

AI is shipping code. Assurance has to ship with it.

A practical path to validating the security, safety, and reliability of AI coding agents.

AIUC-1

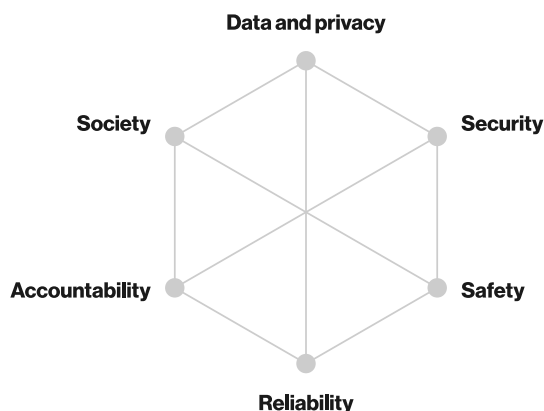
The assurance question

AI coding agents are moving into workflows where they can write and execute code, interact with development environments, handle sensitive information, and influence systems that matter to the business.

Organizations need evidence that the safeguards around a specific agent work in practice.

What AIUC-1 brings into focus

AIUC-1 is the standard for evaluating AI agents across six enterprise risk areas:



AIUC-1 goes beyond principles-based guidance by testing AI agents against thousands of real-world adversarial scenarios to see how they perform in production.

For coding agents, that means asking:



Can the agent protect secrets and credentials?

Does it support secure code generation?

Can it resist prompt injection in files and configuration artifacts?

Are its actions appropriately contained when it runs code or uses tools?

Where Coalfire fits

AIUC provides the AIUC-1 standard and certification model. Coalfire helps organizations scope the right system, identify evidence needs, prepare for technical testing, and align the teams responsible for security, engineering, governance, risk, and procurement.

▶ **Start with one AI system, one workflow, and one focused AIUC-1 readiness conversation.**

To learn more about Coalfire Services visit [Coalfire.com](https://coalfire.com)