AML / Transaction Monitoring
Model Risk Management Checklist

This checklist translates the SR 11-7 framework into actionable steps for AML and transaction monitoring models. Whether you're preparing for a regulatory exam, implementing a new AML system, or strengthening existing model risk management practices, this checklist ensures you've addressed the core requirements across governance, validation, documentation, and ongoing monitoring.

The 12 sections mirror the model risk management lifecycle—from establishing ownership and documenting typology coverage to maintaining examiner-ready documentation—helping you build the comprehensive, defensible MRM framework regulators now expect for AML AI systems. For more information, please see the disclaimer at the end of the document.

---

1. Governance and ownership

☐ **Identify model owner** (e.g., BSA Officer, Head of AML)
☐ **Document purpose and regulatory obligations** (e.g., BSA/AML, sanctions, KYC)
☐ **Assign independent MRM group**
☐ **Include in enterprise model inventory**
☐ **Complete risk classification** (e.g., high, medium, low)
☐ **Engage governance bodies**

- AML Governance Committee
- Model Risk Committee
- Compliance Committee

2. Typology coverage mapping

☐ **Complete full typology inventory:**

- Structuring
- Rapid movement
- High-risk jurisdictions
- Funnel accounts
- OFAC/Sanctions anomalies
- Human trafficking indicators
- Elder abuse
- Synthetic ID / mule activity
- Crypto-related typologies
- Purchase fraud/payment fraud indicators
- Dormant → sudden activity

☐ **Prepare model-to-typology mapping document**
☐ **Identify gaps and mitigation plan** (e.g., rules, features, post-processing, manual review)
☐ **Refresh typology library** (recommended annually)

3. Data governance

☐ **Document data lineage** (e.g., core banking → data warehouse → model → alerting → SARs)
☐ **Check event ingestion** (e.g., balances, transaction codes, timestamps, country codes)
☐ **Test for completeness** (e.g., missing transactions, MT103 fields, merchant data, beneficiaries)
☐ **Monitor data quality** (e.g., schema changes, missing fields, null spikes)
☐ **Document entity resolution quality** (e.g., customer linking, householding, merging parties)
☐ **Check retention schedules for compliance** (BSA/AML 5-year retention rule)
☐ **Validate training data for ML models as representative**
☐ **Document known gaps** (e.g., thin files, third-party processor delays)

4. Model development (Rules, AI, Hybrid)

Rules-based models

☐ **Document rule logic**
☐ **Document threshold rationale** (e.g., historical SARs, risk appetite, peer benchmarks)
☐ **Explain segmentation logic** (e.g., risk-tiering, geography, product type)

Machine learning / AI models

☐ **Document model architecture** (e.g., supervised, unsupervised, anomaly detection)
☐ **List feature definitions and transformations**
☐ **Explain training data windows and labels**
☐ **Test typology alignment** (e.g., does model catch what examiners care about?)
☐ **Document hyperparameters and check for reproducibility**

General build requirements

☐ **State model assumptions clearly**
☐ **Document expected limitations**
☐ **Include benchmark model or rule comparison**

5. Explainability and transparency

☐ **Ensure global explainability** (e.g., SHAP, feature importance, rule contribution)
☐ **Ensure local explainability for each alert** (e.g., why did this surface?)
☐ **Ensure ability to present results to examiners and analysts in plain English**
☐ **Ensure clear mapping to SAR narratives** (e.g., what behavior triggered the alert?)
☐ **Ensure no prohibited or unreviewable features** (e.g., race, gender, sensitive inferences)
☐ **Document prompt design, constraints, and intended use** (e.g., LLMs)
☐ **Define human review criteria and rejection standards for generated content**

6. Independent model validation*

**Must be independent of AML operations and model development.*

Conceptual soundness

☐ **Check methodology is appropriate for AML risk**
☐ **Validate assumptions**
☐ **Test typology mapping independently**

Data and process verification

☐ **Reproduce model outputs**
☐ **Verify ingestion integrity**
☐ **Confirm data transformations and joins**

Outcomes analysis

☐ **Test alert quality** (e.g., precision, lift, SAR-conversion improvement)
☐ **Back-test with historical SARs**
☐ **Anayze false-positives / false-negatives**
☐ **Conduct scenario stress tests** (e.g., seasonal changes, product launches, new geographies)
☐ **Conduct adversarial testing** (e.g., simulate laundering patterns)

Regulatory compliance

☐ **Ensure rules cover required AML behaviors**
☐ **Ensure sanctions/OFAC components are validated separately**
☐ **Ensure model supports SAR decision-making, but does *not* automate SAR filing**
☐ **Verify "human-in-the-loop" oversight**

7. Tuning and threshold management

☐ **Document tuning methodology** (e.g., data period, thresholds, scoring calibration)
☐ **Justify false positives reduction**
☐ **Ensure tuning decisions do *not* reduce compliance coverage**
☐ **Log and version all tuning events**
☐ **Conduct an independent review of tuning changes**
☐ **Measure SAR conversion rate impact**

8. Ongoing monitoring

Operational

☐ **Monitor data ingestion**
☐ **Track systems availability and latency**
☐ **Monitor alert generation stability**

Performance

☐ **Conduct monthly alert KPI reviews:**
- Alert volume trends
- SAR conversion rate
- Analyst productivity
- Typology detection rates
- Distribution of alert types

☐ **Conduct drift monitoring:**
- Feature drift
- Outcome drift
- Customer population changes

☐ **Conduct false-negative logic tests** (e.g., sampling high-risk accounts with 0 alerts)

9. Change management

☐ **Document version control for rules, code, and ML models**
☐ **Perform materiality test** (e.g., does a change require revalidation?)
☐ **Perform UAT testing with evidence**
☐ **Obtain governance approval before deployment**
☐ **Notify stakeholders** (e.g., compliance, investigations, operations, audit)

10. Human-in-the-loop and investigations

☐ **Document analyst override workflow**
☐ **Review all overrides logged** (recommended periodically)
☐ **Align SAR narrative templates to model triggers**
☐ **Ensure availability of evidence available for why the model flagged or didn't flag behavior**
☐ **Perform quality assurance (QA) sampling on alerts**

11. Third-party model considerations

☐ **Complete vendor due diligence** (e.g., MRM, SOC2, AML expertise)
☐ **Receive documentation** (e.g., white-box or black-box expectations)

☐ Ensure explainability is sufficient for regulators
☐ Store model release notes and tuning notes from vendor
☐ Obtain right-to-audit and access to validation results
☐ Obtain vendor SLA for model performance and data integrity

12. Examiner-ready documentation package*

This is what regulators will expect* ***during an AML/model exam**.*

Core documents

- AML Model Development Document
- AML Model Validation Report
- Tuning and Threshold Rationale Document
- Typology Coverage Mapping
- Data Lineage and Data Dictionary
- Alert Quality KPIs (12–24 months)
- Drift Monitoring Reports
- Change Log (rules and ML versions)
- Back-testing and SAR conversion testing
- Quality Assurance Review summaries
- Governance committee minutes
- Vendor documentation (if applicable)

Evidence

- Sample alerts with explanations
- Historical SARs matched to model triggers
- Drift charts
- Fairness or bias checks (if ML used)
- QA sampling worksheets
- Operational dashboards

DISCLAIMER
This AML/Transaction Monitoring Model Risk Management Checklist is provided for informational and educational purposes only and does not constitute legal, regulatory, or professional advice. This checklist is not exhaustive and should not be relied upon as a complete framework for compliance with SR 11-7, Bank Secrecy Act (BSA), Anti-Money Laundering (AML) regulations, or any other applicable laws and regulatory requirements.

Key Limitations:

Not Comprehensive: This checklist represents common elements of model risk management programs but may not address all risks, requirements, or circumstances applicable to your organization's specific business model, risk profile, regulatory environment, or jurisdictional obligations.

Risk Assessment Recommended: Organizations should conduct their own comprehensive risk assessments to identify, evaluate, and mitigate risks specific to their operations, customer base, products, services, and geographic footprint that may not be reflected in this template.

Not Legally Binding: This document does not create any legal obligations, contractual relationships, warranties, or representations. It is not a substitute for consultation with qualified legal counsel, compliance professionals, or regulatory advisors.

Regulatory Change: AML regulations, supervisory expectations, and examination standards evolve continuously. Organizations are responsible for monitoring regulatory developments and updating their programs accordingly.

No Guarantee of Compliance: Use of this checklist does not guarantee regulatory compliance, examination readiness, or satisfactory regulatory outcomes. Regulators evaluate programs based on individual facts and circumstances.

Recommended Actions: Organizations should consult with qualified legal counsel, compliance experts, and regulatory advisors to develop and maintain AML and model risk management programs tailored to their specific needs and risk profile. By using this checklist, you acknowledge that the provider of this checklist assumes no liability for any reliance placed on this information or for any consequences arising from its use or implementation.