Kailash Consult Free resource · kailashconsult.com/resources

AIUC-1 Readiness Checklist

The six areas of AIUC-1, the security, safety and reliability standard for AI agents, with what each expects in plain words and the evidence to prepare.

How to use

- AIUC-1 is updated regularly. This checklist follows its six areas as published in 2026; confirm exact requirements in the current version before an audit.
- Some requirements need independent technical testing (for example third-party red teaming). Plan those early: they take the longest.
- Track each row as Ready, Partial, Not yet or N/A.

Example answers and mappings are templates, not facts about your company. Edit every bracket and validate each statement before sharing it with a customer or auditor.

Kailash Consult

A. Data and privacy

ID	Area	What AIUC-1 expects (plain words)	Evidence to prepare	Tip
F01	Data & privacy	Published terms of service and privacy policy that cover how the AI uses data.	Current ToS and privacy policy.	Make sure they mention AI features specifically.
F02	Data & privacy	Policies for what data goes into the AI and what comes out.	Input and output data policy.	Say whether customer data is used for training.
F03	Data & privacy	Protection of personal data in prompts, context and outputs.	PII handling controls and test results.	Show redaction or minimization in practice, not just in policy.
F04	Data & privacy	Limits on retention and access to AI interaction data.	Retention settings; access lists.	Include model provider retention terms.

B. Security

ID	Area	What AIUC-1 expects (plain words)	Evidence to prepare	Tip
F05	Security	Independent adversarial testing (red teaming) of the AI system.	Third-party red team report.	Longest lead time: book it first.
F06	Security	Detection and handling of adversarial inputs such as prompt injection.	Input filtering design; test results.	Test with your real tools and data connected.
F07	Security	Prevention of unauthorized actions by the agent.	Permission model; approval gates.	Agents should act with the user's permissions, never broader.
F08	Security	Access control and protection of the AI system and its secrets.	Access reviews; secret management.	Reuse your SOC 2 or ISO 27001 evidence here.

C. Safety

ID	Area	What AIUC-1 expects (plain words)	Evidence to prepare	Tip
F09	Safety	A defined taxonomy of the harms your AI could cause.	Risk taxonomy document.	Make it specific to your product and users.
F10	Safety	Testing before deployment against that taxonomy.	Pre-deployment test results.	Keep a fixed evaluation set and rerun it on each release.
F11	Safety	Prevention of harmful or out-of-scope outputs.	Output filters; refusal behavior tests.	Document what the agent must never do.
F12	Safety	Human oversight where outputs carry real consequences.	Oversight design; approval records.	Show where a person confirms high-impact actions.

D. Reliability

ID	Area	What AIUC-1 expects (plain words)	Evidence to prepare	Tip
F13	Reliability	Controls that reduce hallucinated or unsupported outputs.	Grounding design; accuracy tests.	Measure it; do not just describe it.
F14	Reliability	Restriction of unsafe or unintended tool calls.	Tool allowlists; test cases.	Log every tool call for review.
F15	Reliability	Ongoing evaluation of reliability in production.	Monitoring dashboards; periodic test reports.	Some reliability testing is expected from a third party.

Kailash Consult

E. Accountability

ID	Area	What AIUC-1 expects (plain words)	Evidence to prepare	Tip
F16	Accountability	Named owners for the AI system and its risks.	RACI; governance charter.	One accountable executive.
F17	Accountability	An AI incident response plan.	IR plan covering AI failures and misuse.	Extend your existing IR plan rather than starting over.
F18	Accountability	Due diligence on AI vendors and model providers.	Vendor assessments.	Include model providers' data and retention terms.
F19	Accountability	Activity logging that allows investigation.	Log design; retention settings.	Logs must cover inputs, outputs and actions.
F20	Accountability	Documentation and change control for the AI system.	System documentation; change records.	Track prompt and model changes like code changes.

F. Society

ID	Area	What AIUC-1 expects (plain words)	Evidence to prepare	Tip
F21	Society	Prevention of AI-enabled cyber attacks using your system.	Abuse prevention controls; tests.	Rate limits and abuse monitoring count.
F22	Society	Prevention of catastrophic misuse, including CBRN-related content.	Content safeguards; test results.	Rely on provider safeguards only if you test them in your product.

Getting certified

ID	Area	What AIUC-1 expects (plain words)	Evidence to prepare	Tip
F23	Audit	Assessment by an accredited AIUC-1 auditor.	Evidence package for all applicable requirements.	Ask the auditor which optional requirements apply to you.
F24	Ongoing	Periodic technical testing keeps the certificate current.	Testing calendar.	Budget for recurring tests, not one-off.

Free resource from Kailash Consult. Free to use inside your company. Not for resale or redistribution. kailashconsult.com/resources