



THE MISSING RUNTIME DOMAIN IN THE AI RISK ECOSYSTEM

Existing frameworks explain how AI behaves.
Runtime Authority explains **whether execution was legitimate**.

DATA RISKS	
BS	Bias unfair or skewed outputs
PV	Privacy sensitive data exposure
DQ	Data Quality inaccurate data
DL	Data Lineage unclear provenance
DR	Data Drift data changes over time
LE	Data Leakage sensitive data leaks
CR	Consent Risk missing consent
SD	Synthetic Data false confidence
ES	Embedded Secrets hidden in data
PI	PII Exposure personal data exposed

MODEL RISKS	
HL	Hallucination outputs fabricated
EX	Explainability lacks transparency
OF	Overfitting training only
UF	Underfitting fails to learn
RB	Robustness breaks under change
EV	Evaluation Fail poor evaluation
VG	Validation Gap weak validation
MD	Model Drift degrades over time
PS	Prompt Sensitivity too prompt-sensitive
MB	Metric Blindness wrong metrics

AGENT RISKS	
AH	Autonomy Risk too much autonomy
TM	Tool Misuse tools used wrong
UA	Unintended Actions not as intended
PE	Permission Escalation excess privileges
IN	Prompt Injection malicious input
SM	Social Manipulation social tricks
DG	Delegation Risk risky delegation
MR	Memory Risk memory exposure
LF	Loop Failure repeats bad actions
RG	Rollback Gap cannot revert

SECURITY & OPS RISKS	
VP	Vulnerability exploitable gaps
CT	Cyber Threats external attacks
AB	API Abuse APIs misused
TT	Token Theft tokens stolen
MU	Malicious Use harmful intent
DE	Data Exfiltration data stolen
DP	Deployment Risk unsafe deploy
IG	Integration Risk integration fails
LT	Latency Risk slow responses
CO	Cost Overrun costs exceed plans

GOVERNANCE RISKS	
MG	Monitoring Gap issues undetected
DO	Decision Ownership unclear ownership
HO	Human Oversight too little oversight
TR	Traceability not traceable
CP	Compliance Risk violates standards
AG	Audit Gap incomplete audits
LG	Legal Risk legal exposure
IP	IP and Copyright ownership issues
ET	Ethics Risk unethical impact
RR	Regulatory Risk violates rules

EXECUTION GOVERNANCE (THE MISSING RUNTIME DOMAIN)	
	Authority Drift authority changed after authentication
	Current-State Verification verify current authority before execution
	State Divergence systems disagree on authority state
	Revocation Drift revocation not yet operationally effective
	Staleness Window authorization exceeds acceptable window
	Execution Legitimacy action executed on invalid authority
	Authority Integrity proof authority was valid at execution
	Continuous Authority Validation authority rechecked throughout execution

THE EXECUTIVE REALITY

An action can be:

- ☒ Authenticated
- ☒ Authorized earlier
- ☒ Policy compliant
- ☒ Fully logged
- ☒ Technically correct

And still be illegitimate at execution.

THE QUESTION THAT MATTERS MOST

WAS THIS ACTION AUTHORIZED AT THE MOMENT IT OCCURRED?



CORRECT EXECUTION
IS A SECURITY PROPERTY.



LEGITIMATE EXECUTION
IS A GOVERNANCE PROPERTY.

WHY IT MATTERS



Prevents unauthorized actions with valid credentials



Reduces risk from stale, diverged, or delayed state



Strengthens audit, compliance, and trust



Protects people, data, and the organization

THE FIVE-LAYER LINEAGE: FROM HOW IT HAPPENS TO WHETHER IT SHOULD HAVE HAPPENED



IDENTITY

Who are you?



AUTHENTICATION

Can you prove who you are?



AUTHORIZATION

What are you allowed to do?



GOVERNANCE

Can we audit and govern it?



AUTHORITY INTEGRITY

Was it authorized at this moment?

Every previous layer explains how execution occurred.

Authority Integrity proves whether execution should have occurred.

ABOUT AUTHORITY INTEGRITY

Authority Integrity (Execution Governance) is the runtime capability to verify, prove, and evidence that the actor (human or agent) was authorized to perform this specific action at this specific moment, across all relevant systems and states.



AO INTEGRITY PROVIDES EVIDENCE THAT **EXECUTION AUTHORITY** EXISTED AT THE MOMENT OF ACTION.