

Risk Routing Specification

Version 1.0 | October 5, 2026

<https://www.stratedgeworkflow.com/research/specifications/guardroute-risk-routing>

This specification describes StratEdge's own product and control model. It is not an industry standard, a certification, or a customer result.

How GuardRoute decides which control applies before a high-risk action, including an action requested by an AI agent, is allowed to execute.

Purpose

GuardRoute controls what happens before it happens. It does not hold funds and it does not execute the action.

This specification is StratEdge's product model, version 2026-10-05. It is not a regulation and it does not replace fraud, compliance, or treasury judgment.

Path

Action request, then risk signals, then policy evaluation, then a decision, then human or automated control, then execution by the customer's own system, then an evidence record of the control decision.

When an AI agent attempts a sensitive action - moving money, changing a beneficiary, releasing information, or starting another high-risk workflow - the same path applies before execution.

Outcomes

The decision is one of ALLOW, ALLOW WITH LIMITS, REQUIRE APPROVAL, ESCALATE, HOLD, or BLOCK.

A public example is a \$240,000 outbound wire to a new beneficiary, in an unusual geography, at elevated velocity. That illustration returns HOLD and names the reviewers and reason codes. The example is illustrative data.

Boundary

ProofAudit proves what happened. GuardRoute controls what happens before it happens. The document package, when the products are used together, is ProofAudit.

How to cite this specification

StratEdge Workflow Systems. "Risk Routing Specification." Version 1.0, October 5, 2026.
<https://www.stratedgeworkflow.com/research/specifications/guardroute-risk-routing>

PDF: <https://www.stratedgeworkflow.com/research/specifications/guardroute-risk-routing/pdf>