RUNTIME GOVERNANCE EXECUTIVE REPORT™

Monthly Governance Evidence

Northwind Logistics — autonomous operations & procurement agents

REPORTING PERIOD	REFERENCE	PREPARED VIA	CLASSIFICATION
1–31 May 2026	RGER-2026-05-NWL	Managed Governance Partner™	Board · Confidential

1 · EXECUTIVE SUMMARY

The period at a glance.

Runtime Governance evaluated **48,920** agent actions before execution this period across 12 governed agents. **842** unsafe actions were prevented and **466** were escalated for human review. Governance coverage held at 100% of defined forbidden states (Ω), including two newly onboarded tools. No uncovered reachable path to a forbidden state was observed at period end.

48,920
Actions governed (pre-execution)

842
Unsafe actions prevented

466
Escalated for review

100%
Ω coverage (18 states)

2 · RUNTIME ACTIVITY

Every action resolved to a verdict.

ALLOW · 47,612 (97.3%) BLOCK · 842 (1.7%) ESCALATE · 466 (1.0%)

Volume rose 14% versus April as the procurement agent expanded, while blocked actions fell 9% — consistent with an improving governance posture. 12 agents and 34 tools were under governance.

3 · ACTIONS PREVENTED

What was blocked before it executed.

CATEGORY	COUNT	REPRESENTATIVE EXAMPLE
Unsafe external action	572	Calls to unapproved third-party APIs
Data exfiltration	121	Bulk export of customer records to an external endpoint
Privilege escalation	64	Agent attempting to elevate its own role
Destructive operation	47	Mass-delete against a production datastore
Unauthorised fund transfer	38	Transfer above threshold with no approver

4 · ESCALATIONS

Routed to a human, with outcomes.

Of **466** escalations, **449** were approved after review and **17** were rejected. Median time-to-decision was **6 minutes**. Escalations concentrated on first-time vendor payments and cross-system data movements.

5 · GOVERNANCE POSTURE

Coverage against forbidden states (Ω).

18 forbidden states are defined for this environment, spanning financial loss, data exfiltration, privilege escalation, and destructive operations. Two new tools were onboarded and re-mapped to Ω during the period. End-of-period coverage: **100% of defined states**, with **0** uncovered reachable paths.

6 · RISK REDUCTION

Exposure removed before it could occur.

The 38 prevented unauthorised-transfer attempts alone represented a modelled single-event exposure of [redacted]+ had any reached execution. Reachable exposure across all governed agents fell relative to the April baseline. Figures are modelled and illustrative.

7 · RECOMMENDATIONS

Prioritised next actions.

- HIGH — Tighten the approval policy on payment tools so first-time vendor transfers always require a named approver.
- MEDIUM — Review the two newly integrated third-party APIs and confirm their Ω mappings with the security team.
- MEDIUM — Schedule the quarterly Ω revalidation to keep forbidden states aligned with new workflows and regulation.
- LOW — Extend governance to the planned logistics-routing agent before it reaches production.

8 · EVIDENCE APPENDIX

Tamper-evident, reproducible record.

Decisions recorded	48,920
Audit trail	Hash-chained · tamper-check passed ✓
Replay determinism	100% on sampled re-run ✓
Attestation	ATT-2026-05-NWL · engine commit pinned
Evidence retention	12 months

Illustrative sample. “Northwind Logistics” is fictional and all figures are for illustration only. A live report reflects your systems, your defined Ω, your agents, and your data.