SOLUTIONS BY JEWEL
AI & TECHNOLOGY GOVERNANCE ADVISORY

Federal Continuous Authorization Control Map

A structured governance instrument connecting mission requirements, identity, authorization, security controls, evidence, and continuous assessment across federal technology environments.

PURPOSE
Map how a federal mission capability moves from operational need through authorization and control implementation to evidence, continuous monitoring, risk visibility, and reassessment.

1 Control Map

MISSION CAPABILITY
Identify the mission capability being supported.

MISSION-CRITICAL APPLICATION
Identify the application required to support the mission capability.

PLATFORM
Identify the platform or shared technology environment hosting the capability.

IDENTITY / ICAM
Identify how users, services, devices, and privileged actors are authenticated, authorized, and governed.

AUTHORIZATION
Identify the authorization decision, authority, boundary, and applicable authorization mechanism.

SECURITY CONTROL
Identify the security controls directly implemented for the application or capability.

INHERITED CONTROL
Identify controls inherited from the platform, enterprise service, infrastructure, or shared environment.

CI/CD SECURITY GATE
Identify automated security, compliance, testing, or policy gates embedded in the delivery pipeline.

OPERATING FLOW

MISSION › AUTHORIZATION › CONTROL › EVIDENCE › CONTINUOUS ASSESSMENT

2 Evidence & Continuous Assessment

EVIDENCE
Identify the artifacts, telemetry, test results, logs, configurations, attestations, or other evidence demonstrating control operation.

CONTINUOUS MONITORING
Identify what is monitored continuously and how changes in security posture are detected.

RISK STATUS
Record the current risk posture, material findings, exceptions, or conditions affecting authorization.

AO VISIBILITY
Identify the information available to the Authorizing Official for current risk and authorization decisions.

REASSESSMENT TRIGGER
Define the event, threshold, material change, vulnerability, configuration change, mission change, or other condition that requires reassessment.

Governance Questions & Control Principle

4 Governance Questions

MISSION

What mission capability must remain available, including during degraded or disconnected operations?

IDENTITY

Can authorized users, services, devices, and privileged actors be identified and governed at the edge?

AUTHORIZATION

Who has authority to approve access, change, deployment, exception, and risk decisions?

CONTROLS

Which controls are implemented at the application, platform, enterprise, and inherited-control levels?

EVIDENCE

What machine-readable or otherwise auditable evidence demonstrates that required controls are operating?

ASSESSMENT

What is monitored continuously, who sees the current risk posture, and what event triggers reassessment?

5 Control Principle

GOVERNING PRINCIPLE

Authorization becomes operational when identity, controls, evidence, and continuous assessment are connected to the mission capability.

6 Reassessment

TRIGGER DEFINITION

Define the event, threshold, change, or risk condition that requires renewed review and documented authorization.