**Performance Monitoring Plan (PMP) for Azure Fraud Rules Model**

**Overview**

Azure Fraud Rules is an in-house built fraud rules engine designed for digital banking. It uses a rule-based approach (non-AI/ML) to classify transaction statuses into the following categories:

* **Green**: Safe transactions.
* **Yellow**: Transactions requiring additional review.
* **Red Pending**: Transactions pending resolution.
* **Red**: High-risk transactions flagged as fraudulent.

This document outlines the performance monitoring framework, including metrics, thresholds, frequency, and escalation plans.

**Performance Monitoring Framework**

|  |  |
| --- | --- |
| **Aspect** | **Details** |
| **Frequency of Monitoring** | Monthly. |
| **Team Responsible** | Fraud Strategy Team in collaboration with Enterprise Risk Management (ERM). |
| **Stakeholders** | Senior Management, Risk, and Operations Teams. |

**Performance Metrics and Thresholds**

|  |  |  |  |
| --- | --- | --- | --- |
| **Metric** | **Definition** | **Thresholds** | **Escalation Plan** |
| **True Positives (TP)** | Number of correctly flagged fraudulent transactions. | ≥ 95% (Green) | **Amber (90-94%):** Review rules. **Red (<90%):** Immediate escalation to senior management. |
| **False Positives (FP)** | Number of legitimate transactions incorrectly flagged as fraudulent. | ≤ 5% (Green) | **Amber (5-10%):** Review and adjust thresholds. **Red (>10%):** Full model audit. |
| **True Positive Rate (TPR)** | Proportion of actual fraud cases detected (sensitivity). | ≥ 90% (Green) | **Amber (85-89%):** Investigate rule gaps. **Red (<85%):** Immediate rule reconfiguration. |
| **False Positive Rate (FPR)** | Proportion of non-fraud cases incorrectly flagged. | ≤ 5% (Green) | **Amber (5-10%):** Adjust rule specificity. **Red (>10%):** Immediate senior review. |
| **Precision** | Proportion of flagged transactions that are truly fraudulent. | ≥ 85% (Green) | **Amber (80-84%):** Evaluate misclassifications. **Red (<80%):** Comprehensive rule review. |
| **Hit Rate** | Percentage of flagged transactions reviewed and resolved successfully. | ≥ 90% (Green) | **Amber (85-89%):** Investigate workflow issues. **Red (<85%):** Process escalation. |

These threshold for respective metrics ensures effective fraud detection, minimizes financial loss, and maintains regulatory compliance while aligning with industry standards. By reducing operational costs and customer friction, it follows best practices from fraud detection vendors like FICO and SAS. It maintains fraud detection efficiency and avoids unnecessary alerts by adhering to industry benchmarks for rule-based fraud systems. Accurate flagged transactions reduce unnecessary investigations and enhance efficiency. The strategy maximizes fraud coverage, ensures compliance, and maintains high detection rates, balancing detection efficiency with operational resources to optimize fraud prevention.

**Regulatory Guidance**:

* **OCC Bulletin 2011-12**: Recommends setting performance thresholds to ensure fraud detection models meet operational and regulatory needs.
* **Basel Committee’s Principles**: Highlights the importance of monitoring performance metrics to ensure risk mitigation.

**Escalation Matrix**

|  |  |  |  |
| --- | --- | --- | --- |
| **Severity** | **Description** | **Action Plan** | **Responsible Parties** |
| **Green** | Metrics within thresholds. | Continue standard monitoring and reporting. | Fraud Strategy Team. |
| **Amber** | Metrics approaching thresholds; potential risk identified. | Conduct a detailed review of flagged metrics. Implement minor rule adjustments if required. | Fraud Strategy Team in collaboration with ERM. |
| **Red** | Metrics outside acceptable thresholds; critical performance issue. | Escalate immediately to senior management. Conduct a full review and reconfiguration of affected rules. | Fraud Strategy Team, ERM, Senior Management. |

**Monitoring Activities**

|  |  |  |  |
| --- | --- | --- | --- |
| **Activity** | **Frequency** | **Responsible Team** | **Key Deliverables** |
| Generate monthly performance reports. | Monthly | Fraud Strategy Team, ERM | Performance report detailing TP, FP, TPR, FPR, precision, and hit rate. |
| Review flagged metrics. | Monthly | Fraud Strategy Team | Identification of trends or anomalies in performance metrics. |
| Escalate issues outside thresholds. | As needed | Fraud Strategy Team, ERM, Senior Management | Corrective actions and model updates. |
| Update rules based on findings. | Quarterly | Fraud Strategy Team | Adjustments to rules and thresholds to optimize performance. |

**Documentation and Reporting**

* **Monthly Reports**: Include detailed analysis of all performance metrics and comparisons with thresholds.
* **Escalation Reports**: Prepared when metrics exceed defined thresholds, including root cause analysis and recommended actions.
* **Audit Trails**: Maintain logs of all rule adjustments and performance evaluation activities for accountability.

This PMP ensures a robust industry-leading framework for performance monitoring for fraud detection models, such as Azure, aligns with **global fraud risk management standards** to ensure optimal fraud detection while minimizing false positives, reinforcing the model’s reliability and adaptability in detecting fraudulent activities. Continuous evaluation of key performance metrics—such as True Positives (TP), False Positives (FP), Precision, Recall, False Positive Rate (FPR), and Hit Rate—enables organizations to proactively adjust rules, ensuring they remain effective against evolving fraud patterns.