

FOR ISSOS AND AUTHORIZING OFFICIALS

Every path to authorization, mapped before we deploy.

Every AI teammate runs under someone's ATO; the question is whose, not whether. We agree the path in writing before anything goes live.

PATH 1

Inherit the boundary

TYPICALLY WEEKS

The teammate runs inside a system that already holds an ATO, uses only services already authorized there, and does not change its risk posture.

WHAT WE PROVIDE

- Boundary diagram
- Documented data flows
- Written confirmation that no new external endpoints are called

PATH 2

Significant change review

TYPICALLY 1–3 MONTHS, AO-DEPENDENT

The teammate materially changes the authorized system, and the authorizing official can accept it under the existing ATO after review. Most agentic deployments land here.

WHAT WE PROVIDE

- Security impact analysis
- Updated SSP artifacts
- ISSO engagement from day one

PATH 3

New ATO or FedRAMP

TYPICALLY 6–24 MONTHS

The teammate stands up its own infrastructure, or it is hosted and access is sold. The hosted case is where FedRAMP applies.

WHAT WE PROVIDE

- A full RMF package
- Or FedRAMP authorization for a hosted service

WHAT MOVES A TEAMMATE FROM PATH 1 TO PATH 2

New external connection

A call to a model endpoint outside the authorized boundary. The most common trigger.

Write actions

Opening a ticket, provisioning access or submitting a request is different risk territory from read-only advice.

New data flows or aggregation

Reading across systems that were separate can raise the categorization of the whole.

Non-person entity identity

A teammate authenticating on behalf of a person is a question ICAM was not designed to answer.

EVERY TEAMMATE ALSO CARRIES A PUBLISHED AUTONOMY LEVEL

L1 Output	L2 Actions and tools	L3 Decision points	L4 Process and plan	L5 Initiation and time
--------------	-------------------------	-----------------------	------------------------	---------------------------

Everything in production on our roster today runs at L1 or L2 (shaded). The level can change without redeploying the teammate.

We never claim “no ATO required.” We claim inheritance of your existing authorization, subject to your standard change review, and we bring the ISSO in before we deploy, not after.

Let's start a conversation.

questions@empower.ai

EmpowerAI