Session 2 Handout: Redesign with AI and People

FAST-08 AI for Workflow Improvement and Process Automation · 7formations · Instructor: Wadood Chaudhary · All examples fictional

Why this session matters

A good redesign removes waste and puts AI where it is reliable and checkable, while keeping people in charge of anything that affects customers, money, or personal data. This session gives you the four AI step types, the human-in-the-loop rule, and the data and permissions thinking that keeps a flow from becoming a data leak.

Key concepts

1. Four AI step types

Step	What it does	Example	Check
Classify	Assigns one label from a list	quote, status, claim, address_change, other	Review queue for "other" and low confidence
Extract	Turns a document or message into fields	Invoice number, date, total	Person compares fields with the source
Draft	Writes text for a person to edit	Reply to a late-delivery question	Person edits and sends
Summarize	Condenses many records	Weekly request summary	Owner checks totals against the list

AI steps in a fixed workflow are more predictable than an open-ended agent. Start with the simplest design that works.

2. The human-in-the-loop rule

A person approves every step that affects customers, money, or personal data.

- Customer-facing text: draft, then a person sends.
- Money: extracted amounts are approved before payment; larger amounts get a second approver.
- Personal data: changes (address, bank details) are verified with the person through a known channel, then approved.

3. Data and permissions

- **Least privilege:** each connection gets only the access the step needs (one inbox, one list), never a personal account that can read everything.
- **Data minimization:** extract only the fields you need; post IDs, not personal details, to team channels.
- **Logging:** record run time, AI output, reviewer, and decision, without storing restricted data.
- **Untrusted input:** emails and documents can contain instructions aimed at the AI step. The AI step's output never approves anything by itself.

- **Policy:** flows that move MA residents' personal information must fit your written information security program (201 CMR 17.00).

4. Exception paths

Every AI step needs a defined path for "other," low confidence, missing fields, and failures. Usually that path is a person.

Worked example: future-state request flow (fictional)

```
New request (email/form)
  -> AI classify (label only; "other" if unsure)
  -> Log row: time, sender domain, subject, label
  -> Route by label:
       quote   -> AI extract lane details -> pricing analyst confirms
       status  -> AI draft reply -> coordinator edits and sends
       claim   -> claims clerk (photos attached)
       address -> billing verifies by known phone -> approves change
       other   -> review queue
  -> Post request ID + label to team channel (no personal data)
```

Checklist: is my future state safe?

- ☐ Every customer, money, or personal-data step has a named approver.
- ☐ Each AI step has an exception path.
- ☐ Minimum access listed for each connection.
- ☐ No personal data in channels or logs.
- ☐ No AI step sends, pays, or updates records on its own.

Do and don't

Do	Don't
Draft for approval	Auto-send customer replies
Verify changes out of band	Update bank or address details from an email
Scope connections narrowly	Connect with your personal account
Design the "other" path	Force every input into a label