AI Agent Boundary Review Worksheet

Record review status, findings and follow-up actions.

Company / project

Reviewer

System or app

Review date

Review each topic. Record findings and actions below.

01 / Identify Tools and Authority

☐ Reviewed ☐ Needs action

Findings / next step

02 / Policy Enforcement at Boundaries

☐ Reviewed ☐ Needs action

Findings / next step

03 / Prompt Injection and Tool Misuse (Defensive Framing)

☐ Reviewed ☐ Needs action

Findings / next step

AI Agent Boundary Review Worksheet

Record review status, findings and follow-up actions.

04 / Data Leakage Controls

☐ Reviewed ☐ Needs action

Findings / next step

05 / Auditability

☐ Reviewed ☐ Needs action

Findings / next step

06 / Reliability and Failure Modes

☐ Reviewed ☐ Needs action

Findings / next step

07 / Outputs

☐ Reviewed ☐ Needs action

Findings / next step

AI Agent Boundary Review Worksheet

Record review status, findings and follow-up actions.

Summary and next steps

Key findings

Actions, owner and due date

See the reference guide for details. This worksheet does not certify compliance.