

General AI Technology Audit - Post-Deployment

Focus Area: Continuous Monitoring, Production Drift, & Sustained Compliance

Framework Alignment: NIST AI RMF 1.0 (Manage), ISO/IEC 42001, SEC Operational Risk Rules

1. Continuous Drift & Performance Tracking

Control ID	Audit Requirement / Question	Regulatory Trigger
GEN-POS T-01	Are automated latency, concept drift, and data drift metrics actively tracked on live production inputs vs. training baselines?	NIST AI RMF Manage
GEN-POS T-02	Are automated alerts configured to notify the risk owner if accuracy drops below the designated SLA (e.g., 5% variance)?	Enterprise Risk Control
GEN-POS T-03	Is a scheduled re-validation cadence (e.g., quarterly/semi-annual) established to re-bench accuracy against new live data?	ISO/IEC 42001 Continuous Improvement

2. Post-Hoc Explainability & Auditability

Control ID	Audit Requirement / Question	Regulatory Trigger
GEN-POS T-04	Are all production inputs, model version hashes, and generated outputs logged in a tamper-evident audit trail for legal discovery?	SEC Operational Risk / SOC 2 Type II

GEN-POS T-05	Can the system generate post-hoc explanations for contested decisions or adverse actions within legally mandated timeframes?	Adverse Action / FCRA / GDPR Art. 22
-------------------------	--	--------------------------------------

3. Feedback Loops & Incident Management

Control ID	Audit Requirement / Question	Regulatory Trigger
GEN-POS T-06	Is a structured user feedback mechanism (e.g., thumbs down / escalation tag) integrated into the production UI to capture model failures?	ISO 42001 Customer Satisfaction
GEN-POS T-07	Is an AI Incident Response Protocol active specifying notification timelines for data leaks, hallucinations, or bias events?	NIST Computer Security Handling / SEC