OpsPilot

Risk Assessment — User Manual

Hazard Identification & Residual Risk · AI Engineering Co-Pilot

What this guide covers — what a risk assessment is, how the OpsPilot module produces a defensible draft, what to have ready, and the document you receive.

1. What is a risk assessment?

A risk assessment systematically identifies the hazards of an activity or area, scores the risk before and after controls, tests whether those controls actually work, and sets specific additional controls wherever the residual risk is still unacceptable. The whole value is in the honesty of two numbers: the inherent risk (before controls) and the residual risk (after the controls that are genuinely in place).

2. What the OpsPilot module does

Role	Responsibility
🎯 **AI Risk Assessment Coach (OpsPilot)**	Identifies hazards by category, challenges weak or paper controls, tests whether each control is actually implemented, and ensures every unacceptable residual risk gets a specific, practical additional control. It is not the duty holder, regulator or competent person — your organisation remains responsible for verification and legal compliance.
👷 **Risk Owner / Task Expert (you)**	Know the activity, the environment, the people, and the controls actually in place. That ground truth is what makes the assessment defensible.

3. How it works — the 10-step process

#	Step
1	Activity description — what, where, who, when, and any vulnerable people
2	Risk matrix confirmation — company matrix or standard 5×5
3	Systematic hazard identification — 12 hazard categories
4	Hazard confirmation — team review before scoring
5	Inherent risk rating — before controls
6	Control effectiveness — are the controls real or paper?
7	Residual risk rating — after controls

#	Step
8	Additional controls — for every unacceptable residual
9	Emergency requirements
10	Sign-off and document generation

4. What you will be asked — have this ready

- The activity — what, where, who, when, and whether vulnerable people (contractors, visitors, public, inexperienced workers) are involved.
- The risk matrix to use — your organisation's, or the default 5×5.
- The controls actually in place — and honestly, whether they are implemented or just written down.

Tip — the assessment is only as good as your honesty about controls. A control that exists on paper but isn't followed should be scored as if it isn't there.

5. What you receive — the output

A complete Risk Assessment document (Word): the hazard register, inherent and residual risk scores, control-effectiveness assessment, the additional-control action plan, emergency requirements and sign-off.

6. Worked example (illustrative)

Cleaning inside a tank. Inherent risk of the atmospheric hazard is extreme. The site claims a control: “gas testing before entry.” OpsPilot tests it — is it actually done every time, by a competent person, with a calibrated instrument, and continuously monitored? If gas testing is one-off and not continuous, the control is partly paper, so the residual stays high and an additional control (continuous monitoring with an alarmed personal monitor) is required. That challenge — refusing to accept a paper control at face value — is what separates a defensible assessment from a comforting one.

7. Getting the best result

- **Score inherent first.** See the raw hazard before you credit any control.
- **Be honest about controls.** Paper controls don't reduce real risk.
- **Every unacceptable residual gets an action.** A high residual with no additional control is an open hole.
- **Name the vulnerable people.** Contractors and inexperienced workers change the assessment.