

Find the AI system that fits the task.

Browse the boundaries and operating questions behind retrieval, document processing and tool-using agents.

AI capability map

Capability	The boundary to design
Knowledge retrieval	Which sources may this person search and cite?
Document processing	Which fields can proceed and which require review?
Task agents	Which tools may act, with what approval and recovery?

Separate interpretation from authority

A model may interpret a request or prepare an action. The application must still enforce permissions, validate fields and decide whether the action is allowed.

Choose the smallest useful capability

A searchable knowledge base may solve the task without an autonomous agent. A deterministic rule may be more appropriate than a model for a stable calculation.

Connect an agent through a controlled MCP server

An MCP server exposes selected business functions as tools that an agent can call through an MCP client. Start with a specific read operation, such as retrieving an authorised order status. Keep credentials on the server and validate the requesting identity, organisation and record access when the call executes.

Separate reading, preparing a change and applying it. A consequential write needs approval tied to the exact action, plus duplicate protection and an investigation record. Test revoked permissions, hostile tool output and interrupted requests before expanding the catalogue. MCP is the connection mechanism. The application still owns the security boundary.

Choose the workflow before the model

Identify the task, the people affected and the decision the system will support. A knowledge assistant helps a user find and understand existing material. A document workflow extracts proposed values for validation. An agent can prepare or perform actions through tools. These are different responsibilities even when they use the same model provider.

For each candidate, identify the authoritative records and acceptable failure behaviour. A missing answer can be appropriate for an internal knowledge question. An incorrect payment instruction needs stronger controls. Establish who reviews uncertain results and what evidence they need. This prevents a demonstration from quietly becoming an operational system with broader authority than originally intended.

Compare the surrounding controls

A useful comparison includes identity, data preparation, retrieval, application logic, evaluation and operations. For knowledge search, check document permissions, deletion handling and the quality of citations. For extraction, compare field accuracy, cross-field validation and the ability to trace a value to its source location.

For an agent, inspect tool contracts independently of the prompt. Record which tools read records, which create drafts and which can make changes. Evaluate interruption and recovery alongside successful conversations. A strong answer to one test question does not establish that a system's costs, freshness or permissions fit the business. Compare complete workflows using representative examples rather than selecting a provider on a demonstration alone.

Start with a bounded implementation

Choose a narrow collection of tasks and a limited group of users. Establish a baseline using the current process and compare the proposed workflow against it. Measure the time spent reviewing and correcting results, not only the time a model takes to respond. Include requests that should be escalated or refused.

Document the approved scope, data involved and owner of each external dependency. Plan how to investigate a bad answer, disable a tool and return to a previous configuration. Expand the system's responsibilities when evidence supports the change. The library should help teams select an implementation they can operate and improve, rather than assemble a collection of disconnected experiments.

Can several capabilities be combined?

Yes. Keep their boundaries visible so a failure in extraction or retrieval does not silently become an authorised business action.

Read the current resource online

<https://cobnex-review.rgcsekaraa.workers.dev/resources/ai-systems-library/>