AI basics

Who	Procurement teams
What	Overview of GenAI and agentic AI technologies, common use cases, and limitations and risks

What is AI

Artificial intelligence, or AI, is a term that describes computer systems designed to perform complex human-like tasks, such as perception, communication, analysis, and content creation.

An overview of different forms of AI include:

- **Machine learning,** which maps input data (often structured or numeric) to outputs such as predictions or classifications.
- **Deep learning**, a branch of machine learning, uses multilayer neural networks to learn from complex, unstructured inputs like images, text, or video, and can produce outputs ranging from simple labels to complex generated content.
- **Generative AI** (GenAI) uses deep learning models to generate new content, such as text, images, audio, or code, by predicting what is most probable based on patterns learned from training data. Large language learning models (LLMs) are a form of GenAI.
- **Agentic AI** builds on GenAI technology like LLMs, as well as connections with other databases and tools through forms of robotic process automation (RPA), to independently perform complex tasks based on new and evolving inputs. For example, summarizing email text and then proactively scheduling calls.

This guidance is focused on the latest evolutions of AI: GenAI and Agentic.

Defining artificial intelligence

There is no one single standard way of defining artificial intelligence and its various forms. For further information on how entities define AI, check out:

- The definition provided in the John S. McCain National Defense Authorization Act for Fiscal Year 2019, a commonly referenced US federal definition
- The EU Artificial Intelligence Act: General Provisions: Definitions
- The International Organization for Standardization's What Is Artificial Intelligence (AI)?

What is GenAI

Generative AI (GenAI) is a type of AI that can "generate" new content, and passively responds to queries based on recognizing and reproducing patterns from its training data. The technology has recently evolved from simple image and text generation to multi-modal models that can generate content which can be challenging to distinguish from content created by humans. GenAI use cases range from text summarization, to question answering, to digital art creation, to code generation and beyond.

What is Agentic AI

Agentic AI is an emerging technology that builds on GenAI capabilities to execute multi-step workflows. An agentic AI system can act independently to achieve directives. "Agentic" indicates the ability to act independently. Unlike other forms of AI that require prompting and step-by-step guidance, agentic AI can proactively and autonomously perform complex tasks.

AI agents can communicate with each other and other software systems to automate existing processes, as well as make independent decisions. They understand their environments and available tools, and can adapt to changing conditions, enabling them to perform a variety of sophisticated workflows. Agentic AI typically builds upon multiple hyper-specialized agents, with each focused on a narrow area of tasks. These AI-powered agents can coordinate with each other, sharing information and handing off tasks as needed. For example, agentic AI can help a developer not only write code, but automatically test and debug it, or send emails and then automatically schedule meetings based on the contents of the reply.

GenAI Stack

GenAI technology encompasses a lot of different functions. The set of technologies that work together to perform these functionalities is known as the GenAI technology stack. This stack can be thought of as three layers that build on each other and work together: the foundation layer, middle layer, and application layer.

Foundation layer: the model infrastructure

At the bottom of the stack are the foundation models (like GPT-5, Claude Sonnet, or Gemini Pro) and the infrastructure needed to run them. GenAI is powered by foundation models. Foundation models are sets of trained neural networks. They are pre-trained on tremendously large sets of data. Often these models were created based on publicly available data, such as large portions of the internet, books, and other text sources. GenAI can be customized for specific needs through a process called fine-tuning, which retrains the model on more specific data.

Middle layer: integration services

The middle layer consists of solutions and services that make the foundation models usable for specific applications. This includes the application programming interface (API) services that provide access to foundation models, development tools for customizing AI capabilities, and security and governance frameworks, as well as integration services that connect AI with existing systems.

Application layer: solutions

The top layer consists of the actual applications that people interact with. These might be AI-powered document processing systems, virtual assistants for citizen services, content generation solutions for organizational communications, or specialized analytical applications.



To understand the GenAI stack, it can be helpful to think of it like an airplane. The **foundation layer** is like the engine. Just as an engine is needed to get the airplane off the ground, the foundation layer is essential for generative capacity. The **middle layer** is like the body of the aircraft. It is the recipient of the engine's power, and is what makes the engine usable for flight. It's also customizable to meet your purposes. For GenAI, this is the layer that takes the model's power, customizes it, and makes it usable. The **application layer** is like the cockpit. Just like a pilot uses instruments and controls to direct the airplane, a user interacts with applications to use the AI model.

To take the airplane example further, **agentic AI** could be considered the autopilot: it's technology that is intended to be fully capable of flying the airplane, but you'd still want human oversight to deal with emergencies and make sure all goes well.

All the technologies in the GenAI tech stack are cloud-based. While not the focus here, this means that there are also additional hosting infrastructure considerations when buying AI.

When to consider GenAI and agentic agents

Currently, GenAI technology is often compared to an intern at work. An intern can help you do your job well and make a task more efficient. However, you still wouldn't want even the most brilliant intern making high-stakes decisions, or running crucial operations without oversight. You would also not ask an intern to carry out a task you are unable to perform yourself or, at least, you do not know what "good looks like" in relation to that task.

GenAI is great at producing results that are most *likely or plausible*. However, it does not know what is *true or correct* (it does not "know" anything). This is an important distinction. GenAI can also struggle with newer and more complex situations. Together, these factors mean that the outputs from GenAI should be checked by a human.

If GenAI is like an intern, agentic AI is more like a junior colleague to whom you have made a directive. It works independently from start to finish: from receiving a request, to making decisions and implementing solutions based on its own interpretation and analysis of the context and initial input. Since agentic AI is able to leverage LLMs with other AI agents that specialize in tasks beyond text interpretation and generation, agentic AI is capable of dealing with more complex problems. However, agentic AI otherwise faces the same limitations as GenAI, and because it is more powerful, when things go wrong it can also be more risky. Multiple models are interconnected through agentic AI, so an inaccurate output from one of them could feed into another model that processes it inaccurately, and so on, leading to a final response that is impacted by multiple stages of errors.

Consider using GenAI and agentic AI for:

- Repetitive tasks, such as low-risk administrative activities
- Creating an initial synthesis of a lot of different types of data
- Generating first drafts or options for human review
- IT modernization and development

Avoid using GenAI and agentic AI for:

- Higher-stakes decision-making
- Decisions that require transparency and explainability
- Low-quality data

GenAI and agentic agent use cases

GenAI and agentic AI are new technologies, and the public and private sectors are learning where this AI adds value for their organizations, and how to make the most of it. This is especially true for agentic AI.

Five use cases for the public sector include:

Document intelligence:

GenAI can be programmed to automatically read, summarize, and extract key information from thousands of pages in minutes – work that could take staff weeks to complete. This means that GenAI has the potential to transform how agencies handle documents, from complex regulations to registration forms. Ultimately, this may result in faster service delivery, better compliance, and significant operational savings. For example, document intelligence for the procurement function could look like having a "super-paralegal" who instantly flips through thousands of contracts, regulations, or vendor proposals and highlights the exact clauses you need.

Supporting service delivery:

GenAI powers intelligent assistants, such as chatbots for internal or external use, which can handle thousands of inquiries simultaneously, providing information and processing routine requests automatically. These systems can integrate with existing service channels, while potentially reducing wait times and freeing up staff for complex cases. The technology can support consistent service levels in some domain areas while scaling automatically to meet demand peaks, with the potential for improving satisfaction while reducing operational costs. Imagine you're running a call center during the scheduled enrollment period for a public health insurance program. Normally, you'd need to bring in dozens of temporary staff to handle the flood of calls. GenAI is like having an infinitely scalable team of front-desk clerks who answer routine questions and process simple requests automatically. Agentic AI has the potential to build on these capabilities by developing more effective strategies to assist customers. For example, an AI agent may, after several attempts to solve a resident's issue, proceed to contact a human support agent and assign them to the case.

Transcription and translation:

GenAI can create real-time text documentation of meetings or calls, as well as provide rapid translations. This functionality can help improve internal efficiency. For example, social workers can spend less time taking notes and more time on working directly with their clients, and public-facing documents can be quickly translated into different languages. Live simultaneous translation can also enable more community members to better participate in public meetings.

IT modernization and development:

GenAI can assist developers by automating routine coding tasks, suggesting improvements, and helping modernize legacy systems. As part of this, GenAI can help technology ensure compliance with security requirements while accelerating digital transformation initiatives. Likewise, agentic AI can help with code modernization by leveraging machine learning, neural networks, LLMs, and automated reasoning, as well as potentially help with faster responses when technology breaks by expediting the incident response process. For example, agentic AI could automate the entire incident response pathway, rolling back issues, creating incident reports, and notifying any team members who need to stay informed.

Data analysis and insights:

Multi-modal GenAI can process and analyze vast amounts of information from multiple sources – including reports, sensors, and operational data – to identify patterns and generate actionable insights that improve service delivery. These capabilities can help agencies make data-driven decisions, optimize resource allocation, and proactively address emerging challenges. This can reduce the manual effort required for complex analysis while enabling more responsive and effective public sector services. For example, transportation agencies use multi-modal GenAI ↗ to analyze traffic data and optimize signal timing, reducing commute times for schoolchildren ↗ and improving road safety for residents. Picture a highway patrol team trying to monitor every camera, road sensor, and traffic report manually – it would be impossible to catch everything. GenAI is like an always-on traffic controller that watches all feeds at once, spots patterns, and alerts you before a crash or bottleneck happens.

More on public sector GenAI use cases

- The State of California in the US offers a table with use cases
- McKinsey offers a global overview of use cases organized by archetype
- Danks Industri published a white paper on responsible use of AI assistants in the public and private sectors.
- Stanford University Human-Centered Artificial Intelligence has issued a brief on validating claims about AI for policymakers.

GenAI and agentic AI limitations and risks

GenAI and agentic AI holds strong potential to improve organizational efficiency and improve service delivery, but with these opportunities comes risk. It's critical to understand the limitations of these systems so that your organization can use them strategically, responsibly, and safely.

Common limitations include:

GenAI and agentic AI lack a genuine understanding of the world, and hallucinate.

While AI models can generate sentences, these are simply outputs – the LLM doesn't have a true human-like understanding of what the sentence means. Relatedly, GenAI and agentic AI hallucinate, in other words, give you inaccurate results or information that sounds authoritative but is false. Hallucination rates vary by model, but no model is hallucination-free ↗. Examples of hallucinations will be different depending on your use case, but could look like generating a realistic-sounding policy citation that doesn't actually exist, providing inaccurate or illegal advice to business owners through a chatbot, or wrongly denying access to benefits. AI's tendency to hallucinate makes it essential to have a human-in-the-loop to review and think critically about the results, especially for decision-making that directly impacts service delivery.

Agentic AI hallucinations can be particularly worrisome since they have the potential to impact workflows. For example, if the model generates false information and then relays it to the rest of the AI agents, incorrect data can rapidly spread, escalating errors in the final output.

For the public sector, both GenAI and agentic AI hallucinations could have severe real-world implications. Organizations must be confident in their use case and solution before using it extensively.

GenAI and agentic AI results depend on their training data.

GenAI models are only as good as the data they are trained on. For example, if your model is only trained on data up to October 2024, it would be unable to tell you current regulations. This is why understanding the training data sources matters a lot, as well as understanding your own data quality if you will be using it to further refine the model.

Given their reliance on training data, GenAI and agentic AI may pose data security and privacy risks. When you input data into AI systems, that information may be stored, processed, or even used to train future models unless specific protections are in place. This is particularly important for government data that includes personally identifiable information or sensitive operational details. Organizations should ensure their AI solutions include appropriate data-handling safeguards and comply with relevant privacy regulations.

GenAI and agentic AI have a limited ability to explain its results.

GenAI solutions cannot explain in perfect detail how they arrived at their conclusions. This lack of explainability can be fine in some situations, but not ok in others where explainability is critical and a matter of legal risk. For example, an AI chatbot that provides assistance with navigating an unemployment application can be ok, while using an AI system to make decisions around qualifying for public benefits could expose governments to legal concerns given an individual's right to due process.

Likewise, agentic AI produces results that can be hard to trace or reproduce. Since agentic AI works independently and with minimal human intervention, this can make testing, debugging, and determining where an AI model has gone wrong a challenge.

Agentic AI requires very strong system design.

The process of building a multi-agent architecture that effectively coordinates with other models, has specific information of how to carry out certain tasks, and can achieve high-level complex directives is a challenge. Moreover, agentic AI is a new area of technology that relies on successful deployment of other AI strategies. Given this complexity, public sector organizations may struggle to use agentic AI effectively even in low-risk situations where agentic AI could be a strong fit.

For more information on limitations and how to mitigate GenAI and agentic risks during your procurement process, check out our sections on *Myth-busting* and *Key questions to ask.*

GenAI and agentic AI requires ongoing support, which has cost implications.

When implemented thoughtfully, investments in AI can deliver strong returns through improved efficiency and service quality. However, the limitations we explore here have real cost implications for implementation. The need for human oversight, data quality improvements, and ongoing monitoring means AI adoption involves more than just technology costs. Organizations should budget for additional staff time to review AI outputs, potential data preparation work, and ongoing performance monitoring.