# Compliance-Aware Automation Design Guide

US patterns for human-in-the-loop workflow automation

## Direct answer: how do you automate without increasing compliance risk?

Design automation so AI prepares, classifies, and routes work while humans approve high-risk actions. Keep audit logs, exception handling, and rollback steps from day one. Compliance-safe automation is a process design problem, not just a tooling choice.

## Core design rules (use on every workflow)

1. Define what the automation may do without approval.
2. Define explicit review triggers and escalation paths.
3. Store timestamps, inputs, outputs, and approver identity.
4. Keep a manual fallback path for failures and exceptions.
5. Limit data access to the minimum required for the workflow.

> **Sensitive data reminder**
>
> Typical categories to flag early: PHI/health data, PII in client onboarding, Financial account data.

## Control matrix for common automation steps

| Step | Automation role | Human control |
| --- | --- | --- |
| Document intake | Capture + classify | Spot-check confidence and exceptions |
| Data extraction | Draft structured fields | Approve low-confidence fields |
| Routing | Assign owner/queue by rules | Override routing when flagged |
| Notifications | Send reminders/status updates | Approve external messages if sensitive |
| Final action | Prepare transaction or record update | Required approval before commit |

## Region-specific compliance starting points

- HIPAA (if healthcare)

- SOC 2 controls

- State privacy obligations

- Retention/audit requirements

> **Important**
>
> This guide is an operational design framework, not legal advice. Validate controls with your compliance, legal, or security stakeholders.

## What to document before go-live

| Document | Why it matters |
| --- | --- |
| Workflow map + exceptions | Prevents hidden manual work from being skipped |
| Approval matrix | Clarifies who signs off on what |
| Data handling notes | Supports privacy/security review across teams and vendors |
| Monitoring metrics | Shows if the automation drifts or fails |
| Rollback/runbook | Reduces outage and incident response time |

## Common design mistakes

- Automating approvals instead of preparing decisions for reviewers

- No exception queue or owner

- No audit trail for edits, approvals, and outputs

- Mixing production and test data in pilot workflows

- Optimizing for speed before accuracy and control

## Where this fits in the rollout sequence

Use this guide after selecting a workflow with the What to Automate First scorecard and before finalizing pilot scope. It also pairs well with our pilot-first vs full transformation comparison. US teams should also confirm vendor and subcontractor access boundaries early.