

AIUC-1 assurance for AI systems moving into enterprise adoption

A joint path from AI trust questions to a scoped, evidence-based assurance conversation.

The opportunity

AI agents are becoming part of customer-facing and business-critical workflows.

Product, security, engineering, risk, compliance, legal, and procurement leaders need a clear way to understand what an AI system can do, validate the safeguards around it, and provide credible evidence to the people who depend on it.

Three ways to enter the conversation

AI product companies

Differentiate on AI security and demonstrate that safeguards have been evaluated as the product moves beyond pilots.

Enterprise deployments

Secure the last mile of third-party AI solutions before they become part of critical workflows.

Regulated and high-scrutiny use cases

Build confidence in internal coding agents and AI systems involved in high-stakes workflows, including financial reporting.

The joint message

- AIUC provides the AIUC-1 standard and certification model.
- Coalfire brings cybersecurity advisory, technical testing, assessment, and assurance experience.
- Together, the teams can help organizations move from broad AI trust questions to a practical readiness and assessment conversation.

The joint motion

- Identify the AI system, agent, product, or workflow that matters most.
- Clarify the deployment context, stakeholders, risk drivers, and assurance trigger.
- Determine the likely AIUC-1 scope and evidence needs.
- Agree on the next step and the right AIUC and Coalfire participants.

What the conversation can produce

- A clearer scope for the AI system or workflow.
- An initial view of evidence and control-mapping needs.
- Priorities for technical-testing preparation and remediation.
- A defined path toward an assessment or certification discussion.

► **Request a joint AIUC-1 readiness conversation for one AI agent workflow or capability.**

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