**Performance Monitoring Plan (PMP) for the LexisNexis Fraud Intelligence Model**

**1. Introduction**

This document has been structured to address the Model Risk Management (MRM) finding regarding ongoing performance monitoring (OPM) requirements for the LexisNexis Fraud Intelligence Model. The plan ensures that the model continues to effectively detect fraudulent activities while remaining stable, accurate, and compliant with regulatory requirements.

**2. Key Performance Metrics**

The model's performance is assessed using the following key indicators:

**2.1 Discriminatory Power**

* **Area Under the Curve (AUC)** – Measures the model’s ability to distinguish between fraudulent and legitimate transactions.

**2.2 Model Stability**

* **Population Stability Index (PSI)** – Detects shifts in input feature distributions over time.

**2.3 Fraud Detection Performance**

* **True Positive Rate (TPR)** – Percentage of non-fraud transactions incorrectly flagged as fraud.
* **False Positive Rate (FPR)** – Percentage of non-fraud transactions incorrectly flagged as fraud.
* **Fraud Detection Rate (FDR)** – Proportion of flagged transactions that are confirmed as fraud.

**3. Performance Metric Thresholds & Breach Management**

The model's performance is monitored against predefined thresholds categorized as follows:

|  |  |  |  |
| --- | --- | --- | --- |
| **Metrics Category** | **Green (Optimal)** | **Yellow (Warning)** | **Red (Critical – Action Required)** |
| AUC | >0.85 | 0.75 - 0.85 | <0.75 |
| PSI | <0.1 | 0.1 - 0.25 | >0.25 |
| True Positive Rate | >90% | 90% - 80% | <80% |
| False Positive Rate | <5% | 5% - 10% | >10% |
| Fraud Detection Rate | >80% | 60% - 80% | <60% |

**Threshold Breach Management Action Plan**

* **Green (Optimal):** No immediate action required; continue monitoring.
* **Yellow (Warning):** Conduct a diagnostic review; determine potential reasons for performance decline.
* **Red (Critical - Action Required):** Trigger immediate remediation, which may include model recalibration, retraining, or adjusting risk score thresholds.

**1. AUC Improvement:**

* **Feature Engineering**: Add relevant features, remove irrelevant ones, and create interaction terms.
* **Model Selection**: Experiment with algorithms like XGBoost, Random Forest, or Neural Networks.
* **Hyperparameter Tuning**: Use grid search or random search to find optimal settings.
* **Cross-validation**: Use K-fold cross-validation for better model generalization.
* **Ensemble Methods**: Combine multiple models to improve performance.
* **Data Quality**: Ensure data is clean, without missing values or outliers.
* **Increase Data**: More data can help improve model performance.

**2. PSI Improvement:**

* **Check for Data Drift**: Assess changes in feature distribution between training and current data.
* **Retrain the Model**: Use updated data to retrain the model regularly to prevent drift.
* **Review Sampling Techniques**: Adjust for class imbalance using resampling methods like SMOTE.
* **Monitor Inputs & Outputs**: Adjust features or output thresholds if necessary.
* **Model Calibration**: Recalibrate model outputs to better align with current data.
* **Continuous Monitoring**: Set up alerts and regularly monitor PSI to detect drift early.

**3. FDR Improvement:**

* **Enhance Feature Engineering**: Add new features and interaction terms specific to fraud detection.
* **Handle Class Imbalance**: Use oversampling, undersampling, or adjust class weights to focus on detecting fraud.
* **Model Selection**: Try models like XGBoost, Random Forest, or SVM, known for handling imbalanced data.
* **Hyperparameter Tuning**: Optimize model parameters to increase detection sensitivity.
* **Use Ensemble Methods**: Combine models using boosting or voting classifiers to enhance fraud detection.
* **Improve Data Quality**: Clean the data, handle outliers, and normalize features.
* **Increase Training Data**: Gather more fraud cases or generate synthetic data to improve detection.
* **Adjust Model Threshold**: Fine-tune thresholds to increase detection of fraud cases.
* **Post-processing**: Add rule-based checks to catch missed fraud cases.
* **Continuous Monitoring**: Regularly update the model with new data to prevent drift and keep detection rates high.

**4. Monitoring Frequency**

|  |  |
| --- | --- |
| **Monitoring Task** | **Frequency** |
| Real-time fraud detection monitoring | Continuous |
| Performance metrics calculation | Monthly |
| Model stability checks (PSI) | Quarterly |
| Backtesting against historical fraud cases | Semi-annually |
| Annual Model Validation | Annually or as needed |
| Ad-hoc Monitoring (as per vendor guidance) | Weekly and Monthly |

**5. Annual Model Validation**

Annual model validation is considered a best practice for several reasons:

**5.1 Regulatory Expectations**

* Regulations such as SR 11-7 (Federal Reserve) and OCC 2011-12 emphasize ongoing performance monitoring and periodic validation.
* Annual validation ensures the model adapts to shifting fraud risks, customer behaviors, and market conditions.

**5.2 Risk Management & Governance Requirements**

* Financial institutions follow risk-based governance policies that require periodic reviews.
* High-risk fraud models are typically assessed annually to align with best practices in Model Risk Management (MRM).

**5.3 Industry Standards and Vendor Recommendations**

* Vendors like LexisNexis, FICO, and SAS recommend annual validations as standard practice.
* This aligns with Basel II/III risk management principles and best industry practices.

**6. Data Quality Monitoring**

* **Basic Statistical Checks:** Regular evaluation of mean, standard deviation, minimum and maximum ranges, percentiles, and ratios.
* **Kolmogorov-Smirnov (K-S) Test:** A two-sample statistical test to measure distribution shifts.

**7. Corrective Actions**

If performance issues arise, the following actions may be taken:

* **Threshold Adjustment:** Modify risk score cutoffs to optimize fraud detection.
* **Feature Engineering Updates:** Introduce new transaction patterns or behavioral indicators.
* **Recalibration or Model Retraining:** Use fresh fraud cases and legitimate transactions to retrain the model.
* **Alternative Model Evaluation:** Compare with rule-based fraud detection or competitor models.