



AO Integrity
EXECUTION AUTHORITY
YOU CAN TRUST

FW-002

THE RUNTIME AUTHORITY LIFECYCLE

HOW VALID AUTHORITY BECOMES INVALID AUTHORITY OVER TIME

AOI FRAMEWORK SERIES

FW-002 | REV 01

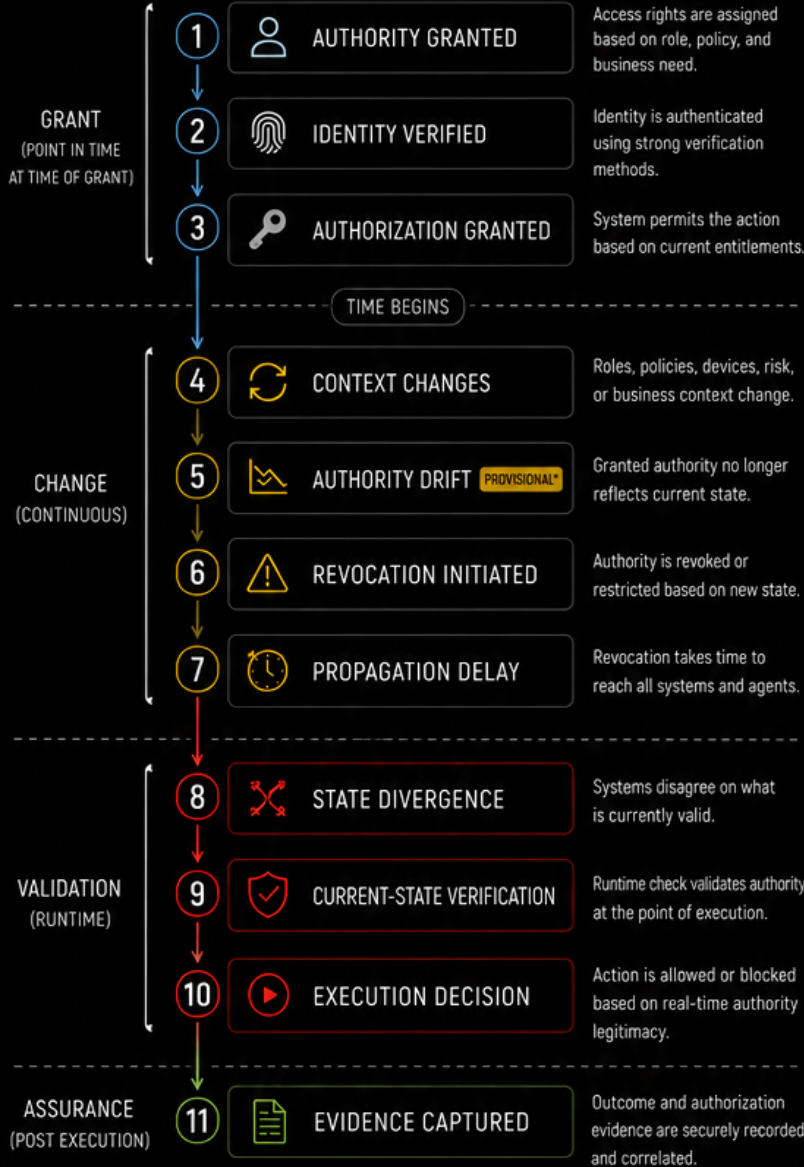
JULY 2026

THE REALITY

- Authority is rarely wrong at the moment it is granted.
- It becomes wrong because organizations change.
- Runtime governance manages the time between change and execution.
- The goal is not just to grant access securely, but to ensure it remains legitimate at the point of execution.

WHAT DRIVES CHANGE

- Role / Job changes
- Manager changes
- Policy updates
- Group / Entitlement changes
- Contractor / Vendor expiry
- Device posture changes
- Risk / Threat changes
- Agent context changes
- System latency & sync delays



COMMON FAILURE POINTS

- Unmanaged Authority Drift**
Access remains after role, policy, or risk changes.
- Revocation Lag**
Delays allow invalid access to persist.
- State Divergence**
Systems, apps, and agents operate on stale state.
- Stale Sessions**
Long-lived tokens or sessions outlive authority.
- Cross-System Gaps**
Not all systems enforce revocation consistently.
- Evidence Gaps**
Inability to prove authority was valid at execution.

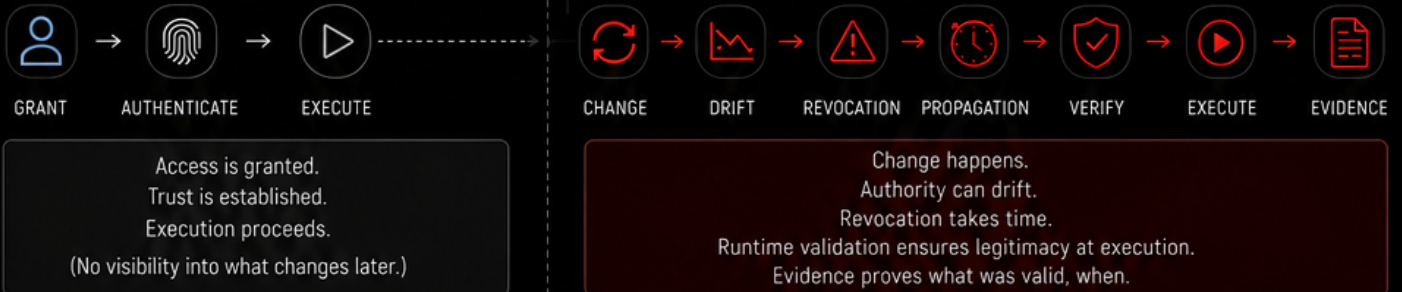
OUTCOMES OF STRONG RUNTIME GOVERNANCE

- Only legitimate actions are executed.
- Risk is reduced from stale or excessive access.
- Compliance and audit evidence is complete.
- Trust in autonomous systems increases.

TRADITIONAL IDENTITY STOPS HERE

VS.

RUNTIME GOVERNANCE CONTINUES



AUTHORITY IS NOT STATIC. IT IS A CONTINUOUSLY CHANGING OPERATIONAL STATE.

PROVISIONAL*

Authority Drift is an umbrella condition: the authority available at execution no longer accurately reflects the authority that should exist in the current operational state. Its three canonical mechanisms — Revocation Drift, State Divergence, and Governance Drift — are formalized in the Authority Drift RRB (forthcoming).