creating content in reaction to your prompts GenAI — Agentic AI agents interpret broader objectives and determine what specific outcomes to pursue on their own.

Agentic AI systems typically organize their goals in hierarchical structures and adjust goal priorities based on changing circumstances, resource constraints, or new information:

- » **Goal structure:** Systems break down high-level strategic objectives into tactical sub-goals and specific actions. For example, a goal to “improve customer satisfaction” might decompose into sub-goals such as “reduce response times” and “increase resolution rates.”
- » **Goal priority:** The agent weighs competing objectives and makes trade-offs in real time. For example, a direct shipping route is usually faster, but not if that route cuts through a natural disaster zone or a country where new regulations outlaw the product. In such a case, the agent has to weigh the advantages of a direct route against the emerging challenges on the route and make or change its shipping decision accordingly.



WARNING Goal setting is a key function that enables AI systems to operate more autonomously in complex, dynamic environments. But the autonomy can raise serious concerns in relation to *business alignment* (adherence to business-wide policies and goals) and keeping the AI agents’ actions safe and beneficial for humans. That’s why, at least for the foreseeable future, Agentic AI systems must have human oversight and are currently more likely to be semi-autonomous — except for a few restricted use cases (for example, automated stock trading that follows strict rules without human input, factory robots with limited actions, or self-adjusting climate control systems of little consequence).

Understanding Adaptive Behavior and Self-Directed Learning

What sets Agentic AI apart from other forms of AI and AI systems is its adaptive behavior. By *adaptive behavior*, I mean that the AI can self-modify its actions based on changing conditions, updated information, or previous failed attempts to reach a goal. This capability is a distinct departure from rule-based AI systems that follow a fixed sequence of programmed steps, regardless of context, conditions, or outcomes.

Self-directed learning, while still limited in current systems, refers to an agent's ability to improve its performance over time based on experience. This process may involve reinforcement learning, fine-tuning on new data, or simply adjusting preferences through accumulated user feedback. For example, a content-generation agent that frequently receives corrections about tone or audience level can incorporate that feedback into future outputs so that it produces more suitable drafts without a user needing to explicitly retrain it for each project.

Together, the capabilities of adaptive behavior and self-directed learning make Agentic AI more useful than an AI that simply executes instructions. In these systems, the agents are adjusting, optimizing, and sometimes even innovating within the scope of their respective assignments. In short, Agentic AI evolves on the fly and of its own initiative.

Dissecting adaptive behavior

Adaptive behavior enables an AI agent to evaluate progress toward its goal, assess whether its current strategy is working, and pivot to an alternative approach, if needed. This flexibility makes AI infinitely more useful in many real-world applications (such as customer service, logistics, and healthcare diagnostics) where new variables often emerge mid-task.



REMEMBER Agentic AI adaptive behavior relies on

- » **The AI's capacity to recognize patterns in its successes and failures:** It can then use those pattern insights to refine its approach. An agent constantly compares the current state of the task to the desired outcome. If it detects a mismatch, the agent can adjust its plan or tactics accordingly. It doesn't need to restart the entire process or be reprogrammed manually.
- » **A combination of memory, world modeling, and planning capabilities:** Memory allows the agent to remember prior actions, decisions, and outcomes. World modeling helps it simulate possible future scenarios and choose the best path based on logical reasoning. Planning enables the agent to restructure tasks, reprioritize steps, or incorporate new information into its execution strategy.

Delving into self-directed learning

In Agentic AI systems, self-directed learning takes adaptive behavior even further by enabling AI systems to identify what they need to learn without explicit human guidance. Rather than training on a fixed data set and then deploying unchanged, these systems actively seek out new information and experiences that help them improve their performance. For example, an agent might notice gaps in data when trying to answer certain types of questions, then autonomously seek out relevant academic papers or databases to fill those gaps.

Self-directed learning involves sophisticated mechanisms for identifying learning opportunities: *meta-learning* (learning how to learn) and *agentic reflection (self-assessment of performance)*. The process follows a path in which the AI must follow these steps:

1. **Recognize when its current knowledge base or capabilities are insufficient to achieve its current goal or complete the assigned task.**
2. **Determine what additional information or skills can provide the most meaningful improvement in its performance.**
3. **Figure out how to acquire the needed information, access, or skills — or all three.**

This learning process might involve experimenting with different approaches to see what works best, seeking out specific types of data or feedback, or even identifying entirely new domains of knowledge that could enhance its effectiveness.

Learning more than new information

In more experimental Agentic AI systems, agents may autonomously refine workflows by testing various methods. After monitoring the success of each, the agent selects the most effective strategy for future tasks. For instance, an agent performing market research might test several search strategies, such as querying academic sources, aggregating real-time news feeds, or scanning social media. It then prioritizes the most accurate or relevant method going forward.

In addition to workflow, meta-learning can affect other components of how the Agentic AI systems work. It can

- » **Require Agentic AI to develop better goal-setting and planning strategies.** The system learns not just how to achieve specific goals, but how to set more effective goals in the first place. The system can then apply the resulting meta-insights across all future goal-setting activities to improve autonomous planning.
- » **Enable Agentic AI to develop better communication and collaboration strategies.** For example, the agent may discover that certain types of explanations work better for technical versus non-technical audiences, or that specific approaches to negotiation are more effective in different cultural contexts. In these and other cases, the AI can apply those discoveries or lessons across the board. In other words, these meta-insights then guide its behavior in future interactions, too.

Examining other aspects of meta-learning

Temporal aspects of meta-learning in Agentic AI — by which I mean that the system learns to balance immediate performance with long-term learning objectives — can really accelerate the agent's overall intelligence and adaptability. The agent can have a sophisticated ability

to determine when accepting short-term inefficiency is worthwhile to achieve long-term improvement. A calculation of this nature involves developing strategies for maintaining multiple learning processes. It also requires the agent to simultaneously make quick tactical adjustments for immediate needs while pursuing slower strategic learning to adapt to future capabilities.

Environmental adaptation is another crucial aspect of Agentic AI systems, which continuously monitor their operating context and adjust their behavior accordingly. A financial trading agent, for example, doesn't just follow predetermined algorithms. The AI system also

- » **Adapts to changing market conditions**, regulatory environments, and economic indicators.
- » **Analyzes results** by noticing that patterns which previously predicted stock movements no longer provide a reliable basis for accurate forecasts. The agent then initiates a self-correction process in which it may adjust its models, retrain on recent data, or explore alternative indicators to restore predictive accuracy.
- » **Analyzes further** to diagnose the sources of deteriorating performance and test potential remedies. To correct the issue, the agent may develop new analytical approaches or adjust the weighting of key factors before proceeding to validation.
- » **Validates improvements** through rigorous *backtesting* (which bases changes on historical data) and simulated trading to ensure that incorporating new data patterns genuinely enhances performance rather than merely overfitting the agent to past data. Only after demonstrating consistent accuracy and stability does the agent reintegrate the updated strategy into active trading operations.

Directing Agentic AI

If you read the earlier sections of this chapter, you may wonder how you can instruct Agentic AI agents or systems to do your bidding. Prompting

comes to mind, I'm sure. But that's not the answer — at least not entirely.

Prompting an AI is a bit like placing an order at a diner, whereas directing Agentic AI is more like delegating a task to your executive assistant and leaving it up to them to figure out how to get that task done. An Agentic AI agent doesn't just take and fill your order, it accepts the mission that you give it and plans how to achieve that mission, what actions to take, where to go for information, and how to adapt along the way. Occasionally, the agent loops you in to check whether its progress is in alignment with what you meant or to get your permission for a key decision before it acts as a safety check to prevent mishaps.

For your part, you don't have to give step-by-step instructions in a prompt. Instead, you state the *intent*, meaning the end goal, of what you want the AI system to accomplish. Occasionally, you may need to give the AI permission to proceed with a specific recommendation or make a decision if the agent has a question of its own. For safety and compliance reasons, the agent may have its own guardrails that require it to check for your explicit permission before proceeding with an action.

In any case, you don't want to just give Agentic AI your high-level objective and call it a day. The agent needs some context so that it can better understand the mission: what needs to be done, why it matters, and how it fits your or the larger organization's goals. Specifically, you need to provide the agent with

» **Background information:** Including an explanation of constraints and preferences, and clarification about what resources the agent can or cannot access.

» **Defined success criteria that go beyond simple task completion:** For example, you can offer your expectations regarding quality standards and strategic alignment with business goals.

Talking it over with Agentic AI

An example of an interaction between you and Agentic AI might look like this:

You: Analyze our customer support logs, identify recurring complaints, and propose solutions.

Agentic AI agent: I'll categorize complaints by frequency, then cross-reference them with product updates to see whether recent changes caused new issues. Should I proceed?

As depicted in this exchange, instead of just spitting out a response like GenAI tools do, the agent might first outline its strategy in its response to you. If you answer the strategy question with *yes*, the agent is off to a running start in getting the work done. If you say *no*, and then explain what you want in more detail, the agent processes that new explanation, provides you with its updated plan, and asks permission to pursue actions on that path.

After you give the agent the go-ahead, it then begins its work autonomously or semi-autonomously, depending on how the agent or system is built to perform. It might query a live database, search the web, retrieve documents, or interact with other software systems, including other AIs, depending on what you empower it to do through your prompting.



REMEMBER Some agentic systems lean on their memory components to streamline their work on this mission. Others may rely on real-time reasoning to resolve ambiguities or fill in missing pieces. What's most striking is how they don't just follow a script; they improvise. If a source is missing, they look for alternatives. If data is inconsistent, they can flag the issue for you and may even recommend how to resolve it.

Continuing direction over the AI's work

After setting the Agentic AI agent on an agreed-upon path (see the preceding section), you still have work to do. At key decision points, the agent pauses its work and asks for a decision and/or permission to proceed. These intermittent interactions might look like this:

Agentic AI agent: Sixty percent of complaints are about slow performance, but I'm not sure if this is a server issue or a user interface problem. Should I investigate further?

You: Yes, investigate further to determine the cause or causes of the issue and provide the sources you used to make that determination, or

No, the cause of the issue is not relevant for my needs.



TIP Answer interim queries from the AI agent however you want so that the agent knows how to proceed from there. This back-and-forth interaction between you and the agent transforms AI from a passive tool (that responds to queries) into an active collaborator (that assists in solving problems).

Completing the mission and next steps

The level of oversight that you want or need with Agentic AI varies depending on the task, the risks, and your preferences. Some people prefer a hands-on role, requiring the agent to check in frequently, while others are comfortable letting the agent proceed without interruption and only want the agent to notify them when it has the final product ready.

To be clear, the system may respond with summaries, offer previews, or request decisions through dashboards, messaging platforms, or direct interaction in a natural language interface.

After the agent believes that it has reached the mission goal, it delivers the output and often suggests what to do next. A well-designed agent doesn't just drop off a report and vanish; it might follow up with a question like these examples:

- » Would you like me to format this as a presentation?
- » Should I schedule a meeting with the top vendor I identified and prepare a list of items for you to discuss?

Interacting with GenAI and Agentic AI

GenAI and Agentic AI have several key differences in the way that you communicate with them:

- » **Interaction:** GenAI offers a one-shot response, but Agentic AI provides dynamic multiple steps.
- » **Autonomy:** GenAI has low autonomy, simply reacting to prompts, whereas Agentic AI has high autonomy, planning and acting independently.
- » **Feedback:** With GenAI, you have to perform manual retries. On the other hand, Agentic AI uses built-in checkpoints to pause, review its own work, and fix mistakes on the fly.

Table 2-1 offers a concise look at the differences in interactions.

TABLE 2-1 Interacting with GenAI versus Agentic AI

Aspect	GenAI	Agentic AI
Method of interaction	Prompting	Instructing
Type of interaction	One-shot response	Multi-step, dynamic
Autonomy	Low (reacts to prompts)	High (plans and acts)
Feedback	Needs manual retries	Built-in checkpoints to monitor progress, evaluate outcomes, and self-correct

Combining Generative Abilities and Real-Time Decision-Making

In this chapter and throughout this book, I compare Agentic AI to GenAI to more easily explain how Agentic AI works and differs from the more familiar and very popular Generative AI models and tools. But in practical use, you don't have to choose only one type of AI. Agentic AI

isn't replacing GenAI. It's more like Agentic AI is giving GenAI an upgrade. Think of GenAI as the part that creates ideas and content, and Agentic AI as the part that plans, decides, and follows through. In other words, Agentic AI adds memory, reasoning, and goal-setting so the system can work toward results over time instead of just reacting to a prompt.

Nearly everyone — from students to CEOs — has experimented with GenAI tools such as ChatGPT, Claude, and Grok, experiencing firsthand these tools' remarkable ability to produce coherent, contextually appropriate outputs. These systems excel at pattern recognition and recombination by drawing from vast training datasets to help them generate plausible responses to prompts.

However, this strength also acts as the GenAI systems' fundamental limitation. They operate within the constraints of immediate stimulus and response. They lack any persistent sense of purpose or context beyond the current interaction or a smattering of instruction in its limited memory. Any actions taken on their responses must be manually undertaken or automated through another software program that the AI is integrated with.

If you want to find out more about GenAI models and tools, ChatGPT specifically, or advanced prompting techniques, check out my books *ChatGPT for Dummies* and *Generative AI for Dummies* (Wiley). I also teach several online courses about AI and prompting for business and creative uses at LinkedIn Learning (www.linkedin.com/learning).

Expanding on content generation

Agentic AI builds on a GenAI foundation, adding autonomous action to creative expression. These agentic systems inherit the ability to produce coherent, human-like language and ideas from GenAI, but Agentic AI goes much further by making decisions, setting goals, and executing plans across time and context. This isn't just a technical upgrade, it's a functional evolution in what AI can do.

Specifically, Agentic AI weaves together two critical capabilities:

» **The creative and generative power of LLMs.** The generative aspect of large language models (LLMs) remains essential. It allows Agentic AI systems to interpret human intent, draft plans, summarize information, produce content, and communicate in nuanced, context-aware ways. Without this generative engine, Agentic AI would lack fluency, flexibility, and the ability to improvise responses or understand the mission it was given. But having these abilities doesn't constitute agency.



» **REMEMBER** **The sophisticated real-time decision-making frameworks that enable independent goal pursuit.** The integration of real-time decision-making processes is what transforms an AI system's generative capability into genuine agency. Rather than static rules or pre-scripted routines, these processes are dynamic reasoning loops that provide ongoing evaluations of what's happening (reconsidering assumptions), what might happen next (adjusting strategy), and how best to proceed toward a defined objective (selecting appropriate action).

This type of reasoning is context-rich. An Agentic AI agent doesn't simply choose the next best word in a sentence in the way that a traditional LLM or GenAI tool does. Instead, it

- » **Chooses the next best action** in a sequence that may span hours, days, or longer. It considers trade-offs.
- » **Balances speed against quality** and short-term outcomes against long-term impacts.

For example, an agent might recognize that providing an immediate answer can solve the current customer service ticket, but if it takes a bit more time to uncover a pattern in the tickets, it can find a common cause to address for preventative purposes or improvement to system-wide performance.

The synergy between these capabilities creates systems that can engage in complex, multi-step problem-solving while maintaining coherent long-term strategies. For example, an Agentic AI tasked with research might generate novel hypotheses through its creative capabilities, then use its decision-making framework to determine which experiments to prioritize, how to allocate resources, and when to pivot based on emerging results. In this scenario, generative power (GenAI) is responsible for ideation, while decision-making (Agentic AI) guides execution.

Applying agentic capabilities to complex interconnections

Agentic AI is new and still evolving, but it can go to work now on more than just theoretical use cases. In enterprise environments, AI teams and technology vendors are already developing agentic systems that can handle workflows that involve dozens of interconnected applications and unpredictable dependencies. For example, an AI assistant tasked with preparing a monthly performance report may need to pull data from different sources, reconcile inconsistencies, interpret anomalies, format the content, and even e-mail the results. And it needs to do all of that while keeping the report's owner in the loop and adjusting its plan if a dashboard goes offline or a new dataset becomes available.



REMEMBER In this use case, the agent needs at least a degree of autonomy so that it doesn't just wait to be told what to do next. It notices, adapts, and keeps working toward the goal of creating a timely and accurate performance report.

Operating autonomously across time

What makes the evolutionary step for AI so transformative is that Agentic AI can operate across time:

- » **Traditional generative models excel in single-session contexts.**
They can generate impressive content, answer questions, and even

simulate dialogue. But they don't persist. They don't remember what they did yesterday, and they don't track what needs to happen tomorrow.

- » **Agentic systems, by contrast, maintain continuity.** They track tasks, store knowledge across sessions, and use memory to reflect on what worked, what didn't, and what they still need to do. They're not just intelligent, they're persistent.

The agentic systems' combination of intelligence and persistence enables sophisticated tool use and interaction with external systems. Agentic AI can generate appropriate commands, API calls, or interface interactions while simultaneously monitoring the results and adjusting its approach. In doing so, it functions more like an orchestrator than an assistant by

- » Not simply responding to requests, but coordinating a series of actions that often run across various software platforms
- » Working to achieve an outcome that's clearly defined but not tightly scripted

This design flexibility makes Agentic AI particularly well-suited to environments in which uncertainty is the norm rather than the exception. Business, science, healthcare, and logistics are all domains filled with ambiguity and change. Success in these areas depends not on executing a single correct answer, but on navigating evolving conditions and revising plans when new information becomes available.

Staying the course in a changing environment

The marriage of content generation and ongoing decision-making enables Agentic AI systems to operate with genuine autonomy in complex, unpredictable environments.

Nothing (and no one) can successfully create and make decisions in a linear fashion. Agentic AI's nonlinear approach isn't a flaw; it's a feature. It reflects the messy, adaptive nature of real-world problem-solving. In many ways, the process mirrors how human beings work when they're pursuing open-ended goals. They gather information,

consider options, make a move, and reassess. They change course when needed, seek help when appropriate, and keep moving toward the finish line. Agentic AI follows the same process, only faster, more consistently, and at greater scale.



REMEMBER Agentic AI uses the blend of GenAI and a solid decisioning framework to engage with the real world. It uses language and logic as tightly integrated tools in the service of action. That integration, the fusion of creativity and control, improvisation and intention, makes these systems so powerful, and so promising for real-world problem-solving and innovation. [Table 2-2](#) offers a comparison of GenAI and Agentic AI capabilities.

TABLE 2-2 Comparing GenAI and Agentic AI

<i>Feature/Aspect</i>	<i>GenAI</i>	<i>Agentic AI</i>
Language/creativity	Yes	Yes (inherited and enhanced)
Decision-making	Limited/static	Dynamic, real-time, adaptive
Goal pursuit	No	Yes (sets and pursues goals)
Execution	No	Yes (executes plans over time)
Adaptability	Limited	High (continuously learns and adjusts)

Generated with AI using Perplexity AI

OceanofPDF.com