

What AI should do and where it should stop

Practical rules for approvals, exceptions and responsibility in everyday AI workflows.

01 Separate preparing from committing

Reading a message, suggesting a label and drafting a reply are different from sending an offer or a promise to a customer. Each action needs its own permission. For a first pilot, let AI prepare drafts. A person approves every message before it is sent.

02 Name the decisions that stay human

Write down who decides on prices, discounts, delivery commitments, accounting questions and payments. A vague instruction to “be careful” is not enough. Be clear about what the system may do on its own and what it must hand to a person.

03 Treat incoming content as information

An email or attachment can contain hidden or misleading instructions. This risk is known as prompt injection. Such text must not change the system’s permissions, approve its own request or reveal unrelated data. Give the system access only to the data and tools the agreed task needs.

04 Define what happens when the system is unsure

When a document is missing, records conflict, a service is unavailable or a request is unclear, the system must hand the task to a person. A useful alert names the problem, shows the source and says what decision is needed. The system must not guess and then mark the task as done.

05 Review what actually happened

Check the action record, the quality of drafts, the exceptions and any unintended changes. Agree who responds when something goes wrong and how the work is paused. An approval button alone does not prove that a process is reliable.

[Read the current guide online](#)

Make it specific to your team.

A working sheet for a focused discussion. Keep sensitive information in your own systems.

01 Allowed preparation

List the reading, sorting and drafting actions AI may perform.

02 Human decisions

Who approves sending, pricing, commitments and changes?

03 Minimum access

Which inbox, records and tools are actually needed?

04 Exception route

What triggers escalation? Who receives it and by when?

05 Pause and recovery

Who can stop the workflow, review the record and resume it?

Put this into practice.

Keep this worksheet for your team. Remove client names and confidential details before sharing examples.

[Find your starting point](#) / [Book a free fit call](#)