

Machine  
Learning  
Prague

# A hands-on guide to AI Agents

Philipp Wendland, Ole Wegeleben  
Deloitte AI Institute Germany

April 28<sup>th</sup>, 2025





**Philipp Wendland**  
Deloitte AI Institute, Germany



**Ole Wegeleben**  
Deloitte AI Institute, Germany





# Agenda

01 | Introduction to AI Agents

02 | Exercise Block 1

03 | Intro to Exercise Block 2

04 | Exercise Block 2

05 | Outlook



# Chapter 1

## **Introduction to AI Agents**

# Evolution from Chatbots to AI Agents

## Chatbot

Stand-alone chat

Chat



## Copilot

Providing support and enhancing productivity



Integration



Flexibility



Interaction



## AI-Agent

**Advanced AI system designed to perform specific tasks autonomously**



Specialisation



Autonomy



Execution

**Deloitte.****Now decides next:**  
Generating a new future

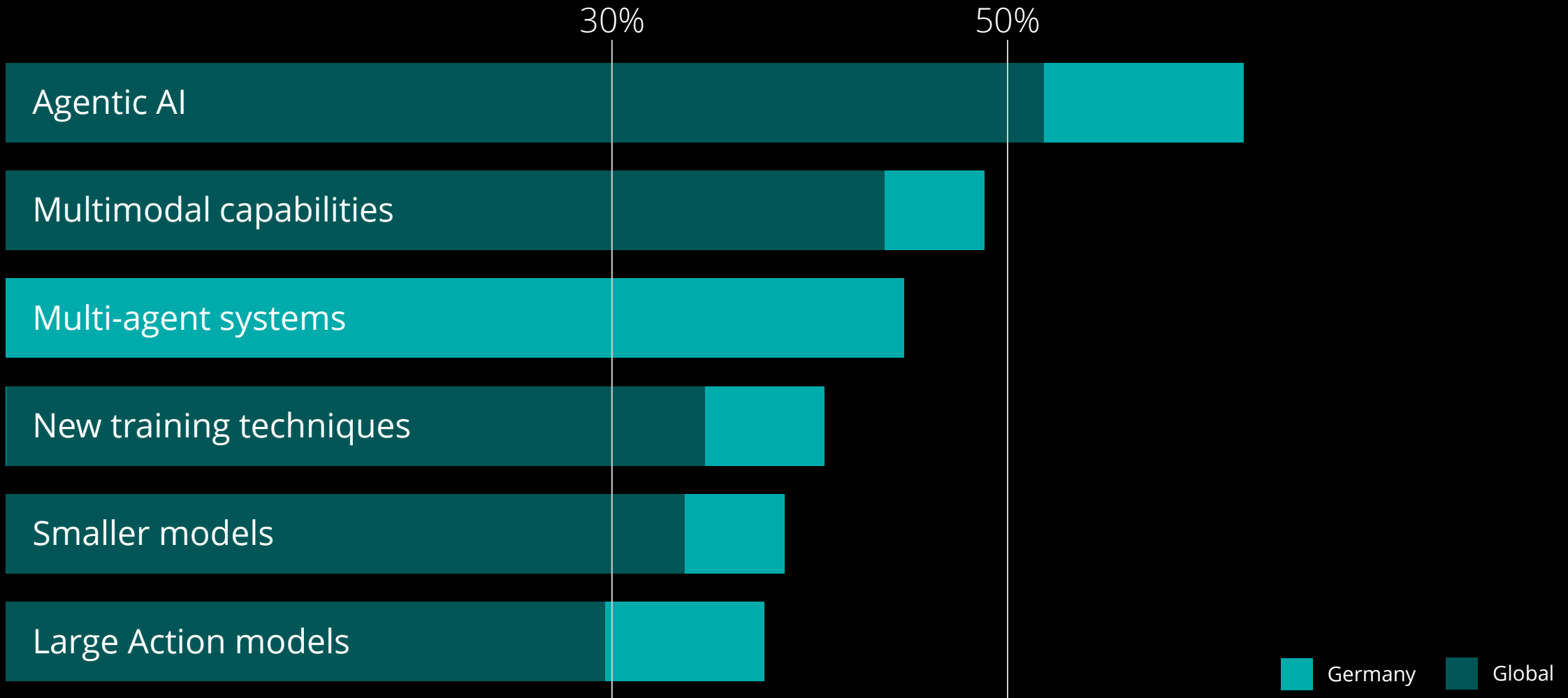
Deloitte's State of Generative AI in the Enterprise  
Quarter four report – German Cut

March 2025

[deloitte.com/de/ki-studie](https://www.deloitte.com/de/ki-studie)

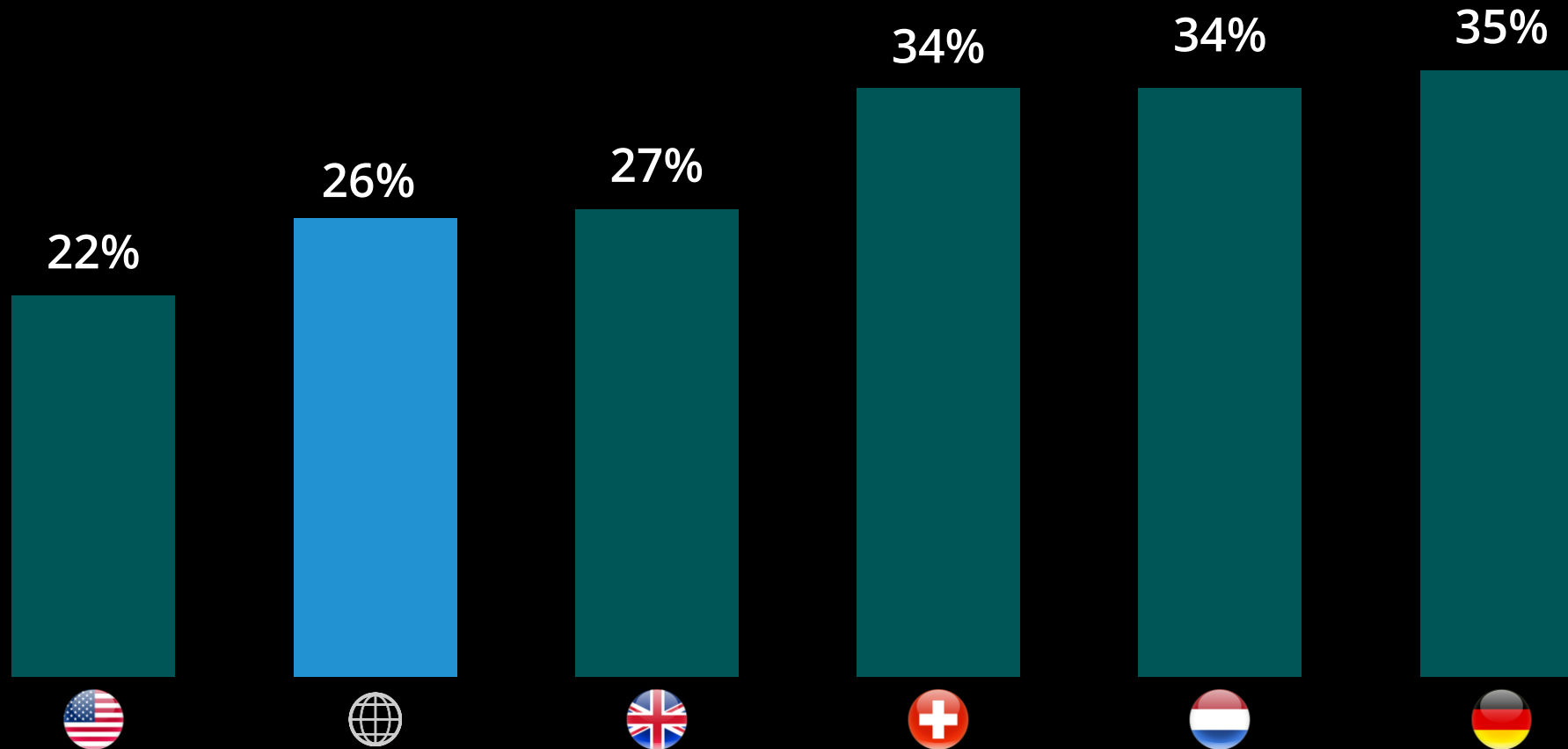


# Organizations are most interested in Agentic AI





# Is your organization exploring AI Agents?



Organizations choosing to a "large" or "very large extent"



The background features a dark blue, almost black, space-themed aesthetic. It includes faint, glowing lines and dots that suggest a network or a starry sky. Two stylized, metallic-looking robot heads are visible: one on the left, partially obscured, and another on the right, more prominent. The text 'AI AGENT' is positioned in the upper left quadrant, with a short teal horizontal line below it.

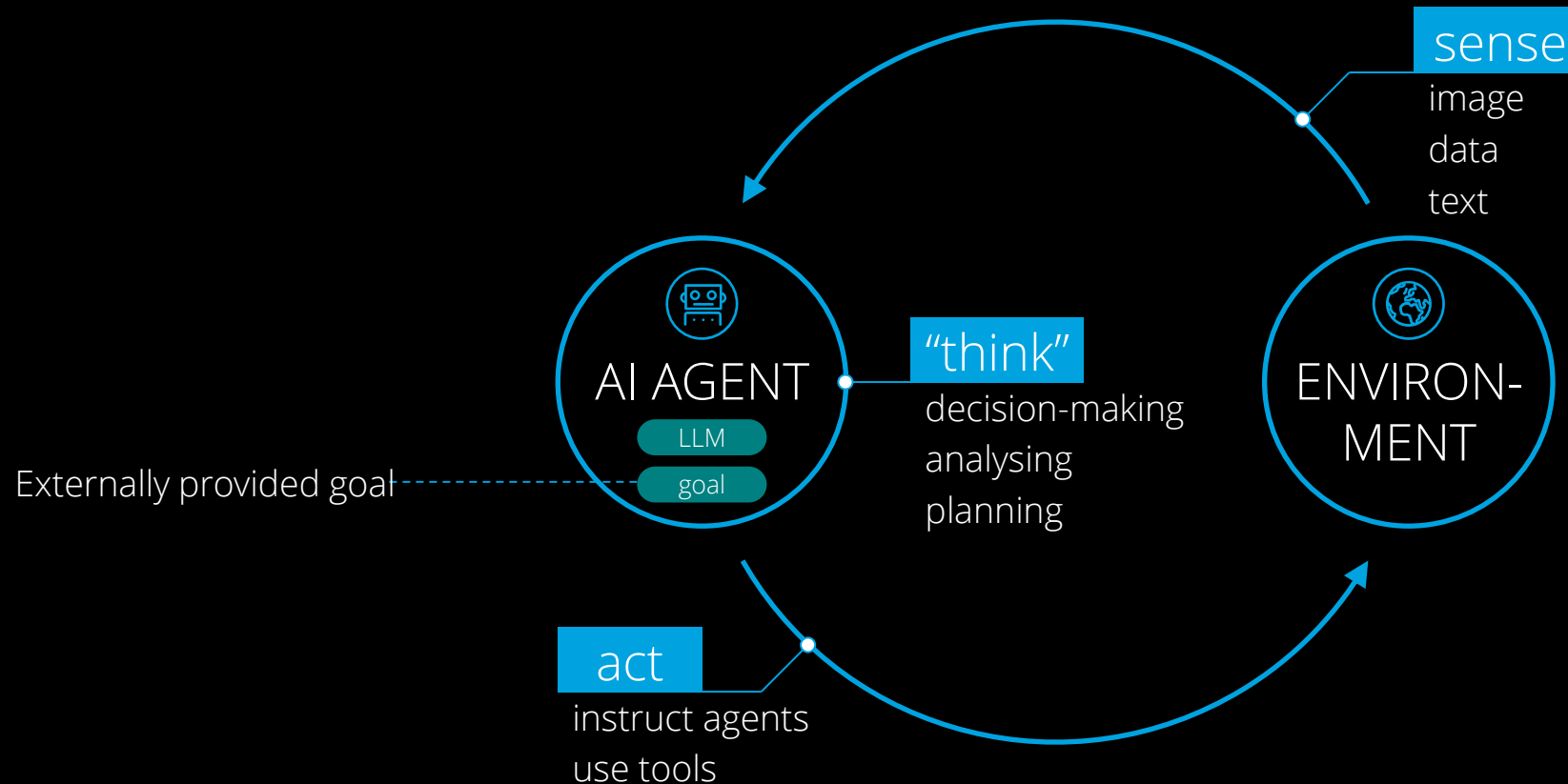
AI AGENT


---

*An AI agent is a software systems that uses AI and has access to tools to accomplish a goal on behalf of a user.*

# The anatomy of an AI-Agent

AI Agents autonomously decide the control flow and perform tasks using tools









The background features a dark, blue-toned image of a robot's head in profile, facing right. Overlaid on this is a faint, glowing network diagram with nodes and connecting lines, suggesting a digital or AI theme. A solid teal horizontal line is positioned above the text on the left side.

*“AI agents will transform the way we interact with technology, making it more natural and intuitive. They will enable us to have more meaningful and productive interactions with computers.”*

Fei-Fei Li | Professor Stanford University

# AI Agents can be built in a variety of environments

Several factors, incl. the use case and data availability will determine the ideal approach

	Platform integrated	Low/No-code	Developer frameworks
Type	<p>Platform providers are introducing agent capabilities into their existing offerings</p> <p>Most simple to set-up, but only works within the specific platform and limited customization</p>	<p>Drag &amp; drop agent builders allow users to build low-code agents relying on the expertise of established providers</p> <p>Best-practices on AI Agent building integrated</p>	<p>Code-based agent frameworks provide a structure to build advanced, customized multi-agent systems</p> <p>Provides full flexibility and requires expertise in AI agent building</p>
Flexibility	 Low	 Medium	 High
Ease of use	 High	 Medium	 Low



# Production-grade agents are part of ecosystems

## Data & Integrations

Data Integration & Orchestration using APIs, events, messages & knowledge repositories

## Business Process Layer

Conducted and governed by people and business applications



## Multi-Agent AI Systems (MAS)



Coordination amongst each other and with humans to accomplish complex tasks

### "Humans in Loop" SOPs

Standard Operating procedures (SOPs) leveraging agentic frameworks & prompts with humans in loop

### Agents

Plan and act as per role by using its knowledge, memory and tools

### Workflows

Orchestrate Agents with Human in the loop to automating processes

### Models, Tools & More

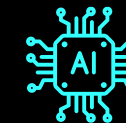
Model (AI/ML, LLM, SLM, etc.) training, mgmt. and finetuning; Automation & Integration Tools etc.

## Vertical Agent Use Cases

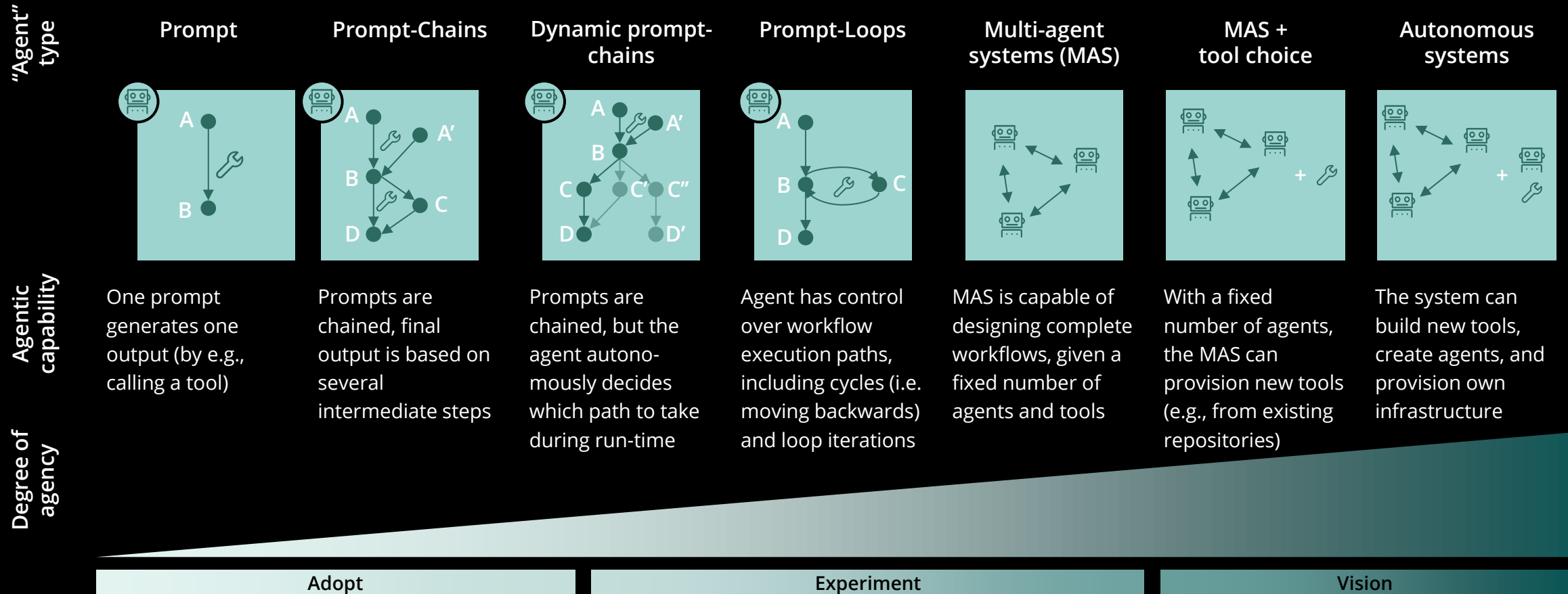
Agent based use cases and solutions for specific functional and domain areas specifically built and customized for an enterprise and its needs

## AI & Data Infrastructure, Platforms and Toolkits

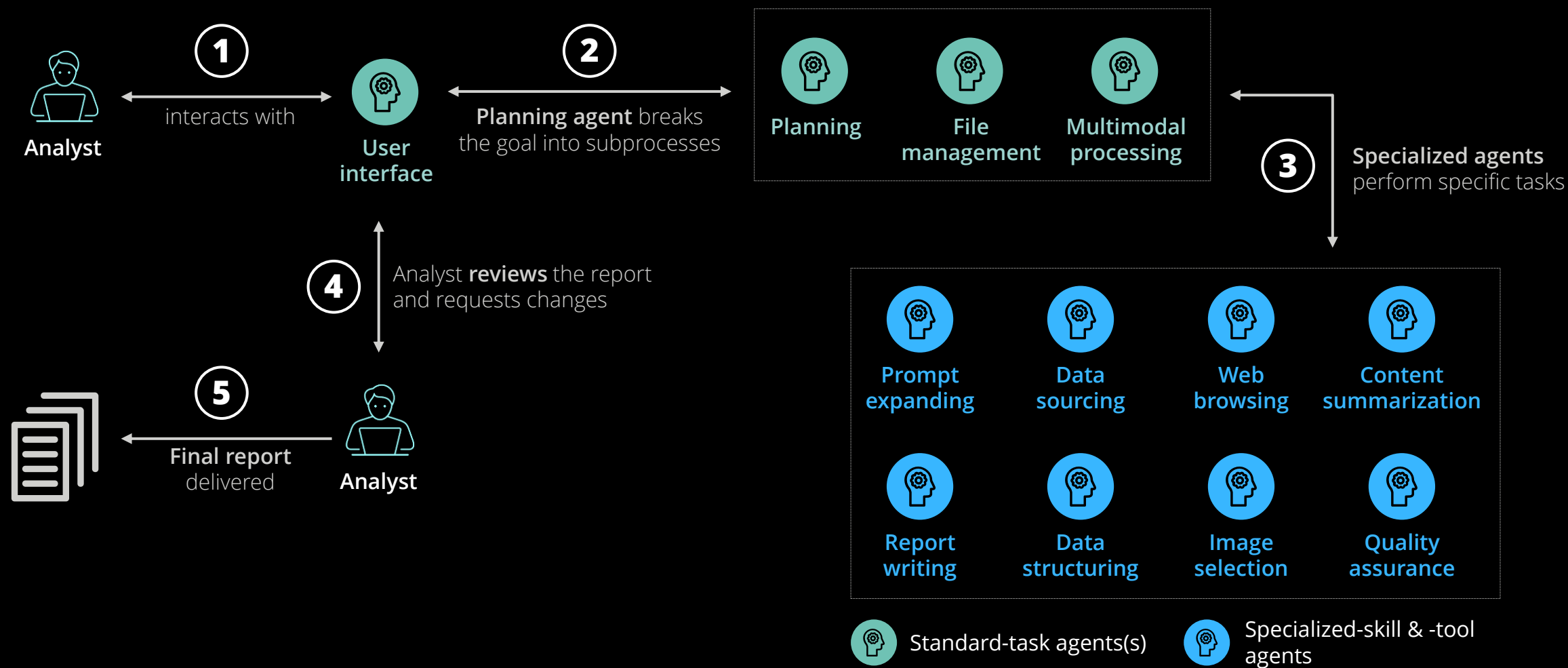
High-performance hardware, and AI and data platforms (Hybrid Cloud)



# Agents exist on a spectrum from simple to complex



# Multi-Agent-System for research and reporting



# The game of protocols

Protocols aim to enhance LLM capabilities and agent orchestration



## MCP (Model Context Protocol)

Developed as an Open Standard to let LLMs mount data sources and tools

Unified communication between LLM and external systems / tools

Allows quick and simple integration through MCP servers



## A2A (Agent to Agent protocol)

Allow agent to agent communication and interoperability across various agent frameworks

Agent card in JSON format

Relies on existing standards (http, json)



## ACP (Agent communication protocol)

A standard for local multi-agent communication (i.e., agent-to-agent messaging)

Focus on single-environment



# Risks & limitations of multi-agent systems



**Premature  
termination**



**Design  
deficiencies**



**Coordination  
complexity**



**Bias**



**Performance  
variability**



**Exposure of  
information**



**Malicious  
Behavior**



**Tracing  
difficulties**

# The difference between jobs and skills is key

Understanding where and what AI systems can augment humans is crucial



## Work

is the result of harnessing human and tool capabilities

Meeting sales, UX, and customer satisfaction targets

Desired outcomes are and will be defined by humans



## Jobs

define the work humans do to achieve outcome

Roles like sales reps, developers, account managers

Not jobs are automated, but tasks and jobs may be redefined based on skills



## Tasks

are specific activities within jobs aimed at producing outcome

Identifying sales channels or tailoring product offerings

AI's role lies in task automation and efficiency enhancement



## Skills

enable us to complete tasks and attain work outcomes

Problem solving, coding, and data analysis skills

Skills can reside in humans and AI  
Crucial for evolving work with Gen AI integration

# Chapter 2

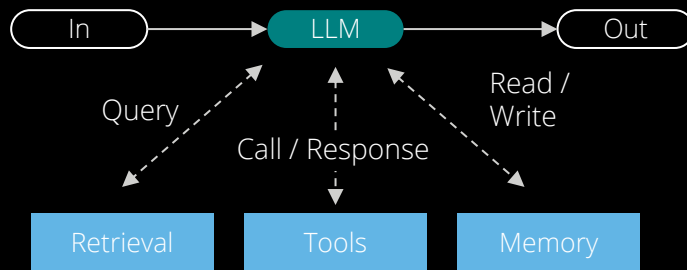
## Exercise Block 1



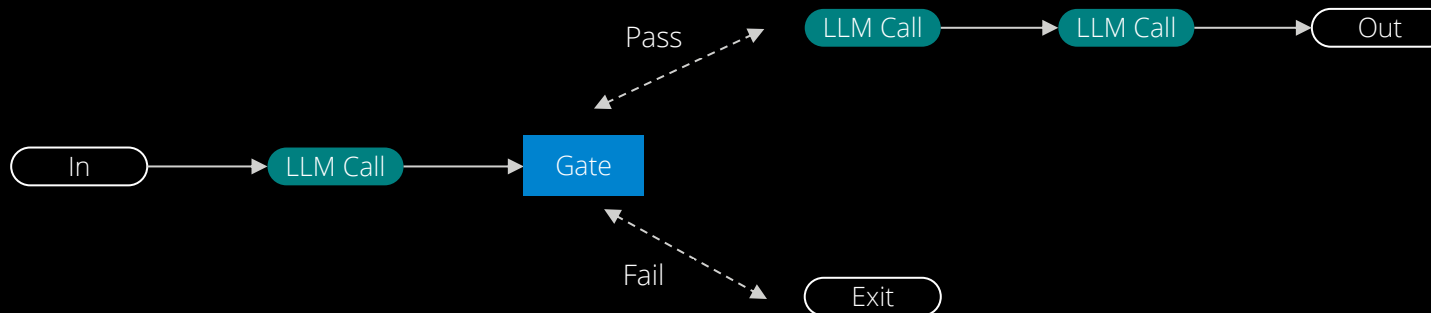
# Anthropic on “Building effective agents”

“Successful implementations use simple patterns rather than complex frameworks”

## Augmented LLMs



## Prompt-Chaining Workflow





# Exercises 1, 2 & 3a

Prompt-chain workflows and basic tool-calling

## Exercise 1

- ✓ Setup the environment & install dependencies
- ✓ Adjust the given prompt
- ✓ Happy with the LLM output? Use it as a baseline for the more complex workflows & agents

## Exercise 3a

- ✓ Extend the previous functions to accept a tools parameter
- ✓ Adjust the prompt chain to include a tool call

## Exercise 2

- ✓ Use the `sequential_chain` method
- ✓ Write an `additive_chain` method
- ✓ Try out your chain with a new use case



## ML PRAGUE 2025: A HANDS-ON GUIDE TO AI AGENTS

# Getting ready for Exercise Block 1

[https://github.com/pwendland/mlprague\\_aiagents](https://github.com/pwendland/mlprague_aiagents)

The screenshot shows the GitHub repository page for `pwendland/mlprague_aiagents`. The repository is public and has 1 branch and 0 tags. The main branch is selected. The repository contains a file named `solutions` and several notebooks for workshop exercises. The README file is open, showing the title "A hands-on guide to LLM-based AI Agents" and the author's name, Philipp Wendland.

**Repository: pwendland / mlprague\_aiagents** (Public)

Navigation: <> Code, Issues, Pull requests, Actions, Projects, Security, Insights

Branch: main, 1 Branch, 0 Tags

Search: Go to file

Code: <> Code

**Files:**

File	Description	Time
solutions	Moved solutions to separate folder	2 minutes ago
.gitignore	Notebooks for workshop exercises	3 minutes ago
MLPrague_ExerciseBlock1.ipynb	Notebooks for workshop exercises	3 minutes ago
MLPrague_ExerciseBlock2.ipynb	Notebooks for workshop exercises	3 minutes ago
README.md	Notebooks for workshop exercises	3 minutes ago
requirements.txt	Notebooks for workshop exercises	3 minutes ago
requirements_mac.txt	Notebooks for workshop exercises	3 minutes ago

**README**

## A hands-on guide to LLM-based AI Agents

ML Prague 2025

Philipp Wendland [pwendland@deloitte.de](mailto:pwendland@deloitte.de)

This notebook contains exercises for the workshop at ML Prague 2025. The goal is to implement an AI Agent that...

**About**

Material for AI Agents workshop at ML Prague 2025 ("A hands-on guide to LLM-based AI Agents")

Readme, Activity, 0 stars, 1 watching, 0 forks, Report repository

**Releases**

No releases published

**Packages**

No packages published

**Languages**

Jupyter Notebook 100.0%

# Coffee Break: Be back by 16:00



Clarify any  
setup-issues to  
be ready for  
smolagents





# Chapter 3

## **Intro to Exercise Block 2**





# Myriads of agent frameworks have emerged

We'll take a closer look at smolagents today



- Lightweight modular agents
- Self-contained agent classes with basic tools and memory



- Build multi-agent workflows as directed graphs
- Offers fine-grained control over agent interactions and state management

# Implementation varies depending on “Agency Level”

Agency Level	Description	How that's called	Example Pattern
☆☆☆	LLM output has no impact on program flow	Simple processor	<code>process_llm_output(llm_response)</code>
★☆☆	LLM output determines basic control flow	Router	<code>if llm_decision(): path_a() else: path_b()</code>
★★☆	LLM output determines function execution	Tool call	<code>run_function(llm_chosen_tool, llm_chosen_args)</code>
★★★	LLM output controls iteration and program continuation	Multi-step Agent	<code>while llm_should_continue(): execute_next_step()</code>
★★★★	One agentic workflow can start another agentic workflow	Multi-Agent	<code>if llm_trigger(): execute_agent()</code>

ML PRAGUE 2025: A HANDS-ON GUIDE TO AI AGENTS

# Basic smolagents architecture

# smolagents consists of several agent types

A CodeAgent is the main type of agent introduced by the smolagents framework



```
from smolagents import CodeAgent, DuckDuckGoSearchTool, HfApiModel

agent = CodeAgent(tools=[DuckDuckGoSearchTool()], model=HfApiModel())

agent.run("Search for the best music recommendations for a party at the Wayne's mansion.")
```



```
from smolagents import ToolCallingAgent, DuckDuckGoSearchTool, HfApiModel

agent = ToolCallingAgent(tools=[DuckDuckGoSearchTool()], model=HfApiModel())

agent.run("Search for the best music recommendations for a party at the Wayne's mansion.")
```

# Structure of a tool in smolagents

```
@tool
def get_weather(latitude: float, longitude: float) -> dict:
    """
    Obtains the current weather based on a given location
    Args:
        latitude: float of latitude of the given location
        longitude: float of longitude of the given location
    Returns:
        dict containing
            "current_temp": current temperature in celsius
            "cloud_cover": current cloud cover in percent
            "percipitation": current percipitation in mm
    """

    try:
        response = requests.get(f"https://api.open-meteo.com/v1/forecast?latitude={latitude}&longitude={longitude}&current=temperature_2m,cloud_cover,precipitation&hourly=temperature_2m,precipitation_probability,cloud_cover")

    except:
        return "Weather data not available"

    response_data = response.json()

    return {
        "current_temp": response_data['current']['temperature_2m'],
        "cloud_cover": response_data['current']['cloud_cover'],
        "precipitation": response_data['current']['precipitation']
    }
```



ML PRAGUE 2025: A HANDS-ON GUIDE TO AI AGENTS

# Exercises 3b & 4

Prompt-chain workflows and basic tool-calling

## Exercise 3b

- ✓ Setup a CodeAgent & examine the system prompt
- ✓ Create an itinerary using a single agent with multiple tools

## Exercise 4

- ✓ Create a multi-agent system
- ✓ Implement a new tool, create an agent and add the agent to the multi-agent system (e.g.,

## Bonus

- ✓ Download a tool from the hub or MCP servers



## ML PRAGUE 2025: A HANDS-ON GUIDE TO AI AGENTS

# Create a map of famous sights in Prague

geojson.io

Open Save New Meta

powered by mapbox Sign up for Mapbox

Search

JSON Table Help

```
1 {
2   "type": "FeatureCollection",
3   "features": [
4     {
5       "type": "Feature",
6       "geometry": {
7         "type": "Point",
8         "coordinates": [
9           14.4214,
10          50.0871
11        ]
12      },
13      "properties": {
14        "name": "Old Town Square"
15      }
16    },
17    {
18      "type": "Feature",
19      "geometry": {
20        "type": "Point",
21        "coordinates": [
22          14.4114,
23          50.0865
24        ]
25      },
26      "properties": {
27        "name": "Charles Bridge"
28      }
29    },
30    {
31      "type": "Feature",
32      "geometry": {
33        "type": "Point",
34        "coordinates": [
35          14.4208,
36          50.0759
37        ]
38      }
39    }
40  ]
41 }
```

Standard Satellite Streets Outdoors Light Dark OSM

mapbox

© Mapbox © OpenStreetMap Improve this map



# Chapter 5

## **Outlook**



# Considerations beyond experimentation

For productive use cases using AI Agents additional aspects need to be considered



**Testing**



**Domain & Process  
knowledge**



**Business value  
(human-in-the-loop)**

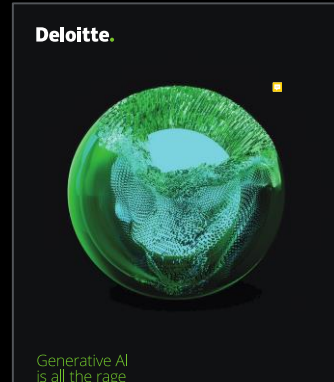


**Governance &  
ethics**

# Further reading on Generative AI

Our thought leadership on (Generative) AI is continuously expanding

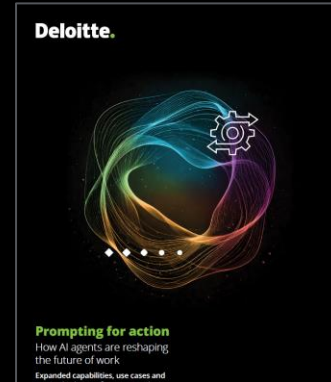
[Generative AI is all the Rage](#)



[A new frontier in artificial intelligence](#)



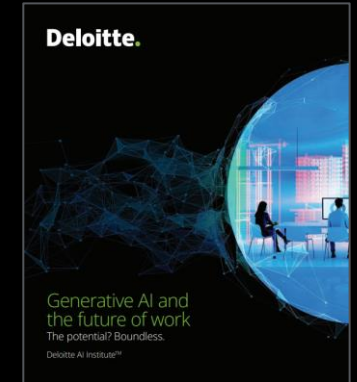
[How AI agents are reshaping the future of work](#)



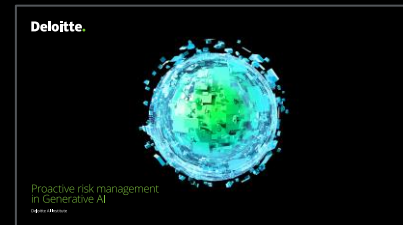
[The legal implications of Generative AI](#)



[Generative AI and the future of work](#)



[Proactive risk management in Generative AI](#)



[State of Generative AI 2024](#)



[State of Generative AI, German Cut](#)



[Generative AI Dossier](#)



[Artificial Intelligence Act](#)





# Thank you.



**Philipp Wendland**

Senior Consultant | AI Institute

[pwendland@deloitte.de](mailto:pwendland@deloitte.de)

Rosenheimer Platz 4  
81669 Munich, Germany  
Deloitte Consulting GmbH



**Ole Wegeleben**

Senior Consultant | AI Institute

[olwegeleben@deloitte.de](mailto:olwegeleben@deloitte.de)

Dammthorstraße 12,  
20354 Hamburg, Germany  
Deloitte Consulting GmbH

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited ("DTTL"), its global network of member firms, and their related entities (collectively, the "Deloitte organization"). DTTL (also referred to as "Deloitte Global") and each of its member firms and related entities are legally separate and independent entities, which cannot obligate or bind each other in respect of third parties. DTTL and each DTTL member firm and related entity is liable only for its own acts and omissions, and not those of each other. DTTL does not provide services to clients. Please see [www.deloitte.com/de/UeberUns](http://www.deloitte.com/de/UeberUns) to learn more.

Deloitte is a leading global provider of audit and assurance, consulting, financial advisory, risk advisory, tax and related services; legal advisory services in Germany are provided by Deloitte Legal. Our global network of member firms and related entities in more than 150 countries and territories (collectively, the "Deloitte organization") serves four out of five Fortune Global 500® companies. Learn how Deloitte's approximately 330,000 people make an impact that matters at [www.deloitte.com/de](http://www.deloitte.com/de).

This communication contains general information only, and none of Deloitte Consulting

GmbH or Deloitte Touche Tohmatsu Limited ("DTTL"), its global network of member firms or their related entities (collectively, the "Deloitte organization") is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser.

No representations, warranties or undertakings (express or implied) are given as to the accuracy or completeness of the information in this communication, and none of DTTL, its member firms, related entities, employees or agents shall be liable or responsible for any loss or damage whatsoever arising directly or indirectly in connection with any person relying on this communication. DTTL and each of its member firms, and their related entities, are legally separate and independent entities.

# Sources

## Deloitte

- Prompting for action: <https://www2.deloitte.com/content/dam/Deloitte/us/Documents/consulting/us-ai-institute-generative-ai-agents-multiagent-systems.pdf>
- GenAI and the future of work: <https://www2.deloitte.com/content/dam/Deloitte/us/Documents/consulting/us-ai-institute-generative-ai-and-the-future-of-work.pdf>

## Anthropic

- Anthropic cookbook (<https://github.com/anthropics/anthropic-cookbook/tree/main>)
- Building effective Agents: <https://www.anthropic.com/engineering/building-effective-agents>
- MCP: <https://www.anthropic.com/news/model-context-protocol>

## Huggingface

- Introducing smolagents: <https://huggingface.co/blog/smolagents>
- AI Agent course: <https://huggingface.co/learn/agents-course/unit0/introduction>
- Smolagents documentation: <https://huggingface.co/docs/smolagents/v1.14.0/en/index>

Agent Communication protocol: <https://research.ibm.com/blog/multiagent-bee-ai>

Agent to agent protocol: <https://research.ibm.com/blog/multiagent-bee-ai>

M. Cemri et al. Why do multi-agent systems Fail (<https://arxiv.org/pdf/2503.13657>)

OpenAI Documentation: <https://platform.openai.com/docs/guides/function-calling>

LiteLLM Documentation: <https://docs.litellm.ai/>

## Resources

[https://github.com/pwendland/mlprague\\_aiagents](https://github.com/pwendland/mlprague_aiagents)