TRAC Council

Enterprise Trust • Financial Risk • Responsible AI

Trust Standards for Real-Time Systems

A voluntary standards charter, promoting safe, secure, and responsible innovation across enterprise technology, financial systems, and AI-driven execution environments.

TRAC Council Charter v1

Effective: January 2026

TRAC-001: Execution Trust Standard (Baseline)

Version: 1.0

Status: Draft (Baseline Standard)

Published: January 2026

Owner: TRAC Council

1. Executive Summary

TRAC-001 defines the baseline execution trust standard for systems operating at machine speed. It establishes minimum enforceable controls required to prevent unsafe or unauthorized execution of actions across automated systems, agentic AI workflows, and platform-level decision engines.

2. Scope

This standard applies to any enterprise system capable of executing actions that may produce material operational, financial, legal, safety, privacy, or reputational outcomes.

Included system categories:

- AI agents and autonomous workflows

- Financial transaction and payment systems

- Access control and identity systems

- Credit approval and underwriting systems

- Configuration and infrastructure automation systems

- Data movement, export, and replication systems

- Customer decisioning and recommendation engines

3. Key Definitions

Execution: A system action that changes state, grants access, transfers value, triggers workflows, or produces irreversible outcomes.

Execution Risk: Risk arising at the moment an automated system executes an action without adequate safeguards.

Execution Trust: The measurable assurance that execution events are authorized, constrained, observable, and auditable.

Hard Stop: A mandatory control that prevents execution until required conditions are met.

Evidence-of-Control: Logs, records, or telemetry proving that controls were applied at runtime.

Machine-Speed Systems: Systems operating in real-time or near-real-time where decisions and actions occur faster than human oversight.

4. Baseline Principles

- Trust must be enforced at runtime, not validated only after execution.

- All material execution must be attributable to an identity, authorization, and justification.

- Controls must operate at the same speed as the system they govern.

- Auditability must be built into execution pathways, not layered externally.

- Execution must be measurable, observable, and interruptible.

5. Baseline Control Requirements

TRAC-001.1 Execution Classification

Organizations MUST classify execution pathways by risk tier (Low/Moderate/High/Critical) based on the materiality of outcomes, reversibility, regulatory exposure, and user harm potential.

TRAC-001.2 Authorization & Identity Binding

All execution events MUST be bound to an authenticated identity (human or system) and must record role, authorization scope, and delegation chain.

TRAC-001.3 Policy-Driven Hard Stops

Critical execution actions MUST be gated by enforceable hard stops that verify required policy conditions prior to action completion.

TRAC-001.4 Justification Capture

Execution pathways MUST require justification metadata for high-risk actions, including reason codes, approvals, and policy references.

TRAC-001.5 Human-in-the-Loop Controls

Where required by risk tier, systems MUST support human approval prior to execution. Human approval MUST be attributable, timestamped, and non-repudiable.

TRAC-001.6 Runtime Monitoring & Alerting

Organizations MUST implement real-time monitoring of execution events, including anomaly detection, velocity thresholds, and alert escalation paths.

TRAC-001.7 Evidence Logging & Audit Trail

Systems MUST generate immutable logs capturing execution intent, pre-checks performed, outcomes, exceptions, and control enforcement results.

TRAC-001.8 Interruptibility & Kill Switch

Systems MUST support interruption mechanisms capable of halting execution flows at runtime, including manual shutdown and automated circuit breakers.

TRAC-001.9 Exception Handling & Override Governance

Overrides MUST be restricted, logged, justified, and reviewed. Emergency override access MUST expire automatically and be subject to post-event review.

TRAC-001.10 Control Testing & Validation

Execution controls MUST be tested regularly through simulation, red teaming, and control validation exercises. Failures MUST be tracked through issue management with defined remediation SLAs.

6. Minimum Evidence Requirements

Organizations implementing TRAC-001 MUST be able to produce the following evidence:

- Execution classification inventory and tier mapping

- Access/authorization matrix for execution roles

- Hard stop enforcement rules and validation checks

- Immutable runtime execution logs

- Alerting and escalation playbooks

- Kill switch / circuit breaker runbooks

- Override governance logs and approval evidence

- Control testing reports and remediation tracking

7. Compliance, Reporting, and Certification Readiness

Compliance with TRAC-001 is achieved when an organization demonstrates that baseline controls are operational, enforceable, and auditable across all material execution pathways. TRAC-001 is designed to support audit readiness and may be mapped to regulatory requirements including OCC, FDIC, FRB, CFPB, SEC, GDPR, and ISO-based control frameworks.

8. Implementation Guidance (Baseline)

Recommended implementation steps:

- Identify all execution pathways across systems, workflows, and agents.

- Classify execution pathways into risk tiers.

- Implement hard stops for high-risk and critical actions.

- Deploy centralized logging and evidence-of-control telemetry.

- Establish real-time monitoring and escalation.

- Implement kill switch and rollback protocols.

- Test controls quarterly through simulation and adversarial exercises.

Appendix A: Example Execution Events

- Initiating a wire transfer or payment

- Granting privileged admin access

- Approving a loan or credit extension

- Deploying infrastructure configuration changes

- Exporting sensitive datasets

- Executing automated vendor payments

- Publishing content or recommendations at scale

Appendix B: TRAC Standard Alignment Notes

TRAC-001 serves as the baseline standard. Higher-tier TRAC standards (TRAC-002+) will extend requirements for sector-specific controls, agentic system governance, evidence maturity scoring, and continuous compliance automation.