

AI Workflow Oversight Checklist

Use before introducing an AI-assisted workflow into production. This is a planning aid, not legal advice, a certification or a complete security assessment.

PURPOSE AND BOUNDARIES

- ☐ Define the permitted task and the tasks explicitly out of scope.
- ☐ Specify the information required and exclude unnecessary sensitive data.
- ☐ Assign a business owner and a technical owner.

HUMAN REVIEW

- ☐ Identify actions requiring approval before execution.
- ☐ Define when uncertainty must trigger escalation.
- ☐ Keep professional advice and consequential decisions with qualified people.
- ☐ Define a usable human takeover path.

DATA AND VENDORS

- ☐ Review access permissions and source-of-record rules.
- ☐ Review vendor processing, model-training, retention and location terms.
- ☐ Agree the rules for logs, sensitive data, deletion and access requests.
- ☐ Verify any claimed certification or contractual control; do not assume it.

TESTING AND OPERATION

- ☐ Test representative normal cases, edge cases and known failure modes.
- ☐ Record quality and acceptance criteria before release.
- ☐ Review action logs and exception queues.

☐ Define spend limits, rate limits and model-change controls.

☐ Maintain a rollback and incident escalation plan.

BEFORE LAUNCH

☐ Obtain the required business, security, legal and user acceptance reviews.

☐ Train the people supervising the workflow.

☐ Document ownership, support scope and periodic review.

Controls must be tailored to the organisation and agreed in the engagement. Conqueror Systems, the enterprise division of Conqueror Capital. Contact: buy@conqueror.capital

Questions or to discuss your answers: buy@conqueror.capital · enterprise.conqueror.capital