**Azure Fraud Model Monitoring Plan**

*(For Model Risk Management Submission)*

**1. Executive Summary**

The Azure Fraud Protection model is a real-time, cloud-based fraud detection solution leveraging adaptive machine learning. This monitoring framework is designed to assess the model's predictive performance, stability, operational efficiency, and governance compliance under SR 11-7 principles and internal risk management standards.

**2. Scope of Monitoring**

* Transaction-level fraud detection scoring
* Decision outputs: Approve, Reject, Review
* Feedback loop monitoring (actual disposition vs prediction)
* Auto-update behavior monitoring (adaptive model learning)

**3. Core Outputs Monitored**

* **Risk Score** (continuous 0–999 or normalized 0–1 scale)
* **Decision Recommendation** (Approve / Review / Reject)
* **Reason Codes** (Top factors impacting fraud prediction)
* **Actual Disposition** (Confirmed Fraud / Legitimate Outcome)
* **Latency Time** (Model response time)
* **Model Version / Update Tracking** (where available)

**4. Data and Variables Required**

|  |  |  |
| --- | --- | --- |
| **Variable** | **Usage in Monitoring** | **Business Significance** |
| **Transaction ID** | Unique traceable event key | Auditability, reconciliation |
| **Timestamp** | Event timing | Trend and latency analysis |
| **Risk Score** | Main predictor for ROC, PSI | Probability of fraud assigned |
| **Predicted Decision** | Decision band for operational use | Flow into business acceptance/rejection workflows |
| **Actual Disposition** | Ground truth for confusion matrix | Performance evaluation |
| **Reason Codes** | Explainability | Monitor fraud typology shifts |
| **Latency (Milliseconds)** | Real-time performance | SLA and customer experience |
| **Feedback Loop Status** | Track whether actual outcomes are reported back to Azure | Ensures adaptive learning remains effective |

**5. Key Monitoring Metrics and Formulas**

**5.1 Confusion Matrix Metrics**

|  |  |  |
| --- | --- | --- |
| **Metric** | **Formula** | **Interpretation** |
| **Precision** | TP / (TP + FP) | Proportion of flagged frauds that are actually frauds |
| **Recall (Capture Rate)** | TP / (TP + FN) | Proportion of frauds caught by the model |
| **Accuracy** | (TP + TN) / Total | Overall correctness |
| **False Positive Rate (FPR)** | FP / (FP + TN) | Customer impact metric |

**5.2 AUC-ROC Curve Monitoring**

* Plot TPR vs FPR at various score thresholds
* **Area under the ROC Curve (AUC)** > **0.80** considered acceptable.
* Measures the model’s ability to distinguish fraud from legitimate transactions.

**5.3 Population Stability Index (PSI) for Score Stability**

* Formula:

PSI=∑(Actual%−Expected%)×ln⁡(Actual%Expected%)PSI = \sum (Actual\% - Expected\%) \times \ln\left(\frac{Actual\%}{Expected\%}\right)

* Interpretation:
  + PSI < 0.10: Stable
  + 0.10–0.25: Monitor
  + PSI > 0.25: Investigate drift

**5.4 Threshold Effectiveness**

* Track the monthly percentage of transactions in Approve, Review, Reject bands.
* Detect shifts in transaction distribution across thresholds.
* Helps assess whether decision thresholds remain effective or need recalibration.

**6. Monitoring Frequency**

|  |  |
| --- | --- |
| **Metric Type** | **Frequency** |
| Confusion Matrix Metrics (Precision, Recall, FPR, Accuracy) | Monthly |
| AUC-ROC Curve | Monthly |
| PSI (Risk Score Stability) | Quarterly |
| Threshold Monitoring | Monthly |
| Latency Monitoring | Monthly |

**7. Governance and Escalation**

|  |  |
| --- | --- |
| **Condition** | **Action** |
| AUC < 0.75 | Immediate escalation to MRM and Model Owner |
| PSI > 0.25 | Drift analysis and threshold review |
| False Positive Rate >5% increase | Root cause analysis |
| Feedback Loop Completion <95% | Risk to model adaptiveness — notify Business and Vendor |
| Latency > SLA for 2 consecutive months | Engage Technology Risk Team |

**8. Special Monitoring Considerations for Azure Models**

* **Auto-Updates:** Monitor model performance after Azure backend updates even if update is silent.
* **Reason Code Trend Analysis:** Monthly tracking of top drivers of fraud prediction to detect typology shifts.
* **Feedback Loop:** Ensure timely fraud outcome feedback is maintained, as it directly impacts model retraining quality.

**Conclusion**

This monitoring framework ensures that the Azure Fraud Protection model maintains robust fraud detection capabilities while minimizing customer friction. It supports early detection of performance degradation, drift, or operational issues, ensuring strong model governance and regulatory compliance.