**Y:\BSA_OFFICE_SECURED\Policy and Procedures\Templates\Logo\Screen - EWB English Logo - small.png**

**OASIS Check Fraud**

**Risk & Operations**

**August/2024**

**Model Documentation Change Log**

|  |  |  |  |
| --- | --- | --- | --- |
| **Author** | **Reviewer** | **Date** | **Details of the Changes** |
| Crowe |  | 4/12/2024 | Draft report delivered to East West Bank |
| Crowe |  | 5/1/2024 | Incorporate feedback provided by East West Bank |
| Crowe |  | 6/17/2024 | Incorporate feedback provided by East West Bank |
| EWB |  | 8/28/2024 | Incorporate input provided by Crowe on final deliverable |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Table of Contents

[1. EXECUTIVE SUMMARY 5](#_Toc175840156)

[1.1 Objective and Background 5](#_Toc175840158)

[1.2 Model Purpose & Use 7](#_Toc175840159)

[1.2.1 Model Purpose 7](#_Toc175840163)

[1.2.2 Portfolio/Product/Transactions Overview 8](#_Toc175840164)

[1.2.3 Applicable Policies and Regulations 9](#_Toc175840165)

[1.2.4 Existing Models 9](#_Toc175840166)

[1.2.5 Upstream/Downstream Model Dependencies 9](#_Toc175840167)

[1.2.6 Process Flow Diagram 10](#_Toc175840168)

[1.3 Model Key Stakeholders, Change Management, & Outstanding Issues 13](#_Toc175840169)

[2. INPUT DATA INTEGRITY & APPROPRIATENESS 16](#_Toc175840170)

[2.1 MODEL DEVELOPMENT DATA 16](#_Toc175840171)

[2.1.1 Overview of Model Development Data 17](#_Toc175840172)

[2.1.2 Development Data Sources, Extraction Process, and Reconciliation 18](#_Toc175840173)

[2.1.3 Development Data Preparation 22](#_Toc175840178)

[2.1.4 Data Limitations 24](#_Toc175840180)

[2.1.5 Data Preparation Software / Platform 25](#_Toc175840181)

[2.1.6 Data Retention 25](#_Toc175840182)

[3. CONCEPTUAL SOUNDNESS 26](#_Toc175840183)

[3.1 MODEL THEORY AND ASSUMPTIONS 26](#_Toc175840184)

[3.1.1 Model Theory and Methodology 27](#_Toc175840185)

[3.1.2 Segmentation Approach 34](#_Toc175840186)

[3.1.3 Model Settings 34](#_Toc175840187)

[3.1.4 Model Assumptions 35](#_Toc175840188)

[3.1.5 Model Limitations and Weaknesses 36](#_Toc175840189)

[3.2 MODEL ESTIMATION / TRAINING AND SELECTION 37](#_Toc175840190)

[3.2.1 Estimation Methodology and Assumptions 37](#_Toc175840191)

[3.2.2 Modeling Software / Platform 37](#_Toc175840192)

[3.2.3 Hyper-parameter Tuning 38](#_Toc175840193)

[3.2.4 Feature / Variable Selection 38](#_Toc175840194)

[3.2.5 Model Estimation / Training Results 39](#_Toc175840195)

[3.2.6 Other Types of Model Estimation 40](#_Toc175840196)

[3.3 Model Development Testing 41](#_Toc175840197)

[3.3.1 Statistical and Technical Assumptions Testing 41](#_Toc175840198)

[3.3.2 Model Performance / Fit Testing 42](#_Toc175840199)

[3.3.3 Model Stability and Overfitting Testing 43](#_Toc175840206)

[3.3.4 Back-testing 44](#_Toc175840207)

[3.3.5 Model Explainability Testing 45](#_Toc175840208)

[3.3.6 Benchmarking 46](#_Toc175840209)

[3.3.7 Sensitivity Analysis 46](#_Toc175840210)

[3.3.8 Stress Testing / Scenario Analysis 47](#_Toc175840211)

[3.3.9 Other Testing 47](#_Toc175840212)

[3.3.10 Overall Performance Assessment 47](#_Toc175840213)

[3.3.11 Need for Model Overlays 48](#_Toc175840214)

[4. PRODUCTION PROCESS COMPLETENESS & ACCURACY 49](#_Toc175840215)

[4.1 Production Application Testing 49](#_Toc175840217)

[4.1.1 System Testing Approach and Results 50](#_Toc175840218)

[4.1.2 User Acceptance Testing Approach and Results 50](#_Toc175840219)

[4.2 Model Production Specifications 51](#_Toc175840220)

[4.2.1 Model Platform 51](#_Toc175840221)

[4.2.2 Data and Process Flow Diagram 51](#_Toc175840222)

[4.2.3 Input Data Specifications 55](#_Toc175840223)

[4.2.4 Model Formulas / Algorithms 57](#_Toc175840224)

[4.2.5 Model Parameters and Settings Values 57](#_Toc175840225)

[4.2.6 Model Outputs 57](#_Toc175840226)

[4.2.7 Reports 58](#_Toc175840227)

[4.3 Operational Controls 59](#_Toc175840228)

[4.3.1 Model Access and Security 59](#_Toc175840229)

[4.3.2 Production Deployment 60](#_Toc175840230)

[4.3.3 Model Usage Controls 61](#_Toc175840231)

[4.3.4 Model Backup 61](#_Toc175840232)

[4.4 Contingency Plans 62](#_Toc175840233)

[4.4.1 Disaster Recovery Plan 62](#_Toc175840234)

[4.4.2 Business Continuity Plan 63](#_Toc175840235)

[4.5 Operating Procedures / User’s Guide 64](#_Toc175840236)

[5. ONGOING MODEL GOVERNANCE & OUTCOME ANALYSIS 65](#_Toc175840237)

[5.1 Ongoing Risk & Performance Monitoring Plan 65](#_Toc175840238)

[5.2 Model Approval and Change Management Process 69](#_Toc175840239)

[5.2.1 Model Approval Process 69](#_Toc175840240)

[5.2.2 Model Change Log 70](#_Toc175840241)

[6. APPENDICES 71](#_Toc175840242)

[6.1 Appendix A 71](#_Toc175840243)

[6.2 Appendix B 71](#_Toc175840244)

# EXECUTIVE SUMMARY



## Objective and Background

Please provide a high-level description of:

* The model’s business objectives.
* Business background including history where appropriate.
* Related regulatory requirements that relate to the business objectives.
* Any other information you see appropriate.

Model Owner:

Check fraud occurs in a variety of ways including counterfeiting, forgery, and theft. Increased check fraud may expose the bank to heightened deposit fraud risks. The Bank has implemented a check fraud detection solution to minimize monetary loss and maintain trust among customers.

The Bank implemented Argo Optimized Assessment of Suspicious ItemS (OASIS) system in 2007 to monitor on-us check fraudulent activity. Within the OASIS system, the Bank can create customized queues to filter for suspicious level activity based on the transactional and image analysis scores.

The Bank’s business objective of implementing the OASIS fraud check model includes establishing a framework for continual improvement to address evolving threats. This involves regular monitoring of model performance, incorporating feedback from stakeholders, and staying in touch with emerging technologies and industry trends to enhance the effectiveness of check fraud detection efforts.

Additionally, the OASIS check fraud model ensures compliance with the Uniform Commercial Code (UCC) which governs the rights and liabilities of parties involved in check transactions, including provisions related to unauthorized signatures and alteration. The OASIS check fraud model adheres to Regulation CC requirements related to check processing and availability of funds, ensuring compliance with check payment regulations issued by the Federal Reserve.

|  |  |
| --- | --- |
| **Model Name** | * *Please provide the official model-name that is used by the model owners and the MRM Group (mutually agreed).*   Model Owner: Argo OASIS (Model ID:033) |
| **Primary Model Owner Entity** | * *Please provide the model owner business entity name, e.g., US, China, or Hong Kong.*   Model Owner: US |
| **Primary Model Owner Group** | * *Please provide the model owner business group name.*   Model Owner: Enterprise Risk Management |
| **Model Owner** | * *Please provide the model owner names.*   Model Owner: FVP - ERM Data Manager |
| **Model Developer** | * *Please provide the model developer names (vendor name if vendor model).*   Model Owner: Argo (<http://argodata.com/)> |
| **Model Production Process** | * *Please provide the model production process environment. A high-level description is encouraged.*   Model Owner:  The model applies fraud transaction analysis and image analysis for each on-us check and computes a score, between -100 and zero (0), for each test, based on level of risk. A more negative score indicates the model assessed a higher degree of failure and a higher probability of a fraud suspect item. Alerts are generated via work queue creation and prioritization for check transactions that meet a set of conditions, for each individual test score, preconfigured by the bank. |
| **Model User** | * *Please provide all model usernames along with business group names.*   Model Owner: Risk & Operations |
| **Portfolios the Model Applies to** | * *Please provide high level portfolio size and description that the model is applied to.*   Model Owner:  • Account types: All depository accounts.  • Exclusions: An on-us check cashed at the bank, accounts that have Positive Pay process, and cashier’s checks. |
| **Model Objective** | * *Please list all model objectives at a high level.*   Model Owner:  The OASIS solution analyzes on-us check transactions based on active Transaction Analysis (TA) and Image Analysis (IA) within the OASIS environment. Negative OASIS test score on item indicates a possible suspect item. Suspect items presented in a queue is flagged for review by deposit fraud analysts. |

## Model Purpose & Use



### Model Purpose

For each business purpose, discuss the following in detail:

* The overall business purposes.
* The specific role that the model output plays in business use (for example, if the model output is used as a secondary source of information in the decision-making process, this should be detailed here).
* The specific products/portfolios/customers/transactions for which the model is suitable (e.g., types of retail mortgages, types of derivatives, types of consumer transactions, etc.)
* Any restrictions on model use, for example, excluded product types within product categories or transaction size limits.

Model Owner:

The objective of the ARGO OASIS model is to monitor for fraudulent activity in check transactions. OASIS is a vendor solution provided by ARGO. Per the vendor model documentation, OASIS “provides cross-channel, multi-fund analytics and adjudication workflow to detect fraudulent transactions and suspicious items. OASIS starts prevention at the point of disbursement with automated verification and fraud detection at all points in the clearing process.”

While OASIS is functionally designed to create and maintain behavioral profiles for each of the financial institution’s customers and apply predictive machine learning techniques to detect unusual behavior in check transactions, the Bank has not implemented the machine learning functionality. The Bank is using the OASIS feature calculations tests of Transaction Analysis (TA) and Image Analysis (IA) check image comparisons to analyze daily imported on-us check data.

OASIS is used by the Bank to monitor on-us check fraud for all depository accounts. On-us checks cashed out, accounts that have Positive Pay process, and cashier’s checks are not monitored for check fraud.

The OASIS coverage assessment can be found within **“EWB Fraud Coverage Assessment FINAL.xlsx.”**

For additional information on the model, please see **“OASIS-2-5-Release-Notes.pdf.”**

The ARGO OASIS check model is subject to all requirements detailed within the Bank’s Model Risk Management policy. Please see **“MRM-PnP01 EWBC MRM Policy v12.5.pdf”** for additional details.

### Portfolio/Product/Transactions Overview

* Provide the current size of the portfolio of assets or liabilities (if applicable) and describe the history of the portfolio characteristics (e.g., the inception time frame, any notable idiosyncratic events such as mergers/acquisitions or asset sales, any notable management strategic changes, etc.)
* If the model is being applied to analyze transactions or events (e.g., debit card transactions analyzed for money laundering risk, or cyber-attacks on the Company’s infrastructure), provide the historical volumes of transactions and trends.
* Describe any specific product/customer/transaction types that are being proxied by other product types (e.g., a new product for which the model developed on a more seasoned product is applied).
* When applicable, please describe which portion of the portfolios/transactions/products that is supposed to be covered by the model (for the same business objective) but is decided to be excluded. For such portion, what business strategies are applied to ensure the same business objective is met (e.g., for BSA/AML purpose, certain transactions are monitored manually instead of using the BSA/AML model).

Model Owner:

Products being monitoring by the model include all check activity processed for all depository accounts. On-us check cashed out, accounts that have Positive Pay process, and cashier’s checks are excluded from monitoring through OASIS at this time.

The Bank does not currently have any specific product/customer/transaction types that are being proxied by other product types.

Total portfolio assets of 12/31/2023 are $31.86 billion.

### Applicable Policies and Regulations

* List and discuss all regulatory, accounting, legal, and/or compliance rules that are relevant to the model data, design, or use (if any).
* List and discuss all applicable internal policies relevant to the model design and use, if any.

*Note: Please provide document name including suffix.*

Model Owner:

The Uniform Commercial Code (UCC) body of law framework contains provisions that address aspects of check fraud, including unauthorized signatures and alteration.

UCC Section 3-403 Unauthorized Signature provides guidelines for determining whether a signature is authorized and imposes a liability on parties who fail to exercise reasonable care in preventing unauthorized signatures.

UCC Section 3-407 Alteration imposes a liability on the party who altered the instrument or benefited from the alteration if it results in a loss to another party.

Regulation CC, also referred to as the Expedited Funds Availability Act (EFA), sets specific requirements and timelines for financial institutions to make deposited funds available to customers. This regulation also states financial institutions must provide safeguard exceptions to delay the availability of funds to reduce fraud risk.

Relevant regulatory considerations to the model include but are not limited to Supervisory Guidance on Model Risk Management (SR 11-7: Guidance on Model Risk Management), issued by the Federal Reserve and Office of the Comptroller of the Currency (OCC) on April 4, 2011, and the Bank’s internal **“MRM-PnP01 EWBC MRM Policy v12.5.pdf.”**

### Existing Models

* If this model is replacing existing model(s), provide details of the existing model(s) and the rationale for the replacement.
* Discuss whether the existing model(s) will be retired once this model goes into production.

Model Owner:

Not applicable. Model has been in production since 2007.

### Upstream/Downstream Model Dependencies

* Provide a listing and description of upstream and/or downstream models or other key systems (e.g., the Empyrean ALM model).
* Discuss the impact of known limitations of upstream models on this model.

Model Owner:

Not applicable, the model does not impact, and is not impacted by, other upstream or downstream models.

### Process Flow Diagram

* Provide a process flow diagram showing how the model is used by the functional / business area. Include upstream and downstream models and systems listed in Section 1.2.5 Upstream/Downstream Model Dependencies.

Model Owner:

The following Model Users considered as Model Business Owners have the ability and authority to make changes to the OASIS Check Fraud Verification document:

1. SVP Risk & Operations Manager

2. SVP – Director of Retail and Digital Banking Operations

Risk & Operations management employees provide oversight and ensure enforcement of procedures with the Risk & Operations team.

1. **Process to onboard Bank fraud analysts.**

The onboarding process for Bank employees includes side-by-side training. The Bank employee sits with and learns from a seasoned Bank analyst experienced in the OASIS alert review process.

1. **Generating the alert review queue in OASIS**

Predictive tests determine fraud suspicion for each transaction. These analytics tests’ global test parameters allow test scores and scope data to be adjusted. Test results range from -100 to zero (0), and result in one (1) of three (3) determinations:

1. Test Passed – returned with a positive ten (+10) considered a good transaction.
2. Test Bypassed – returned with zero (0) value that the test was performed.
3. Test Failed – returned negative values between (-100) and zero (0) indicate degree of failure on the individual tests.

A test may not be performed under the following circumstances:

* If the amount of the transaction is below the configured caps minimum amount $500.If the test is not activated by the bank.

Items resulting in a ‘Test Failed’ are selected for review by a Bank employee. For more information about predictive testing and scores, please refer to 6.01.2 OASIS Analytics Tests and Understanding OASIS Analytics Test Results in ***“*Output Review - OASIS Check Fraud Verification.pdf*.”***

1. **Process to access the alert review queue in OASIS.**

Bank employees access OASIS by entering a username, password, and realm. The User Access Request (UAR) is an internal application tool used by Bank employees to submit access requests such as physical building, network, and application. The UAR tool routes a Bank employee’s request to obtain the required approvals. The Bank user administration group provisions the user access and will grant the Bank employee access to OASIS. For information about login problems and employee support (<UserAdministration@eastwestbank.com>), please refer to 6.01.1 Sign into OASIS in **“Output Review - OASIS Check Fraud Verification.pdf.”**

Once signed into OASIS, employees are instructed to navigate to ‘Suspect Analysis’ and select a report. An employee can access their predefined queue by expanding ‘Queue Definitions’ and clicking ‘Choose Queue.’ Before reviewing items in the queue, Bank employees must check the ‘To’ and ‘From’ transaction dates to verify the work of day is correct. Then, employees can click ‘Scrub’ to review items in the queue.

For further details on OASIS alert review queues, please refer to 6.01.4 Selecting Queues and Scrubbing in **“Output Review - OASIS Check Fraud Verification.pdf.”**

1. **Process to perform a check fraud verification alert review in OASIS.**

Employees are instructed to pay close attention to specific characteristics including handwritten checks, computer generated digital image of check also known as substitute checks, check stocks or alterations. For a full list of characteristics to pay close attention to when reviewing an item, please refer to 6.02.1 Characteristics of a Suspicious/Fraudulent Item in **“Output Review -** **OASIS Check Fraud Verification.pdf.”**

Items with a predictive test result ‘Test Failed’ are selected for further review by a Bank employee. Bank employees follow instructions based on the test result and type of review item. For example, ‘Duplicate Check Number’ requires validating the check number against previous check history, and if the history is unavailable in OASIS, the employee must access IBS Insight and/or FIS Workstation/Vision Archive for the review. For instructions for all review items, please refer to 6.02.2 Item Review Process in **“Output Review - OASIS Check Fraud Verification.pdf.”**

If the Bank employee determines the alerted item is valid, the employee documents rationale and dispositions the item as ‘Accept.’ If the Bank employee is unable to determine if the alerted item is valid, the item must be further reviewed as a suspicious item in OASIS.

To review a potentially fraudulent item in OASIS, the Bank employee must refer the item via email to the domiciling branch, account officer or relationship manager for verification with the customer. For the escalation email, reminder email, and final email templates used by the R&O team when contacting the domiciling branch, please refer to 6.04 Exhibits – Email Notifications in **“Output Review - OASIS Check Fraud Verification.pdf.”** The domiciling branch, account officer or relationship manager will call the customer to verify identity, ask whether the customer issued the check, and validate the payee and dollar amount. Until a response is received from the domiciling branch, the Bank employee dispositions the item as ‘Defer.’ If no response is received from the domiciling branch by 3:00 pm PST the same business day, the Bank employee designates the item as ‘Refer to Maker (RTM)’ and no other actions are required by the Bank employee once the item is returned. The Deposit fraud team provides a return log to Exceptions, who process all the return items.

The domiciling branch is still responsible for restricting the account, adding a remark, and contacting the customer for validation of the item. The table below depicts the four (4) courses of action taken by a Bank employee based on the determination made by a domiciling branch after attempting to verify an item with the customer:

|  |  |  |
| --- | --- | --- |
| Check/item determination (by domiciling branch) | Disposition (by Bank employee) | Actions taken (by Bank employee) |
| Fraudulent | Reject | Add the item details to the Return Items Transmissions Worksheet. |
| Domiciling branch is unable to reach the customer to verify the check/item before the deadline | Disposition the item appropriately. | Reply to the branch requesting continued efforts to verify the check/item with the client.  Add the item details to the Return Items Transmission Worksheet. |
| Fraudulent (due to negotiability standards) or validation with customer is questionable | Disposition the item appropriately. | Refer the item to a member or designee of R&O management for review. |
| Fraudulent (activity detected such as kiting or NSF check writing) | Disposition the item appropriately. | Refer the account via email to [<FraudInvestigations@EastWestBank.com](mailto:%3cFraudInvestigations@EastWestBank.com)> and include R&O management on the email. |

The OASIS system maintains documentation on each alert. For detailed instructions concerning reviewing suspicious items in OASIS, please refer to 6.02.2 Item Review Process in **“Output Review - OASIS Check Fraud Verification.pdf.”**

1. **Return Items Transmission Worksheet**

The Return Items Transmission Worksheet is an excel spreadsheet that is updated daily, and logs items returned by the Exceptions Processing Team. Item data includes account number, dollar amount, check number, return reason, and microfilm number (also known as the control number on IBS Insight).

At the end of each day, a Bank employee sends the log via email to <Exceptions@EastWestBank.com>. For more information about the Return Items Transmission Worksheet, please refer to 6.02.3 Return Items Transmission Worksheet in **“Output Review - OASIS Check Fraud Verification.pdf.”**

1. **Process to file a Possible Suspicious Activity Report (PSAR)**

When appropriate, the Deposit fraud team will file a Possible Suspicious Activity Report (PSAR). This PSAR then goes to the BSA group who is responsible for timely filing a Suspicious Activity Report (SAR).

1. **Supporting Documentation**

For each item reviewed, a Bank employee will save all emails containing pay or return decisions to the applicable shared folder on the Risk & Operations share drive.

1. **Internal Controls and Management Review**

Bank employees are expected to review their own work. At the end of each business day, Bank R&O management performs a secondary review of all items reviewed by an analyst in OASIS that is above or equal to $250,000.00.

For information about internal controls over the check fraud verification alert review process, please refer to 6.03.1 Secondary (Management) Review in **“Output Review - OASIS Check Fraud Verification.pdf.”**

1. **OASIS End of Day Process**

At 6:00 pm PST, OASIS runs end of day processes to auto close any alerts that have not been decisioned. This ensures all items are dispositioned before the OASIS End of Day processing.

1. **Process to revoke access to OASIS.**

If user access to OASIS needs to be revoked, the Bank’s User Administration Group is responsible for provisioning and notified by HR to revoke user access.

## Model Key Stakeholders, Change Management, & Outstanding Issues

Describe, at minimum, the following:

1. Model output key stakeholders, review committee(s).
2. High level summary of model changes in recent time or since last model validation.
3. High level summary of the latest model related business area audit and regulatory exam results including any outstanding findings, regulatory Matter Requiring Attention (MRAs), and management self-identified issues.

Please ensure that **all of** the points mentioned above are addressed.

Model Owner:

1. The key roles and responsibilities as they pertain to the ARGO Oasis model are as follows:

**Model Owner**

* Enterprise Risk Management (ERM): Lead and coordinate with Risk and Operations (Model User) to implement framework, include performance monitoring and reporting and corrective measures based on MRM findings.

**Model User (Model Business Owner)**

* Senior Management of Risk and Operations (R&O): Responsible for granting approval of UAT results and any changes to filtering logic used in the model. Senior Management of R&O consists of two members: the Senior Director of Retail & Digital Banking Operations and the Deputy Director of Centralized Operations. Both members are involved in the approval process; however, the Senior Director of Retail & Digital Banking Operations must provide the final approval.

**Model Support User (Fraud Strategy Team)**

* Fraud Strategy team: Support both the model owner and model user (model business owner) in modifying and creating new queues, creating monthly reports for monitoring performance, communicating changes that impact model performance (i.e., modification and creation of queues) to the model, and engaging OASIS customer support via email for inquiries on item scoring or general product questions. The Fraud Strategy team consists of two members: the Digital Fraud Risk Strategy Development Manager and the Senior Fraud Strategist.

**Model Developer (Vendor)**

* ARGO: Responsible for providing software enhancements, aiding in implementing system upgrades, and providing support via email when requested by the Bank.

**Model Operation User (Deposit Fraud Team)**

* Deposit Fraud team: The Deposit Fraud Team is responsible for reviewing alerting items, accepting or rejecting alerted items, and daily monitoring of the Oasis system to ensure the system and alerts are working as expected.

**Model Support**

* Information Technology (IT)/Database Administrators (DBAs): The IT Application team and internal DBAs support the model as they work with the Fraud Strategy team to test any system changes in a lower environment prior to implementation in production, as required by the change control procedures. In addition, the IT team and internal DBAs are responsible for implementing approved changes to any existing rules or queues or any other necessary system changes.

**Model Validators**

* Bank Model Risk Management determines who the model validators of the OASIS model will be on a case-by-case basis. Based on each model validation’s requirements, internal resource availability, and subject-matter expertise required, the Bank Model Risk Management may engage outside consulting firms to support a specific validation need.
* Model validators are responsible for completing an independent model validation with a scope as determined by Model Risk Management’s defined Independent Model Validation Methodology. Please refer to the ***“*EWB Model Validation Methodology.pdf”** for more information on the Bank’s independent model validation methodology.

1. No changes have been made to the model since the validation completed in 2023.
2. The most recent model validation dated May 14, 2024, by Model Risk Management and seven (7) findings were noted: four (4) rated moderate and three (3) rated low. The findings are as follows:

**Moderate**

*OASIS-M01:* The Bank does not have a data dictionary, production data reconciliation process, or data lineage

independent testing.

*OASIS-M02:* The Bank does not have an implementation test plan which has resulted in inaccuracies in

implementation.

*OASIS-M03:* The Bank does not have a formalized procedure to determine model performance or a tuning

procedure which has resulted in poor model performance.

*OASIS-M04:* The Bank did not perform pre-implementation testing and has not defined benchmarking for their

use of the model.

**Low**

*OASIS-L01:* OASIS documentation lacks rationale for choosing the OASIS model and its configurations.

*OASIS-L02:* OASIS documentation lacks identification of the underlying assumptions and limitations of the

model and limitations identified by the vendor lack appropriate risk mitigants.

*OASIS-L03:* OASIS documentation does not include change control management procedures or model version

control procedures, and model development documentation is not maintained.

# INPUT DATA INTEGRITY & APPROPRIATENESS

## MODEL DEVELOPMENT DATA

Model Development Data refers to the data used in the research & development process to determine the model specifications. That is, the process for determining the exact mathematical formulas, algorithms, inputs, parameters, and assumptions that comprise a model.

Note: This documentation section is not applicable for those models whose structure is not determined through empirical data analysis. This includes, for example, some market risk / trading models where the model structure is based on financial theory (e.g., Black-Scholes options pricing model) or qualitative models whose structure and parameters were determined judgmentally.

**Reference Document List**

Please list all the documents referred to in this section.

|  |  |  |
| --- | --- | --- |
| **#** | **Reference Document Name** | **High Level Description and purpose of the Document** |
| 1 | model-documentation-faqs-oasis.pdf | High level overview of the development and model logic of the OASIS model |
| 2 | OASIS Performance Tuning and Optimization.pdf | Vendor provided user guide for the predictive analytics, machine learning, and performance of the OASIS model |
| 3 | Argo OASIS Check v2.pptx | ETL and high-level data flow information into the OASIS model |

**Data Assumptions Summary**

Please list out data assumptions applied in the model development and model production process, such as missing value treatment, outlier treatment, etc.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **#** | **Assumption Name** | **Assumption Description** | **Materiality of Assumption** | **Rationales for this Assumption**  (Business driven or quantitative methodology driven) |
| 1 | Data Availability | Check transaction data is available for ongoing fraud monitoring | Sufficient historical data and daily check data transaction is available for model | Availability of check transaction data is essential for the model in detecting and preventing fraudulent activities, and serves as valuable resource for resolving inquiries, and discrepancies. |

**Data Limitation Summary**

Please list out data limitations, their impact of business use, and ongoing monitoring program to appropriately manage the related risk.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **#** | **Limitation Name** | **Limitation Description** | **Impact on Business Use** | **Monitoring Description & Frequency** |
| 1 | Print quality of check | Low quality printed check can obscure relevant information in Optical Character Recognition (OCR) processing | Low quality printed check with smudged Magnetic Ink Character Recognition (MICR) can result inaccurate data extraction | The item processing department will review the low-quality printed check with smudged account number encoded in MICR and determine reject no-post and return as Unable to Locate (UTL) account. |
| 2 | Same day account open without a branch identifier | Same day account open may not be as robust as in providing branch identifier reference. | The absence of a branch id can hinder the OASIS queues output for east and west branches. | The Fraud Strategy team workaround to monitor this limitation via the daily OASIS queue performance. Working with Argo to develop a non-post queue as a permanent monitoring solution in OASIS. |

### Overview of Model Development Data

Provide descriptive characteristics of the model development data, for example, coverage of products / portfolios / transactions, time periods, geographic distribution, etc.

The sources and flows of all the data leveraged in model development should be illustrated with a data flow diagram. The diagram should show each stage of the data preparation process from the initial data pull to the final datasets used for model development and testing including data quality assurance controls.

Model Owner:

The data flow of from VisionIP to OASIS is as follows:

A diagram of a computer server

Description automatically generated

Per the model documentation provided by the vendor, **(“model-documentation-faqs-oasis.pdf”),** implementing the ARGO OASIS fraud model consisted of five (5) logical steps:

1. Selecting the appropriate historical transaction data for training the model.
2. Defining, calculating, and selecting appropriate features.
3. Building and training the models.
4. Model testing during development.
5. Model validation in production.

For additional detail regarding the steps above, please refer to pages 4 and 5 of **“model-documentation-faqs-oasis.pdf.”**

However, it should be noted that the current deployment of OASIS does not include the Machine Learning functionality. As such, the model requires no training as the current functionality is limited to features, feature calculations and check image comparisons.

### Development Data Sources, Extraction Process, and Reconciliation



#### Data Sources

Identify the sources of the model development data, for example, internal data from specific corporate data warehouse tables, desktop databases, text files, or external data from third-party vendors or websites. Development data may also include the output of other upstream models or computational tools.

If both internal and external data are used in the model development, you may want to create subsections covering them separately.

Model Owner:

The primary data source is transactional data, which is imported from the Bank’s on premise VisionIP core item processing application to OASIS and includes data from two stages of checking processing called ‘inclearing’ and ‘Proof of Deposits (POD)’.

Inclearing refers to the process by which a check is presented by the payee’s bank (the bank where the check is deposited) to the payor’s bank (the bank that issued the check) for payment. Inclearing occurs when the payor’s bank processes the check. The Bank receives Inclearing ICL files (Image Cash Letter) from the Federal Reserve Bank and JP Morgan Chase & Co (JPMC).

Proof of deposit (POD) refers to the process for a branch teller deposit provide assurance to customer that their funds have been processed. VisionIP captures all the physical and electronic documents received by the teller line. The Item Processing dept processes POD and inclearing checks throughout the morning, but the Inclearing runfiles are keyed, balanced, and closed first, so the Inclearing file is generated and sent to Oasis first. The Bank processes image cash letters from vendors for POD.

The secondary data source is check imaged data. The Bank check images are stored in the VisionIP application and check data is stored in VisionArchive. OASIS uses Application Program Interface (API) to pull images to conduct image comparisons.

#### Data Relevance

Discuss the relevance of the development data to the modeling objective. For example, is the composition of the development data representative of the current portfolio in terms of coverage and distribution of data attributes? Is the time period selected for development data appropriate for the model’s business purpose and the statistical estimation technique?

If proxies for internal data are used, such as internal data for other products or external data from public databases or third-party services, justify and document the applicability and appropriateness of the proxy data to the specific internal portfolio / purpose.

For vendor models, document a comprehensive assessment of the vendor’s development data applicability to the Company’s internal portfolio/products/customers. This typically involves a comparison of the external and internal data for key model drivers (e.g., geographic distribution, loan/transaction size, loan/product type, etc.).

Model Owner:

Transactional and check image data are relevant for OASIS features to conduct calculated tests to determine suspect item probability.

#### Data Extraction Process

Describe how the development data is extracted, either automatically or manually, or otherwise obtained.

Include references to the code or files used to extract the data or to the data files received from other individuals / departments.

Model Owner:

Two (2) files are extracted from VisionIP using a program called XLAT.exe, which takes the data from the proprietary VisionIP database and transforms it into a flat file. The flat file format is defined by the layout of the CDCIOUT.tbl table structure. The following data load processes provide detail on how the POD and Inclearing files are ingested from the VisionIP source into the Oasis model.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Vendor Solution | Data Type | Job Name | Job Frequency | Job Description |
| VisionIP | Inclearing (ICL) | ASD Fraud File Inclearing | Manually run at 4PM PST daily | ALLITEMINC file is generated by VisionIP and delivered to the OASIS app server landing zone: PRVIPOA102W.      Files are stored in PRVIPVS101W\vision\bank\EWB\  DATA\mmddyyyy\SPOOL\ |
| VisionIP | POD | ASD Fraud File POD | Manually run at 12AM PST daily | ALLITEMPOD file is generated by VisionIP and delivered to OASIS app server landing zone: PRVIPOA102W.    Files are stored in PRVIPVarS101W\vision\bank\EWB\  DATA\mmddyyyy\SPOOL\ |
| OASIS | Inclearing (ICL) | OASIS Subprocess | Automatically run at 7:30PM PST Monday through Friday, excluding holidays | ALLITEMINC file is imported into the OASIS\_TRANSACTIONS table. Applicable data filters are applied. |
| OASIS | POD | OASIS Subprocess | Automatically run at 3AM PST (next day) Tuesday through Saturday, excluding holidays | ALLITEMPOD file is imported into the OASIS\_TRANSACTIONS table. Applicable data filters are applied. |

Inclearing file refers to the process by which a check is presented by the payee’s bank (the bank where the check is deposited) to the payor’s bank (the bank that issued the check) for payment. The bank receives an inclearing Image Cash Letter (ICL) file from the Federal Reserve Bank and JPMorgan & Chase Co (JPMC).

Proof of Deposit (POD) file refers to the process of verifying the documentation of a check deposit into a bank account. The Item Processing department processes Inclearing and POD checks throughout the morning, but the inclearing run files are keyed, balanced and closed first, so the inclearing file is generated and sent to OASIS first.

#### Data Reconciliation

Demonstrate that the development data has been reconciled with a source system (e.g., the general ledger) or line of business report, or alternatively, explain how the extracted data was determined to be complete and accurate.

In addition, provide a step-by-step waterfall of data counts and balances at every step in the data preparation process from the raw data extract to the final modeling dataset.

Model Owner:

The Bank conducted data reconciliation test on an annual basis to ensure data accuracy, completeness of the data from the VisionIP to OASIS and OASIS tables after the End of Day (EOD) processing.

The data reconciliation test is conducted with two distinct scenarios.

Scenario 1- Data reconciliation test between VisionIP to OASIS for accuracy verification

This scenario to ensure that data reconcile from VisionIP accurately reflects the transaction being imported into OASIS. The data is sourced from two VisionIP all item files and OASIS table. This test required the use of SQL Server Management Studio (SSMS) to run a SQL query to extract one (1) business date of imported check data. The Bank gather the correspondent business date of two (2) VisionIP extracted all item files. In order to ensure the data from both sources are in compatible format for comparison, the two (2) raw VisionIP flat files required formatting to ensure the data is structured into columns for data attributes such as item processing trace, check number, account number within Excel.

Scenario 2 – Data reconciliation test within OASIS tables for completeness assurance

This test to confirm that all relevant data imported and processed in OASIS with no significant transactions are omitted. This test required the use of SQL Server Management Studio (SSMS) to run SQL queries to extract the same business date used for scenario 1 in OASIS database processed tables in good items and suspect items history. Compare the matched items processing trace and identify discrepancies between OASIS import check data, and OASIS good/suspect items history. Check data attributes are monitored through the data reconciliation process.

### Development Data Preparation



#### Data Quality and Treatments

Describe the raw data quality and any treatments used to address missing or erroneous values, for example, algorithms applied to impute values.

Document any analysis of data outliers and their impact on model development / outputs. Provide support for the selected approach for treating the outliers (if any).

Model Owner:

In the VisionIP application, the on-us check account number is checked against the daily Customer Information File (CIF) from Fidelity Information Services (FIS) Global.

#### Data Filtering and Exclusions

Provide a detailed description of, and justification for, data filtering and significant data exclusions that may potentially introduce model bias. Where a significant number of records is excluded due to data quality or other reasons, to the extent possible, analysis should be performed and documented showing the impact of the filtering rule.

A complete waterfall from the point of raw data extract to the final development/testing data showing the impacts of each exclusion (in terms of the number of records and other key metrics) should be provided.

Model Owner:

An on-us check cashed at the bank, accounts that have Positive Pay process and cashier’s checks are the only data excluded from monitoring through OASIS at this time.

Cash paid items are excluded from the VisionIP files sent to the OASIS solution since Teller completed the due diligence and determined it is not suspect item to complete cash out at the branch.

Below is number of cash paid items excluded from OASIS – sampled for four (4) business date from 4/18/2024 to 4/23/2024 during data reconciliation.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Date | OASIS Processed Items | | FIS Deposit History | |
| **Source Table OASIS\_TRANSACTIONS** | **Source Table OASIS\_SUSPIC\_HIST** | **Source Table**  **EWB\_fact\_hist** | |
| **Good Items** | **Return Items** | **Cash Paid Items** | **Percentage (%)** |
| 4/18/2024 | 21,449 | 11 | 402 | 1.84% |
| 4/19/2024 | 22,078 | 9 | 744 | 3.26% |
| 4/22/2024 | 36,205 | 17 | 700 | 1.90% |
| 4/23/2024 | 31,528 | 25 | 354 | 1.11% |

#### Data Sampling

Provide details of statistical sampling, if any, performed to create the model development and testing datasets.

Model Owner:

The machine learning capabilities of the OASIS model are not implemented at the Bank; therefore, the data sampling used for model development is not applicable.

Please refer to **“OASIS Performance Tuning and Optimization.pdf”** and **“model-documentation-faqs-oasis.pdf”**or more information on the machine learning capabilities of the OASIS model.

The Argo OASIS model inputs a dataset of on-us check transactions from Bank’s records. The Bank must ensure the dataset includes both legitimate transactions and instances of known fraud.

#### Data Transformations

Provide a description of, and rationale for, operations/calculations on raw data, such as scaling, forming data segments, averaging, or combining data from multiples sources (for example, to calculate charge-off rates) in order to produce model development-ready data.

Describe the composite/derived variables created out of raw data. For example, splines, Weight-of-Evidence transformations of variables, interaction terms, etc. Provide support for the technical soundness and appropriateness of the selected transformations in the context of the specific modeling approach you selected and the overall model purpose.

Specifically:

For models that utilize feature engineering, provide detailed documentation of the engineering process, including a description of the software/package used to perform the feature engineering and a discussion on the limitations of the selected engineering approach.

For models that utilize unstructured data, include detailed description of the data pre-processing of unstructured data. Provide analysis/test/comparison results with related data/scripts/outputs if any to justify the pre-processing performed.

For advanced machine learning models, also include detailed discussion on the sufficiency and appropriateness of data transformations and treatments applied with respect to the ML algorithm used (for example, standardization/normalization is required for KNN but not for Random Forests). Provide analysis/test/comparison results with related data/scripts/outputs if any to support the discussion.

Model Owner:

Argo defines the file layout for the two (2) imported files. The fields include: VisionIP sequence number, check/serial number, on-us transit routing number (aka TR or ABA number), check account number, transaction code (trancode), dollar amount and transaction date. There is no data transformation in the data extraction and feeding into OASIS.

#### Variable Definitions

Provide definitions of variables, including alternative transformations of variables tested. For vendor models, describe how the vendor’s definitions for inputs and outputs compare with the Bank’s internal definitions (e.g., delinquency, defaults, accounting losses, etc.).

Reference the location of the comprehensive data dictionary that lists each variable’s description, source, allowable values, and other relevant information.

Response Variable

Describe the response/performance/dependent variable that the model is designed to estimate/project.

Model Owner:

The response variables within the OASIS model are the alerts generated by the queue criteria.

Explanatory Variables

Describe the explanatory/independent variable candidates assessed in the model development process.

Model Owner:

The Bank does not maintain any artifacts from the initial implementation of Oasis.

For information from the vendor regarding variables used during the model development process, please refer to **“model-documentation-faqs-oasis.pdf.”**

### Data Limitations

Provide information about known data limitations / weaknesses and an assessment of their impact on the final model’s output. For example, if the model was developed based on external data that differs notably from the Bank’s data, the differences and their potential impact must be documented. For each noted weakness / limitation, describe how the associated risk is currently being mitigated. Additionally, where longer-term remedial actions are being undertaken or planned (e.g., an initiative to clean up the existing data or collect incremental data), such actions should also be documented.

Model Owner:

Low quality printed check can obscure relevant information in Optical Character Recognition (OCR) processing for check image. A poorly printed check with smudged Magnetic Ink Character Recognition (MICR) can result in inaccurate data extraction especially for the on-us account number. The image data will be compared in OASIS, but with an incorrect on-us account number due to the smudged account number encoded in MICR. Thus, it will analyze but not alert in queue since the incorrect on-us account will have not a matching reference to an actual Bank branch.

To address this risk, there is a compensating control in the item processing department. The item processing department will review the low-quality printed check with the smudged account number encoded in MICR and the rejected item. After review, the item is not posted and is returned with unable to locate (UTL) account.

Opening a same day account may not be as robust in providing branch identifier reference during OASIS process. The lack of a branch identifier means less contextual information about the account for OASIS queues, especially east and west coast branches. As the queues are segmented into East and West Coast geographies for easier analyst prioritization.

To address this data limitation, the workaround to monitor this limitation via the daily OASIS queue performance. Model owner/user working with Argo to develop a non-post queue as a permanent monitoring solution in OASIS.

### Data Preparation Software / Platform

Provide information on the software and/or programming language used in the data extraction, transformation, and other steps to prepare the model development and testing data. Provide a reference to the location of the development programming codes, associated log files, and other data preparation artifacts.

Model Owner:

The Bank does not maintain any artifacts from the initial implementation of OASIS. However, Production transactional data is extracted from VisionIP using a program called XLAT.exe, which takes the data from the proprietary VisionIP database and transforms it into a flat file.

### Data Retention

Describe where the development data is stored (post development) and how the environment is controlled. Provide the minimum time period for data retention.

Model Owner:

Argo configured the Bank’s OASIS solution with production check data retention for account history of 365 days and image history of 700 days. For each account, system configured to hold up to maximum 15 check images for comparisons.

# CONCEPTUAL SOUNDNESS

## MODEL THEORY AND ASSUMPTIONS

**Reference Document List**

Please list all the documents referred to in this section.

|  |  |  |
| --- | --- | --- |
| **#** | **Reference Document Name** | **High Level Description and purpose of the Document** |
| 1 | OASIS Performance Tuning and Optimization.pdf | Vendor provided user guide for the predictive analytics, machine learning, and performance of the OASIS model |
| 2 | model-documentation-faqs-oasis.pdf | High level overview of the development and model logic of the OASIS model |
| 3 | MD.06 Model Solution Guides Oasis.pdf | Vendor provided OASIS user guide |

**Model Assumption Summary**

Please list out model methodology assumptions applied in the model development and model production process, such as missing value treatment, outlier treatment, etc.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **#** | **Assumption Name** | **Assumption Description** | **Materiality of Assumption** | **Rationales for this Assumption**  (Business driven or quantitative methodology driven) |
| 1 | Feature relevance | Uses Parascript software to analyze check images to calculate image analysis scores | High | Licensed Parascript software to compare check stock and signature against the reference check images to calculate score. Incorrect image labeling can generate additional false positive. |

**Model Limitation Summary**

Please list out model methodology related limitations, their impact of business use, and ongoing monitoring program to appropriately manage the associated risk.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **#** | **Limitation Name** | **Limitation Description** | **Impact on Business Use** | **Monitoring Description & Frequency** |
| 1 | Model Accuracy – False Positive | Model produces false positive where legitimate transactions flagged as fraud | Legitimate transactions flagged as fraudulent | Continuous monitoring of the OASIS queue in production. Periodically reassess the model’s performance and update it as needed to address emerging limitations |
| 2 | Model Accuracy – False Negatives | Anomaly fraudulent transactions missed | Fraudulent transactions are not flagged can result in financial losses | Feedback from Deposit Fraud team who works on the model output. Their insight can help identify previously unseen types of fraud. Also, Fraud Strategy team review the Forgery Affidavit Claims (FAC) log data. |

### Model Theory and Methodology

#### Modeling Approach

Provide a description of the modeling approach you have selected, including the statistical estimation approach or machine learning technique, if applicable (with further details of the model construction/estimation process to be provided in Section 3.2 Model Estimation/Training and Selection).

For advanced Machine Learning (ML) models, discuss briefly whether a self-explanatory or less complex model (e.g., logistic regression, linear regression) is viable in solving the same business problem. If not, explain why not. Detailed information on this topic should be provided in Section 3.1.1.3. Alternative Approaches Explored

Model Owner:

The machine learning capabilities of the OASIS model are not implemented at the Bank.

The current implemented model version is limited to queues, feature calculations, and check image comparison.

Feature calculations evaluate aspects of an item that could increase its risk. Feature calculations, including OASIS fraud tests, produce numerical risk scores, where higher scores correlate to a greater degree of risk. Each fraud test examines one (1) aspect of an item’s transaction, such as serial number on a check, to identify outliers.

The Bank’s OASIS model analyzes suspicious items based on Transaction Analysis (TA) and Image Analysis (IA) tests.

* Image Analysis tests verify signatures and verify check stock.
* Transaction Analysis tests identify, flag, and review unusual account activities and suspicious items.

The Bank utilizes six (6) Image Analysis tests and two (2) Transaction Analysis tests for queue. Details on the Bank’s OASIS model’s eight (8) analytics tests and 21 filters are provided in section 3.1.1.2 Model Structure/Formulae.

In the OASIS Predictive Analytics process, analytics tests numerically measure the probability of fraud, with 0% being “impossible” and 100% being “certain.” Each analytics test used in the predictive analysis process tests for a specific fraud type and has global test parameters that are configurable.

Next in the OASIS Predictive Analytics process, OASIS DSL (Determination of Suspicion Level) analytics aggregate all individual scores from the analytics tests into a single probability suspicion score to assess an item’s fraud suspicion level. Probability suspicion scores range in negative value between -100 to 0. A score of 0 indicates the test was passed or bypassed, -75 indicates the test was undetermined due to insufficient data, and a negative score of 1-74 or 76-100 indicates the test failed, with -100 being the maximum risk probability.

When reviewing suspect items, OASIS displays a side-by-side comparison of the image of a suspect transaction and a reference image, such as check images. The output is a decision of whether the check is within norm, outside the norm, and the extent of the departure from the norm. Check images pass when the analyzed image is at or above an Image Analysis Confidence Level and fail when the analyzed image is below an Image Analysis Confidence Level. The analyzed item’s raw score is compared to the confidence value:

* Raw > confidence: the item passed and is considered in the norm and not suspect.
* Raw <= confidence, the item failed. The suspect level is then calculated by normalizing the engine score relative to this confidence level value. The suspect level is displayed on the Suspicious Transactions or Images window in OASIS.

Image Analysis Confidence Levels can be configured in OASIS. Increasing the confidence value implies a stricter strategy versus lowering it implies a more risk tolerant strategy. If an item’s raw score is below or equal to the confidence value, increasing the confidence value results in the item’s score value becoming more suspicious. For more information on IA confidence levels, refer to pages 98 and 146-150 in **“MD.06 Model Solution Guides Oasis.pdf.”**

Overall, the Bank’s model applies individual fraud analytics tests, determines the Suspicion Level (DSL) score, and routes to a work queue for adjudication. The OASIS queue identifies and prioritizes suspicious items for further review by a Bank analyst. Bank analysts can review and disposition a transaction before EOD processing, at which point OASIS assigns a disposition to all suspect items with no disposition. OASIS assigns a disposition of “Accept” or “Reject based on the Bank’s auto close configuration. Suspect resolution is final after EOD processing.” Refer to page 2 in **"OASIS Performance Tuning and Optimization.pdf."**

#### Model Structure/Formulae

*Detail all relevant mathematical equations applied in the model with a clear explanation of the notation*. Describe the model inputs and outputs if not already provided in Section 2.1.3.5. Variable Definitions

Note: This section applies to all models and should be especially detailed for models that were not developed through statistical or machine learning analysis of empirical data (e.g., the market risk / trading models based on financial theory). For these models, the rationale for the particular choice of inputs (e.g., prices, interest rates, volatilities, variance/covariance matrices) should be provided.

Model Owner:

Per the **“MD.06 Model Solution Guides Oasis.pdf,”** OASIS analyzes potentially fraudulent items based on the Transaction Analysis (TA) and Image Analysis (IA) implemented at the Bank. The model analyzes various risk indicators for check transactions to calculate check transaction attributes and assigns a score, between -100 and zero, to each attribute, based on level of risk - the more negative the score, the higher the degree of failure and the more fraudulent the model believes the transaction to be. Alerts are generated for check transactions that meet a set of conditions, for each individual score, preconfigured by the bank.

The Bank has implemented the following eight (8) tests, consisting of six (6) transaction analysis (TA) tests and two (2) image analysis (IA) tests in the queues:

| OASIS Test Name | Fraud Type | Test Type / Score | Description |
| --- | --- | --- | --- |
| Account Dormant | * First-party dormant or inactive account * Third-party account takeover | Binary  Score Information   * +10 if the account is not dormant (passed). * 0 if the test did not perform. * -100 if the account is dormant (failed). | The system performs the Account Dormant test for every account with at least one transaction on a given processing date. The first part checks whether an operator has manually updated a given account to a dormant status. The second part involves verification of account activity to mark dormant or inactive accounts on the available account history for the past 90 days. All accounts with no activity for the past 60 days are flagged. |
| Check Number Out of Range | * Third-party counterfeit * First-party stolen checks * Account used in pre-approved debits | Probabilistic  Score Information   * +10 if the check number is in range (passed). * 0 if the test did not perform. * any value between -1 and -100 if the check is out of the range (failed). The close to -100, the more out of pattern. If a new check range is built the test will fail at -75 | The test compares the distribution of check numbers seen in the past for a given account and determines if the presented check falls within the distribution (this also applies to accounts that utilize multiple check ranges). |
| Daily Amount Out of Range | * Third-party counterfeit * First-party stolen checks * Third-party large withdrawal or first-party deposit * Account takeover | Probabilistic  Score Information   * +10 if the daily amount is in pattern with other days (passed). * 0 if the test did not perform. * any value between -1 and -100 if the daily amount is out of pattern (failed). The close to -100, the more out of pattern. | This test consists of two parts. The first two tests are transaction type- based tests and are performed for each transaction type encountered on a given processing date. The last two tests combine all transactions, discarding their transaction type |
| Duplicate Check Number | * Third-party counterfeit * First-party deposit bad checks * First-party multiple deposits | Binary  Score Information   * +10 if the check number is valid (passed). * 0 if the test did not perform. * -100 if the check is duplicate (failed) | The test reviews all debit DDA transactions over the minimum amount defined for this account type or account to compare the transaction’s serial number against account activity for the past 90 days. Additionally, this test checks all of today’s items to make sure that there are no items with a duplicate check number. |
| Invalid Check Number | * Third-party counterfeit * Bad data captured | Binary  Score Information   * +10 if the check number is valid (passed). * 0 if the test did not perform. * -100 if the check is number is zero (failed) | This test reviews all debit DDA transactions over the minimum amount defined for this account type or account to ensure that a check number is a non-zero value. |
| Transaction Amount Out of Pattern | * Third-party counterfeits * First-party stolen checks * Third-party large withdrawal or first-party deposit * Account takeover | Probabilistic  Score Information   * +10 if the transaction amount is in pattern (passed). * 0 if the test did not perform. * any value between -1 and -100 if the transaction amount is out of pattern (failed). The close to -100, the more out of pattern. | This test consists of several parts. The first part involves verifying the amount of a given transaction against the Cap amount defined for this account type or account. The second part involves comparing the number of items within the tolerance of the amount for a given transaction to all transactions of a given transaction type in history for this account. The third part consists of checking how high the given amount is compared to all amounts for a given transaction type in history for this account. The last part includes verifying whether there are any items in the history for this account within the same amount as the given transaction. |
| Signature Verification | * Counterfeit * Forged maker signature-stolen checks * Pre-approved debits | Probabilistic  The score is normalized to a value between -100 (no match) and 0 (match found) | This test compares the signature of a presented item with a signature of the template image(s). |
| Check Background Verification | * Counterfeit * Altered * Pre-approved debits | Probabilistic  The score is normalized to a value between -100 (no match) and 0 (match found) | This test intakes the current day’s transactions and account reference images in OASIS to test the background of a check. The test marks a transaction as suspicious when the check background on the check does not match the account reference images. |

For additional information about additional analytics tests available in OASIS, refer to pages 6-8 of **“OASIS Performance Tuning and Optimization.pdf.”** For information relating to the configuration of the model at the Bank, refer to the Configuration section of this document.

The Bank has a total of 21 queues developed to monitor for on-us check fraud. These queues employ a combination of eight (8) different analytics tests and employ dollar amount filters to target higher-risk fraud. The queues are also segmented into East and West Coast geographies for easier analyst prioritization. See the table below for a complete list of queues developed.

| Queue Name | Dollar Threshold | Configuration |
| --- | --- | --- |
| West Coast | > $1,499.99 | NOT East Coast Branches  (Check Number Out of Range - failed more than 80 AND  Check Background Verification - failed more than 80)  OR  NOT East Coast Branches  Invalid Check Number - failed more than 80 |
| East Coast | > $1,499.99 | In East Coast Branches  (Check Number Out of Range - failed more than 80 AND  Check Background Verification - failed more than 80)  OR  In East Coast Branches  Invalid Check Number - failed more than 80 |
| High Risk West Coast | > $1,399.99 | Not East Coast Branches  Check Number Out of Range - failed more than 75 AND  Check Background Verification - failed more than 75 AND  Signature Verification - failed more than 75 |
| High Risk East Coast | > $1,399.99 | In East Coast Branches  Check Number Out of Range - failed more than 75 AND  Check Background Verification - failed more than 75 AND  Signature Verification - failed more than 75 |
| $125k West Coast | > $124,999.99 | Not East Coast Branches  Check Background Verification - failed more than 100 AND  Check Number Out of Range - failed more than 75 |
| $125k East Coast | > $124,999.99 | In East Coast Branches  Check Background Verification - failed more than 100 AND  Check Number Out of Range - failed more than 75 |
| $500k West Coast | > $499,999 | Not East Coast Branches  Daily Amount Out of Range - failed more than 75 OR  Signature Verification - failed more than 75 OR  Check Number Out of Range - failed more than 75 |
| $500k East Coast | > $499,999 | In East Coast Branches  Daily Amount Out of Range - failed more than 75 OR  Signature Verification - failed more than 75 OR  Check Number Out of Range - failed more than 75 |
| Signature Verification $10k West Coast | > $9,999.99 | Not East Coast Branches  Signature Verification - failed more than 95 |
| Signature Verification $10k East Coast | > $9,999.99 | In East Coast Branches  Signature Verification - failed more than 95 |
| Check Background West Coast | > $8,999.99 | Not East Coast Branches  Check Background Verification - failed more than 95 |
| Check Background East Coast | > $8,999.99 | In East Coast Branches  Check Background Verification - failed more than 95 |
| East Coast – Dormant & Signature $2k | > $1,999.99 | In East Coast Branches  Account Dormant - failed AND  Signature Verification - failed more than 60 |
| West Coast – Dormant & Signature $2k | > $1,999.99 | Not East Coast Branches  Account Dormant - failed AND  Signature Verification - failed more than 60 |
| East Coast – $9.5k – $10k | Between $9,500.00 and $9,999.99 | In East Coast Branches  Signature Verification - failed more than 40 AND  Check Number Out of Range - failed more than 75 AND  Transaction Amount Out of Pattern - failed more than 50 |
| West Coast – $9.5k – $10k | Between $9,500.00 and $9,999.99 | Not East Coast Branches  Signature Verification - failed more than 40 AND  Check Number Out of Range - failed more than 75 AND  Transaction Amount Out of Pattern - failed more than 50 |
| Multiple Highest Scores | Between $500.00 and $1,499.00 | Check Number Out of Range - failed more than 95 AND  Signature Verification - failed more than 95 AND  Check Background Verification - failed more than 90 |
| $7.0-8.8k Mid Scores | Between $7,000.00 and $8,800.00 | Signature Verification – failed more than 90 AND  Check Background Verification – failed more than 65 AND  Transaction Amount Out of Pattern – failed more than 35 |
| $3.5K Invalid Check | > $3,499.99 | Invalid Check Number – failed AND  Transaction Amount Out of Pattern – failed more than 95 AND  Check Background Verification – failed more than 40 |
| $18K Tran Amt Out of Pattern | > $17,999.99 | Check Background Verification – failed more than 86 AND  Transaction Amount Out of Pattern – failed more than 60 |
| $30K Tran Amt Out of Pattern | > $29,999.99 | Signature Verification – failed more than 90 AND  Transaction Amount Out of Pattern – failed more than 90 |

Refer to the **“MD.06 Model Solution Guides Oasis.pdf”** and **“OASIS Performance Tuning and Optimization.pdf”**documents for complete information regarding the analytics tests and their uses.

Per Argo, in OASIS 2.5 scores were presented in the UI as negative values as calculated in the backend. Post 2.5, to migrate user confusion the UI and documentation was updated to remove the negative indicator. The “**OASIS Performance Tuning and Optimization.pdf”** is written for Argo OASIS 4.3. However, the algorithms still calculate the suspicion score as negative values and are stored as such in the database tables. Functionally there is no change to the degree of suspicion.

#### Alternative Approaches Explored

Describe how the selected model theory/methodology (and estimation technique, if applicable) compares with industry practices for similar models and provide rigorous support for a selected approach that is non-standard or innovative. Provide references to industry and academic publications supporting the choice of this modeling methodology.

Describe alternative modeling approaches (including alternative estimation/numerical techniques, if applicable) that were considered and why they were not selected. Provide references to industry and academic publications discussing the alternative methodologies.

For machine learning (ML) models, provide performance comparison between the self-explanatory model and the selected ML model and a discussion on the trade-offs between model performance and transparency/interpretability. If a self-explanatory model is viable, also provide analysis/test/comparison results with related data/scripts/outputs if any to support the discussion.

Provide a comparative narrative for the selected ML model vs. other comparable/state-of-the-art methodologies with a discussion on the advantages and disadvantages of the selected ML model vs. the alternatives.

Model Owner:

The Bank does not maintain any artifacts from the initial implementation of Oasis. In addition, the Bank has not implemented the Machine Learning functionality of OASIS.

Check fraud range in complexity from simple as (duplicate presentment and check out of sequence) to more complicated (counterfeit and altered). Image Analysis is a traditional method of solving check fraud are effective for these type of typologies (counterfeit, and altered)

Positive Pay is a service the bank offer to small and mid-size business client and helps detect fraud by comparing a company’s issued checks with check presented for payment. This service is out of scope for OASIS to identify possible fraudulent checks.

### Segmentation Approach

Describe and justify the selected model segmentation scheme (or lack thereof), including any related quantitative analyses performed and subject matter expert qualitative considerations. Provide the segmentation waterfall logic, if applicable. Assess the impact of the selected segmentation scheme on the model estimation and output.

If in-model segmentation approach was followed (rather than developing separate equations/model objects for each segment), explain this with the rationale for going the route of in-model segmentation.

Model Owner:

The Bank does not include customer segmentation for on-us check fraud.

### Model Settings

If applicable, describe model settings and parameters, including vendor model customizations. For example, a vendor model may offer alternative interest rate term structures for valuation purposes. or a vendor may recommend updated model tuning parameters (e.g., for mortgage prepayment models) to be used in place of default values. For each setting/parameter, justify the selected value relative to the other choices available.

Model Owner:

The Bank’s OASIS model settings include the minimum Cap setting, where transactions with an amount lower than the minimum $500 will not be processed. The test score defaults to zero (0).

The Bank has implemented the following eight predictive (8) tests, consisting of 6 transactional analysis (TA) tests and 2 image analysis (IA) tests:

* Account Dormant
* Check Number Out of Range
* Daily Amount Out of Range
* Duplicate Check Number
* Invalid Check Number
* Transaction Amount Out of Pattern
* Signature Verification
* Check Background Verification

### Model Assumptions

List and justify the implicit and explicit assumptions associated with the model, including qualitative or quantitative expert judgments. Assess the impact of each assumption to the extent possible. For example, if a model relies on an average of historical values over the last 6 months, it may be important to test the impact on the model output of selecting alternative assumptions, e.g., 3 months, 9 months, etc.

If any assumptions are intended to be conservative, explain in what way they are conservative.

NOTE: Testing of any technical assumptions underlying the selected statistical/machine learning technique should be documented in Section 3.3.1. Statistical and Technical Assumptions Testing.

Model Owner:

The set of feature analytic tests in the model provides adequate coverage per the Bank’s check fraud coverage assessment. The model assumes that each transaction is independent of other transactions. The OASIS coverage assessment can be found within **“****EWB Fraud Coverage Assessment FINAL.xlsx.”**

The model assumes third party Parascript software development kit (SDK) used to analyze check images are capable to detect fraud and calculated scores for two (2) OASIS image analysis tests. The current implemented OASIS solution has Parascript licensed for CheckStock and SignatureXpert. Licensed CheckStock is used for the OASIS Check Background Verification image analysis test to identify counterfeit checks by inspecting pre-printed objects individually for instant comparison against reference check stock. Licensed SignatureXpert is used for the OASIS Signature Verification image analysis to prevent signature fraud and can use references to differentiate between natural anomalies and true irregularities that indicate fraud.

When check images are accepted in OASIS and added as reference images, it can be labelled as 1 – check image, 2 – Image Replacement Document (IRD), 3 - Signature or 4 – Pre-Authorized Debits (PAD). Associate the check image with incorrect label can result image test to calculate a more negative score which can result potential false positive in distinguishing fraud item.

### Model Limitations and Weaknesses

List any known model limitations and weaknesses. For each weakness / limitation, there should be a description of the associated model risk and, if applicable, the risk mitigant designed to address this risk. See the following example:

| ***Model Weakness or Limitation*** | ***Associated Model Risk(s)*** | ***Model Risk Mitigants / Remediation*** |
| --- | --- | --- |
| The model output is heavily impacted by several judgmental management assumptions, including x, y, and z. These assumptions are currently lacking empirical support. | Use of judgmental assumptions increases the risk of poor model predictions / measurements and unsupported model estimates, which may lead to inappropriate business decisions. | **Short Term Risk Mitigants**:   1. The judgmental assumptions will be subject to oversight by the governance committee X that will review and challenge the model owner's support for the assumptions on a monthly basis. 2. The model output will be benchmarked to the output from the alternative model Y on a quarterly basis. Significant divergence in the outputs will be investigated.   **Longer Term Remediation Plan**:   1. The model owner will investigate the possibility of obtaining empirical support for the assumptions x and y once an additional 6 months of data are collected. 2. The model owner will investigate the possibility of modifying the modeling approach to reduce the reliance on judgmental assumptions. |

Model Owner:

|  |  |  |
| --- | --- | --- |
| ***Model Weakness or Limitation*** | ***Associated Model Risk(s)*** | ***Model Risk Mitigants / Remediation*** |
| Model produces false positive where legitimate transactions flagged as fraud | Impacting model efficiency | * Continuous monitoring of the OASIS queue in production. * Periodically reassessing the model’s performance and updating it as needed to address emerging limitations. |
| Anomaly fraudulent transactions missed | Impacting model effectiveness | * Feedback from Deposit Fraud team who works on the model output. Their insight can help identify previously unseen types of fraud. * Also, Fraud Strategy team reviews the Forgery Affidavit Claims (FAC) log. |

As a compensating control, the Bank monitors activity on a daily basis in order to identify areas of improvement for the model.

## MODEL ESTIMATION / TRAINING AND SELECTION

Note: “Model estimation/training” is mostly applicable for those models that rely on statistical estimation and optimization techniques, such as regression analysis or machine learning techniques. However, this section is also relevant to some other types of models, including those that are developed using expert judgment (qualitative models).

**Reference Document List**

Please list all the documents referred to in this section.

|  |  |  |
| --- | --- | --- |
| **#** | **Reference Document Name** | **High Level Description and purpose of the Document** |
| 1 | EWB Fraud Coverage Assessment FINAL.xlsx | Coverage assessment completed of the Bank’s Fraud Program |

### Estimation Methodology and Assumptions

Describe in detail the model estimation methodology, including the assumptions that may be implicit in the estimation technique. For example, ordinary least squares estimations include assumptions about regression residuals. Describe any expert judgments related to the estimation, such as the selection of variable weighting methodologies.

For machine learning (ML) models, discuss whether monotonicity of relationships between the model features and the target variable is important or required, and whether the ML algorithm is configured to ensure such monotonicity.

Model Owner:

The machine learning functionality of the OASIS model are not implemented at the Bank; therefore, Estimation Methodology and related Assumptions are not applicable.

### Modeling Software / Platform

Provide information on the software and/or programming language used in the model estimation/training (including the version number, if applicable). If relevant, list the specific algorithms and packages used in model training.

Model Owner:

The vendor has shared this version of OASIS is written in java and connecting to Microsoft SQL database data repository.

### Hyper-parameter Tuning

For machine learning models, include a detailed description of the hyper-parameter tuning process, including the following information:

* The approach used for hyper-parameter tuning, including the rationale for leveraging this approach.
* The list of the hyper-parameters tuned (as well as those that are left at default values) and the range of values searched. If applicable, explain why some hyper-parameters were not tuned.
* Performance metric(s) used to select the optimal hyper-parameters and the supporting rationale.
* Sufficiently detailed discussion of the results of the tuning process and selected values, including any judgmental adjustments to the parameters, if any.

If the model also utilizes pre-training during development, provide details of the pre-training process and the pre-trained model as well as related analysis/test/comparison results.

Model Owner:

The machine learning capabilities of the OASIS model are not implemented at the Bank; therefore, this section is not applicable.

### Feature / Variable Selection

Describe in detail the approaches used to select candidate and final model variables/features, including the relevant criteria/thresholds for quantitative selection criteria, as well as any expert judgments.

Describe the process for involving subject matter specialists from the line of business to obtain their views on candidate variables, including the associated economic theory/business intuition behind each variable, as well as the expectation for the directional impact of each variable on the model output.

Describe any algorithms or statistical procedures (such as correlation analysis, Information Value analysis, stepwise regression procedure, etc.) used as part of the process to select final model variables from the full set of candidate model variables.

Model Owner:

The learning capabilities of the OASIS model are not implemented at the Bank.

The Bank used the following eight predictive (8) tests (6 transactional analysis and 2 image analysis) in the queue:

* Account Dormant
* Check Number Out of Range
* Daily Amount Out of Range
* Duplicate Check Number
* Invalid Check Number
* Transaction Amount Out of Pattern
* Signature Verification
* Check Background Verification

A check fraud coverage assessment was completed for Argo OASIS in March 2024. The summary of the results stated that additional analytics tests could be enabled to enhance coverage for stop payments, check kiting, check fraud rings, and payroll check fraud. The OASIS coverage assessment can be found within **“****EWB Fraud Coverage Assessment FINAL.xlsx.”**

Coverage for check theft, forged maker, and altered check schemes begins at caps minimum process amount $500. Coverage for these schemes could be enhanced with lower dollar amount thresholds, depending on the risk appetite of the Bank.

### Model Estimation / Training Results

**For statistical models,** provide statistical estimation results for the final model, as well as other model structures that were considered to be strong candidates. Estimation results should include not only the estimated coefficients, but also the t-statistics and associated p-values, measures of model fit, and summary of results of the appropriate statistical diagnostic tests (detailed statistical testing should be documented in the Statistical Testing section).

In addition to providing the estimation results, explain why this model was selected (relative to other candidate models), including both quantitative and qualitative factors.

**For machine learning models:**

* Provide a listing of the full set of features included in the final model.
* Provide a feature importance chart showing the top X most important features in the final model.
* Provide information on the number of features that contribute 90%, 95%, and 99% of model fit. If the number of features providing the last 1-2% of model fit is significant, explain the rationale for their inclusion.

**For both statistical and machine learning models**, this section should contain for each feature an explanation of the economic theory/business intuition for the inclusion of this feature, as well as the assessment of the estimated directionality of the relationship between the feature and the target variable relative to the a priori expectations. For simple statistical models this assessment can be accomplished through the evaluation of the estimated coefficient signs. For complex statistical and machine learning models, use of explainability testing techniques is required (refer to Section 3.3.5 Model Explainability Testing).

Model Owner:

The learning capabilities of the OASIS model are not implemented at the Bank.

The Bank uses the following six (6) transaction analysis (TA) tests to measure potentially fraudulent activities in the queue.

| Transaction Analysis | Purpose |
| --- | --- |
| Check Number Out of Range | Test if the check number is reasonably within range against other check numbers seen in the past and try to estimate/verify if the presented check falls within the range of those that were processed. |
| Transaction Amount Out of Pattern | Test is performed for each transaction over the minimum amount defined for this transaction type based on an account’s activity for a given transaction type. |
| Account Dormant | Test is performed for every account with at least one (1) transaction on a given processing date that has been inactive or dormant for the past 45 days (or configured value). |
| Invalid Check Number | Verifies if the check serial number is valid (non-zero). |
| Duplicate Check Number | Test transactional serial number against account activity for the past 90 days to make sure there are no items with a duplicate check number. |
| Daily Amount Out of Range | This test compares the total daily amount for all transaction types against the daily amounts seen in previous days or other daily patterns. |

The Bank uses the following two (2) image analysis (IA) tests in the queue to identify content alternative and validate payee handwritten signature.

| Image Analysis | Purpose |
| --- | --- |
| Signature Verification | Parascript SignatureXpert performs a comparison of signatures on presented checks against reference check images that represent the signatures of multiple account holders and optionally with different variations for a given processing date. |
| Check Background Verification | Parascript CheckStock performs a comparison of personal or business checks against reference check images that represent the different check stock that is accepted on the account. |

#### Judgmental Adjustments

Describe and justify any judgmental overlays/overrides of statistically estimated input parameters. If any such adjustments are intended to be conservative, explain in what way they are conservative. Note: this section should not be used to detail any overlays/overrides to the model outputs (described in Section 3.3.11. Need for Model Overlays).

Model Owner:

The Bank has identified thresholds for individual check transactions attributes, and conditions for generating alerts. Currently there is no judgement overlays and overrides by the model owner/user. If judgmental adjustments are required, it will be driven based on the ongoing fraud risk assessment in response to significant risks to the bank.

### Other Types of Model Estimation

#### Model Calibration

If applicable, describe the calibration process for models that are regularly fit to market data.

Model Owner:

Model owner/user will explore model calibration on feature selection and not regular fit to market data. Assess features that are strong indicators to fraudulent behaviors.

#### Vendor Model Tuning

If applicable, describe the process and results for any customization of vendor models (e.g., tuning of vendor model behavioral model parameters to Bank portfolio credit or prepayment experience) that is analogous to a statistical estimation.

Model Owner:

This section is not applicable as the vendor machine learning capabilities of the OASIS model is not implemented.

## Model Development Testing

For each test discussed in the following subsections, include the purpose of the test, the testing methodology, the criteria used to evaluate test results (that is, the applicable metrics and thresholds), and a summary of the results with commentary and conclusions. For any anomalous results, the conclusions should include information on the impact of these results on the model outputs and business use, and whether they require any specific risk mitigant.

The level of detail for the testing documentation should be sufficient to provide a clear and definitive basis for the model owner’s conclusions about model’s performance and robustness.

**Reference Document List**

Please list all the documents referred to in this section.

|  |  |  |
| --- | --- | --- |
| **#** | **Reference Document Name** | **High Level Description and purpose of the Document** |
| 1 | N/A | N/A |

### Statistical and Technical Assumptions Testing

For statistical and any other models that include statistical and other technical assumptions, provide testing of all assumptions associated with the selected estimation technique (e.g., for Ordinary Least Squares models on time series data this includes testing for multicollinearity, heteroscedasticity, non-normality of errors, autocorrelation, non-stationarity, seasonality, etc.).

For vendor models, to the extent that the assumptions testing information is available from the vendor, include the model owner’s assessment of the testing results and any associated risks.

Model Owner:

The learning capabilities of the OASIS model are not implemented at the Bank; therefore, this section is not applicable.

### Model Performance / Fit Testing

Provide testing of model performance / fit on the estimation and hold-out samples, including calculations of relative and absolute model errors for different population/product/portfolio risk segments and time periods. For some models, their fit can be evaluated using various additional statistical metrics and analytical techniques. This includes, for example: the K-S test, ROC curves (and AUC/Gini coefficient and similar measures of discriminatory power), lift charts, Precision/Recall, F1 score, risk profiling, etc.

For vendor models, include the model owner’s assessment of the model performance/fit testing results provided by vendor (based on vendor’s data) and any associated risks. In addition, include testing results on the Company’s internal data (or explain why it is not feasible).



#### **In-sample Performance/Fit**

Use this section for the testing of model performance/fit on the data on which the model was estimated/trained.

Model Owner:

The learning capabilities of the OASIS model are not implemented at the Bank; therefore, this section is not applicable as the model was not trained.

#### **Out-of-sample (but not out-of-time)**

Use this section for the testing of model performance/fit on data from the same time period as the in-sample estimation/training data but held out for model testing purposes.

Model Owner:

The learning capabilities of the OASIS model are not implemented at the Bank; therefore, this section is not applicable as the model was not trained.

#### **Out-of-time**

Use this section for the testing of model performance/fit on data from the time period different from the in-sample data, and not used in the estimation either because it was not yet available at the time of model estimation, or because it was available but excluded from the estimation/training for the express purpose of performing out-of-time model fit testing.

Model Owner:

The learning capabilities of the OASIS model are not implemented at the Bank; therefore, this section is not applicable as the model was not trained.

### Model Stability and Overfitting Testing

Provide testing to assess the stability of the model’s estimated relationships, for example:

* For statistical regression models, this involves regression coefficient stability testing and testing for structural breaks. Coefficient stability testing can be performed by repeatedly re-estimating the model on different subsets of the development sample (e.g., random sub-samples or samples representing different time periods covered by the dataset) as well as out-of-sample / out-of-time datasets. Values of regression coefficients and p-values across all samples are then assessed to evaluate the model stability.
* For machine learning models, because a comparison of model parameters is either impossible or impractical, testing of model stability generally involves a comparison of key performance statistics (e.g., K-S, AUC, Precision, Recall, F1, etc.) on different training and testing datasets. A common technique for assessing machine learning model’s stability and evaluating the risk of model overfitting is k-fold analysis. K-fold analysis should be performed in addition to testing of the model on the training, validation, out-of-sample, and out-of-time datasets.

Model Owner:

The model owner/user will evaluate model performance metric to monitor stability.

**Suspect Rate** – It is calculated the number of suspect items / total number of transactions. Suspect rate is equivalent to alert rate.

Evaluate the model’s ability to identify true positive (precision) and false positive (recall).

True Positive (TP) refers to the check selected by a Deposit Fraud Analyst for reason code 11 – fraud/counterfeit.

False Positive (FP) refers to the check item flag suspect item for review and Deposit Fraud Analyst disposition the item with other reason codes.

**Precision** = TP/ (FP+TP), where TP is the number of the true positives, and the FP is the number of false positives

**False Positive Rate** (FRP) = FP/ (FP+TP)

False Negative (FN) refers to the check later claimed by customer as a fraudulent item and updated by a Deposit Fraud Analyst for reason code 10 – forgery.

**Recall** = TP (TP+FN), where TP the number of true positive, and FN is the number of false negatives

### Back-testing

In addition to the model performance/fit testing documented in Section 3.3.2. Model Performance / Fit Testing, back-testing is highly beneficial and should be performed/documented for certain types of models. Back-testing is a class of testing techniques designed to assess the consistency of model predictions/estimations with the actual observed values, especially for different historical periods and over longer testing horizons.

These tests are designed to measure the accuracy of model performance over specified time periods. When documenting back-testing analyses, it is critically important to provide a detailed description of the test design including, for example:

* The design of the testing dataset includes the description of the time period, and information about any notable exclusions/inclusions that are inconsistent with the data used to develop the model.
* The logic for generating model predictions. For example, when back-testing a mortgage default model, the model developer would typically start with a particular historical portfolio snapshot and then use the model to generate predictions for each subsequent month/quarter without truing the model up using subsequent historical data.
* The source and nature of inputs and assumptions used in the back-test. For example, for a model that uses macroeconomic variables as inputs, the typical practice is to use actual historical values of such inputs during the back-test period (in order to isolate the error of the tested model from the error in the economic forecasts).

Use of graphical presentation of actual and predicted values is necessary in addition to any quantitative measures of model error (e.g., MAPE, MSE, etc.). This allows the model developer and reader to observe any areas of persistent model bias.

The developers should ensure that performance metrics and thresholds for acceptable performance are clearly stated and are aligned with the model’s business use. For example, for stress testing or CECL model designed to produce loss forecasts over a 2-year period, one of the error metrics should be based on the cumulative actual vs. predicted losses over a 2-year back-testing horizon.

Back-testing results should be accompanied by detailed narrative providing the model developers’ assessment of said results and their conclusions about any notable model biases or elevated error rates. Some such notable biases and performance issues may need to be noted as model weaknesses that must have associated risk mitigants.

Back-testing should be carried out for different populations. For example, when analyzing performance of residential or commercial mortgage loans, one should separately evaluate performance of the model on sub-populations that can be reasonably expected to have different behavioral characteristics. For example: different products, different vintages, or different segments of population by FICO score or by LTV or by another key risk driver.

Predictive models should also be back-tested over different economic environments, e.g., periods of stress vs. periods of economic growth. This is especially important for stress testing, CECL, and IFRS 9 models.

For vendor models, include the model owner’s assessment of the back- testing results provided by vendor (based on vendor’s data) and any associated risks. In addition, provide testing results on the Company’s internal data (or explain why it is not feasible).

In-time

Use this section for backtesting using the data from the same time period on which the model was estimated/trained.

Model Owner:

The Bank does not currently maintain any procedures for conducting backtesting in-house for OASIS.

Out-of-time

Use this section for backtesting using data from the time period different from the in-sample data.

Model Owner:

The Bank does not currently maintain any procedures for conducting backtesting in-house for OASIS.

### Model Explainability Testing

**For machine learning models**, provide sufficient information to understand the drivers of the model outputs and the directionality of their impacts. Use feature importance, Partial Dependency Plots, and a global interpretation method that explains the relationship between model inputs and outputs (e.g., SHAP feature importance, permutation-based feature importance, etc.)

For models that require generation of adverse action reason codes, testing of local interpretability using methods such as LIME is also required.

Advantages and disadvantages of the selected explainability testing methods should be discussed as well.

Model Owner:

The machine learning capabilities of the OASIS model are not implemented at the Bank; therefore, this section is not applicable.

### Benchmarking

Compare model results with alternative results using other models and/or other data (if available). Describe the benchmark model or data in sufficient detail to enable an assessment of its value as a reference point. For example, a benchmark model that is also a formal Challenger model that has been independently validated (with a successful validation outcome) would be a stronger reference point than a benchmark model that may be available but that has not been extensively tested. Similarly, external peer data may be more relevant in a benchmark comparison than broader industry data. Provide a detailed narrative explaining the outcome of the comparison and any notable differences between the model outputs and benchmarks.

Model Owner:

The model owner/user will monitor performance of the current model using historical metrics, which serves as baseline. If model performance is drifting away from the historical average or significant decline as indication of becoming less effective, then will explore alternative methods to introduce a challenger model to compare and run alongside the existing model.

### Sensitivity Analysis

Quantify the impact on model outputs of changes in the value of model inputs and assumptions (e.g., economic inputs, tuning parameters, calculation rules, and scenarios). If the model design is such that the sensitivity of the model output to changes in an individual input would depend significantly on the value of one or more of the other inputs, the impact of simultaneous changes in inputs should also be evaluated.

Model Owner:

Fraud Strategy team conduct sensitivity analysis on approved new queue or edit to existing queue to implement and evaluate potential risk factors in test environment using historical production data.

### Stress Testing / Scenario Analysis

Quantify the impact on model outputs of stressed changes in the values of inputs, including scenarios that are outside the range of ordinary expectations.

For stress testing/CECL/IFRS 9 and other models dependent on economic scenarios, assess the model forecast across benign and stressful scenarios. When evaluating model forecasts under different economic scenarios, the forecasts should be compared to historical values during similar economic conditions (to the extent that such comparison is meaningful). Any notable differences should be explained and justified. For example, if a model produces drastically lower forecasts of losses under a severe stress scenario compared to the historical losses during the Great Recession, an explanation (e.g., notable improvements in the portfolio quality) should be provided and supported with quantitative analysis, where possible.

The forecasts should also be assessed for internal consistency. For example, do the base, adverse, and severely adverse forecasts reflect incremental macroeconomic stress, or, if not, are they consistent with the unique characteristics of the scenarios and business intuition?

For vendor models, stress testing/scenario analysis should be performed on the Company’s internal data. If not feasible, include the model owner’s assessment of the stress testing and scenario analysis provided by vendor (based on vendor’s data) and any associated risks.

Model Owner:

The Bank does not currently maintain any procedures for stress testing in OASIS.

### Other Testing

Describe other testing performed applicable to the selected modeling approach, **if any**.

Model Owner:

No additional testing is conducted on the OASIS model.

### Overall Performance Assessment

Discuss overall conclusions on model performance based on the results of the testing described above.

Model Owner:

The model owner/user will conduct performance monitoring on the Argo OASIS model. Track metric such as precision or recall ensuring the model’s predictive performance remain stable.

### Need for Model Overlays

Document any proposed or implemented adjustments or overlays to the model outputs and their rationale. Describe the process for derivation and application of these overlays. Provide the impact by including model results with and without these overlays. Finally, outline the overlay review & challenge/approval process, including any Senior Management / Committee reviews and approval process if applicable, and the frequency of the overlay re-evaluation.

For vendor models, discuss the need for model tuning/dialing settings to better align model outputs to the Company’s internal outcomes.

Model Owner:

The Bank has identified thresholds for individual check transactions attributes, and conditions for generating alerts however, the Bank does not maintain documentation of the rationale for their selection or a Tuning Methodology.

# PRODUCTION PROCESS COMPLETENESS & ACCURACY

This section includes procedures and information related to model testing and usage following model development or vendor model acquisition.

**Reference Document List**

Please list all the documents referred to in this section.

|  |  |  |
| --- | --- | --- |
| **#** | **Reference Document Name** | **High Level Description and purpose of the Document** |
| 1 | VisionIP Diagram\_Prod\_10242023.pdf | VisionIP high level architecture diagram |
| 2 | OASIS Dictionary.pdf | OASIS data dictionary |
| 3 | Oasis.suspic.hist.Sept.01-13.2023.csv | List of required data elements for the OASIS model |
| 4 | SV\_CS model results.pdf | Description of the Image Analysis models, Check Stock Validation and Signature Verification. |
| 5 | OASIS-2-5-Release-Notes.pdf | Information on the newest model upgrade implemented at the Bank in 2020 |
| 6 | Monthly Risk Focused Meeting – Dec 23 Xceed & Oasis Slides.pdf | Evidence of metric presentation in December 2023 to senior management |
| 7 | MD.06 Model Solution Guides Oasis.pdf | Vendor provided OASIS user guide |
| 8 | Oasis\_Transactions.Sept.01-05.2023.xlsx | List of required data elements for the OASIS model |
| 9 | model-documentation-faqs-oasis.pdf | High level overview of the development and model logic of the OASIS model |
| 10 | OASIS Performance Tuning and Optimization.pdf | Vendor provided user guide for the predictive analytics, machine learning, and performance of the OASIS model |
| 11 | EWB Model Validation Methodology.pdf | The Bank’s independent model validation methodology |
| 12 | MRM-PnP01 EWBC MRM Policy v12.5.pdf | The Bank’s Model Risk Management (MRM) policy |
| 13 | OASIS Configuration Settings.xlsx | All active configurations currently implemented in the OASIS model |
| 14 | OASIS Application Disaster Recovery Plan.pdf | Disaster Recovery Plan (DRP) for OASIS in the banks’ business continuity tool Castellan (Riskonnect) |
| 15 | Risk Operations Department BIA.pdf | Risk & Operations Business Impact Analysis (BIA) |
| 16 | Risk Operations Department BC Plan.pdf | Risk & Operations Business Continuity Plan (BCP) |
| 17 | Argo OASIS Data Lineage and Data Reconciliation Testing Plan | Argo OASIS data lineage and conducting reconciliation testing plan to ensure data accuracy, and completeness |
| 18 | ITDBA-Automated Database Backups.pdf | IT DBA Automated SQL Database Backup |



## Production Application Testing

Describe the testing for accuracy of implementation of the model into production systems.

### System Testing Approach and Results

The objective of model production application testing is to ensure that computational processes implementing model calculations:

* Are consistent with the documented model specifications produced as part of the model development process. This includes source data fields, data transformation rules, mathematical equations, assumption values, etc.
* Are consistent with the documented business / user requirements.
* Are mathematically accurate and complete.
* Have been reviewed for consistency with any applicable accounting/finance specifications (e.g., GAAP and/or accounting policy requirements), stress testing requirements, or any other applicable regulatory requirements.
* Are operationally stable, repeatable, and sustainable.
* Interface accurately with both upstream and downstream systems (where applicable).

For vendor models, the purpose of the production application testing is to ensure that the models are correctly implemented on the Bank’s systems—if on-premises production process is selected, or the vendor’s model production environment is correctly connected to the Bank’s production data environment—if a cloud-based production process is selected, that the Bank’s production data inputs are consistent with the model publisher’s input specifications, and that all applicable software patches and fixes have been applied.

Describe in detail the testing plan for the individual model’s production implementation and its integration within a larger system and the vendor’s model production environment, if applicable. Include User Accepting Testing cases and scenarios, expected outcomes, and the individuals responsible for executing the test cases.

Document the results of the UAT testing execution, and the associated log of issues and subsequent resolutions.

Model Owner:

OASIS Graphical User Interface (GUI) is a web-based model with application and database server., The vendor is responsible for developing and releasing software updates and patches. The Bank is responsible to conduct testing the software update and patches in non-production environment before applying the update to the production environment to minimize interruption. The Bank's data is consistent with the input specifications that were completed during initial implementation.

The Bank does not maintain any artifacts from the initial implementation and testing plans are not available.

### User Acceptance Testing Approach and Results

Document the User Acceptance Testing approach, results, and sign-offs.

Model Owner:

Documentation of pre-production model implementation was not maintained. Documentation of a testing plan (including the testing approach, scope, testing scripts, test cases, test results as well as metrics/criteria used for verifying that the model was correctly implemented in production) is not available.

The Bank intends to perform implementation testing for any future model version grade with adequate documentation. The Bank will develop testing scripts and perform steps to ensure that all upgraded and new models are working as intended and meet the business requirements as part of UAT.

## Model Production Specifications

The following technical specifications should cover the end-to-end operation of the model, from data inputs and assumptions to final model reports. **To avoid duplication of information, some of the following sections may refer to earlier document sections instead of repeating the information.**

### Model Platform

Describe the technologies used for running the model, for example, Python, R, Excel, etc.

Model Owner:

OASIS is a web-based model that is accessed online.

### Data and Process Flow Diagram

Provide a flow diagram showing data sources, inputs, quality assurance control points, intermediate results, outputs, and reports.

Model Owner:

**Data Flow**

The following data flows provide a high-level overview of how data from the source system moves between applications and ultimately is ingested into the Oasis model for check fraud monitoring. Additionally, it provides a breakdown of the VisionIP architecture to store and pre-configure the POD and Inclearing source files.

**VisionIP to Oasis Application Data Flow**

A diagram of a computer server

Description automatically generated

**VisionIP Architecture**

A diagram of a server

Description automatically generated

Additional details regarding the Items Processing VisionIP production environment and system architecture can be found in **“VisionIP Diagram\_Prod\_10242023.pdf.”**

**Data Mapping**

Before input data can be used in the model, it must be mapped from the original source into a format that can be ingested by the model. Data mapping involves matching fields from a source file or table level attributes to a corresponding attribute in the Oasis model. In the case of mapping VisionIP source files to the Oasis model, all fields are pre-configured to be standardized by VisionIP. As a result, data transformations are not applied when exporting data from the VisionIP database into the POD and Inclearing source files. Data from these files is directly mapped to the Oasis target schema. VisionIP receives a daily CIF file from FIS to compare On-Us check account numbers to the master list of account numbers maintained by FIS. The account lookup ensures the transaction was executed on a valid bank account. No additional transformations are applied to the data outside of table level filtering, which can be found in the VisionIP to Oasis Data Mapping:

VisionIP to OASIS\_TRANSACTIONS and OASIS\_SUSPIC\_HIST Data Mapping:

| ALLITEMINC  ALLITEMPOD | | | OASIS\_TRANSACTIONS  OASIS\_SUSPIC\_HIST | |
| --- | --- | --- | --- | --- |
| Source Column Name | Description | Key Data Element | OASIS Transaction Column Name | Transformation Logic |
| Sequence | Item Processing Trace Number - Unique number to identify the transaction that is processed per day | Yes | trace | Direct Map to Oasis |
| Serial | Check Number | Yes | trans\_ID | Direct Map to Oasis |
| RIC | Return Item Code | Optional | N/A | Returned checks are processed in EWBRET, a separate VisionIP institution |
| TR | Transit Routing (ABA Routing Number) | Yes | transit | Direct Map to Oasis |
| Account | Account Number (On-Us) | Yes | acct | Direct Map to Oasis |
| TC | Tran Code (FIS Deposits Transaction Codes) | Yes | N/A | POD F~~i~~lter on On-Us Check Tran Codes: WHERE TC IN (210, 211, 482, 484, 800)    ICL filter on On-Us Check Tran Codes: WHERE TC IN (482, 800) |
| Amount | Transaction Dollar Amount | Yes | amount | Direct Map to Oasis |
| DBCR | Debit / Credit | Yes | N/A | N/A |
| Date | Transaction Date | Yes | trans\_date | Direct Map to Oasis |
| N/A | Identifies type of transaction flagged.  101 – paper based (checks or deposits) | Yes | trans\_type | Default to ‘101’ |

FIS Deposit Processing Transaction Codes:

|  |  |  |  |
| --- | --- | --- | --- |
| Transaction Code | Default Name | Transaction Code Description | VisionIP Source File |
| 210 | CHECK | Used to post over the counter checks before clearing items | POD |
| 211 | CHECK | Charge to customer’s account identifying a check transaction | POD |
| 482 | SUB INCLEARING CHECK | Used to generate a debit to the account presented as an Image Replacement Document (IRD) | Inclearing |
| 484 | SUB ON-US DEPOSIT CK | Used to generate a debit to the account posted prior to clearing items and presented as an Image Replacement Document (IRD) | Inclearing |
| 800 | CHECK | Charge to customers account identifying a check transaction. If a MICR serial number is available on the document, this will show as a part of the description | Inclearing |

The POD and Inclearing data ingested into the Oasis model is limited to On-Us Check transactions as defined in the FIS Deposit Processing Transaction Codes list. No other transaction types are monitored for fraud in the Oasis model.

Key Data Elements are identified below:

**Input File Format for ALLITEMINC and ALLITEMPOD**

A screenshot of a data

Description automatically generated

Additional fields listed in the **“OASIS Dictionary.pdf”** are model calculated fields used for scoring the degree of failure of a Bank configured test. Tests include Invalid Check Number, Transaction Amount Out of Range, and Number of Transactions Out of Range, amongst others. As a result, data mapping to calculated fields from VisionIP source files is not applicable. Additional filtering logic is applied to the CONUS\*.DBF run file, which scans Cash Paid Checks through an On-Us Image only run. An input file mask is utilized to exclude these transactions from the POD and Inclearing files before being loaded into the OASIS model.

Please note the information in this section does not include Image Cash Letters (ICL) from the Fed and JPMC for processing. OASIS will run a pre-configured API call to view check images from the Vision Archive system. No check images or image data is imported or stored in OASIS.

### Input Data Specifications

Provide a list of all inputs, including measurement units, a description of valid values or ranges (a full data dictionary should be attached in an appendix). Describe any data processing rules, such as filtering missing or invalid values infilling / overrides, substituting ceiling or floor values, data transformations, etc.

Model Owner:

**Data Input**

Input data for the Oasis model is produced by the Vision Content Application (eVision) and stored in the PRVSQL104W\PROD07 database prior to being sent to the OASIS application server. The two (2) VisionIP source files sent for ingestion into the Oasis model include:

* Inclearing (ICL) Transaction File: ALLITEMINC
* POD Transaction File: ALLITEMPOD

**Input File Format for ALLITEMINC and ALLITEMPOD**

A screenshot of a data

Description automatically generated

**Data Dictionary**

An Oasis data dictionary has been provided for high level data requirements and to aid in the creation of data mapping documents:

Oasis Suspicious Historical Data Requirements: See **“OASIS Dictionary.pdf”** and **“Oasis.suspic.hist.Sept.01-13.2023.csv”** for a full listing of data elements required for the OASIS model.

Oasis Transactions Data Requirements: See **“Oasis\_Transactions.Sept.01-05.2023.xlsx”** for a full listing of data elements required for the OASIS model.

**Model Inputs**

As noted in section 3.1.3, the model evaluates analyzes various risk indicators for check transactions to calculate check transaction attributes and assigns a score, between 0 and 100, to each attribute, based on level of risk - the higher the score, the more suspicious the model believes the transaction to be. Alerts are generated for check transactions that meet a set of conditions, for each individual score, preconfigured by the bank.

Per **"model-documentation-faqs-oasis.pdf,”** OASIS uses five (5) information types:

1. Item Data: Item amount, check serial number, date, account, etc.
2. Check Images: OASIS performs image analysis of checks.
3. Account Type: Different account types have different levels of risk.
4. Fraud Labels: For the model to learn to recognize and predict fraud, it needs to know which of its training items are fraudulent. Thus, the bank must provide labels of which of the provided items turned out to be fraudulent, along with the classification of same day returns and late day returns.
5. Teller, Mobile and Other Deposit Channels: In order to create deposit fraud models and collectability assessment for hold requirements, or check cashing requirements, OASIS will need deposit activity, teller journal activity, including geolocation and conductor, along with returned deposited items history, both metadata and images.

For additional information relating to the model inputs, please refer to page 10 of **"model-documentation-faqs-oasis.pdf.”**

### Model Formulas / Algorithms

Describe detailed model formulas, algorithms, and numerical techniques, if possible.

Model Owner:

The Bank has not evaluated the model structure or formulae of the OASIS model. Additionally, the machine learning capability of the OASIS model is not implemented at the Bank.

Please refer to **“model-documentation-faqs-oasis.pdf”** for full evaluation of the model structure and formulae of the OASIS model.

### Model Parameters and Settings Values

Provide the values for all parameters and other input assumptions, including hyper-parameters for machine learning models.

For vendor models, specify values of user-selectable settings.

Model Owner:

Please refer to **“Oasis Configuration Settings.xlsx”**for a full listing of all user-selectable settings.

### Model Outputs

Provide a list of all model outputs, including expected values or ranges.

Model Owner:

The model analyzes various check transaction attributes and assigns a score, between -100 and zero, to each attribute, based on level of risk – the higher the negative score, the more fraudulent the model believes the transaction to be. Alerts are generated for check transactions that meet a set of conditions, for each individual score, which have been preconfigured by the bank.

The table below shows the individual test results for the OASIS predictive analytics process, OASIS DSL (Determination of Suspicious Level):

|  |  |
| --- | --- |
| Resulting Test Score Value | Interpretation of Test Score |
| 0 | The test passed OR the test execution was bypassed because one of the following is true:   1. The test is configured not to run, 2. The transaction information matches a filter definition that specifically excludes the item, 3. The transaction amount falls below the minimum threshold for test execution. |
| (Negative) 1-74; 76-100 | The test failed. A score of 100 indicates a maximum risk probability. When a binary test fails, the test score is 100. These values serve as input to determine the aggregate suspicion-level score. |
| (Negative) 75 | The probabilistic test is undetermined due to insufficient statistical historical data for the account |

Please refer to pages 3, 4 and 5 of **“OASIS Performance Tuning and Optimization.pdf”**for details on understanding individual test results and probabilistic tests and caps.

For more information on the OASIS fraud model output, please refer to page 11 in the document named **"model-documentation-faqs-oasis.pdf.”**

**OASIS Image Analysis**

OASIS performs image analysis, check stock validation and signature verification. OASIS check stock Validation and OASIS Signature Verification are image-based analytical tools to validate the consistency and accuracy of check stocks and digitized signatures.

OASIS’ Check Stock Validation tool compares checks against check images stored within the OASIS application’s account profiles. OASIS produces a score indicating the degree of difference between the compared check images. Check features such as type, size, spacing, and font are examined for inconsistencies. Output scores have a value between 0 (match found) and 100 (no match). If the calculated score exceeds a predefined threshold, the check is marked for further review by a Bank fraud analyst. This comparison approach is repeated for the check signature verification process to identify irregularities and select items for further review by a Bank fraud analyst.

For details on the OASIS image analysis models, check stock validation and signature verification processes, please refer to **“SV\_CS model results.pdf”** and pages 1 and 2 in **“OASIS-2-5-Release Notes.pdf.”**

### Reports

Provide a list of all standard output files or reports and describe how they are used in the business.

Model Owner:

The fraud strategy team holds a monthly risk-focused meeting to review model performance.

They analyze the Forgery Affidavit Claims Log (FAC log) which tracks all fraudulent items where the bank is liable for loss to investigate suspicious historical data of the fraudulent accounts including analyzing how items are scored on both transaction analysis and image analysis tests for these accounts. They also research whether potential queue changes in Oasis can minimize loss. Refer to **“****Monthly Risk Focused Meeting – Dec 23 Xceed & Oasis Slides.pdf”** for the metrics reviewed in the meeting. The key stakeholder and approval responsibilities are with Sr. Management R&O. There is no defined threshold to re-evaluate and trigger a model recalibration.

Fraud Strategy, in collaboration with the Enterprise Risk Management team, is defining enhanced monthly metrics for OASIS. The intent is to establish key metrics to gauge the overall performance of the OASIS system. Also defined reporting to give insights into the performance of the specific queues we have defined. Refer to section 5.1 for the developed reports detail and data point.

## Operational Controls

Operational controls related to the model should be in place prior to the production deployment of the model.

### Model Access and Security

Access controls prevent unauthorized changes to the production code and unauthorized operation of the model in production. Describe who has “write access” to the model and can make changes to the underlying code of the model in development and in production, who has access to run the model in production, and who controls model access rights. If there is a formal access monitoring and review process in place, describe it here. Indicate whether any model files are password protected.

If there is no technical mechanism to prevent changes to the model in production (e.g., if the model is implemented using Python code), describe any checks performed to verify that no unauthorized changes have been made since the last approved update or use of the model (such as code comparisons).

Model Owner:

**Process to add/delete/edit a user in Oasis.**

 All access is granted, deleted, or edited through User Access Request (UAR), an internal application tool in which a Bank employee can submit an access request for physical buildings, applications, or networks.

**The process to add, remove, or edit a user in Oasis is as follows:**

1. The Bank employee who requires access must submit the UAR including their network ID, their employee ID, and the necessary access permissions (i.e., read, write).
2. The UAR application will route the request to the appropriate approving parties. For access to the Oasis model, the requesting employee’s reporting manager and the User Administration group must both approve the request.
3. Once approval has been granted, the User Administration group will update the user permissions in the model and notify the employee.
4. The employee will receive an email notification from User Administration <UserAdministration@eastwestbank.com> confirming access to the model.

For the process that the User Administration team undergoes to update the user settings in Oasis, please refer to Managing Users in the **“MD.06 Model Solution Guides Oasis.pdf.”**

**Restricting User Access**

Access to the Oasis model is restricted in the following ways:

* Log on Timeout
* Log on Retries
* Password Expiration
* Password Reuse

The following table outlines the current parameters for user access restriction.

|  |  |  |
| --- | --- | --- |
| Parameter | Default Value | Bank Value |
| Log on Timeout | 20 minutes | 20 minutes |
| Log on Retries | 3 attempts | 3 attempts |
| Password Expiration | 90 days | 90 days |
| Password Reuse | 365 days | 365 days |

For more information on resetting passwords and access restriction to the Oasis model, please refer to Resetting User Passwords in the **“MD.06 Model Solution Guides Oasis.pdf.”**

**Periodic Evaluation**

Bank User Administration is responsible for the periodic evaluation of the OASIS model. Per the Vendor Management System risk rating of the model, a periodic evaluation of user access rights must be completed every other year (biennially). In this process, Bank User Administration provides the model owner with training and a template to aid in the periodic evaluation process. Those documents must be returned to the User Administration team who will upload them to the Vendor Management System. The upload of this documentation closes out the periodic evaluation process.

**User Access Roles**

Oasis does not maintain different roles to which users are assigned. Users are individually assigned read, write, create, delete, and execute permissions to data objects or business processes, and as a result, each user maintains its own set of unique access permissions. For a full listing of all data objects, business processes, and their applicable permissions, please refer to Objects in the **“MD.06 Model Solution Guides Oasis.pdf.”**

### Production Deployment

Describe the production deployment process for the new model or changed model, including related controls.

Model Owner:

**Current Model Version**

2.5 V23

It should be noted that there is no documentation of the implementation of the current model version.

**Model Version Control**

When a new software version of OASIS is released by the vendor, ARGO, it is the responsibility of ARGO to notify the Bank. Additionally, it is the responsibility of the Fraud Strategy team to proactively reach out to ARGO for a new release when bugs in the software are found.

Please refer to **“OASIS-2-5-Release-Notes.pdf”** for the guide followed to implement the current version of the model.

**Required Testing Procedures**

It is the responsibility of ARGO to aid the IT Application Support team in implementation of the new software version. Specifically, they are responsible for ensuring that functionality is working as designed such as enhanced user interfaces and other tests including image analysis. After successful implementation, the Fraud Strategy Team will conduct User Acceptance Testing (UAT) for sign off by the Senior Management of Risk & Operations prior to implementation.

### Model Usage Controls

Describe the controls related to model usage, such as verification of inputs (including reconciliation to the general ledger or other reference data, as applicable), confirmation of successful model execution (e.g., all input records were processed, output values are within valid ranges), completion of hand-offs to downstream users of the model’s outputs, etc.

Model Owner:

The Bank has implemented processes to periodically data reconcile testing with 2 scenarios, annually.

Scenario 1 – Vision IP to OASIS model data

Data reconciliation test between VisionIP to OASIS for accuracy verification. Ensure that the data reconcile from VisionIP accurately reflects the transactions being imported into OASIS.

Scenario 2 – within OASIS tables

Data reconciliation test within OASIS tables for completeness assurance. Confirm that all relevant data imported and processed are included in the reconciliation process and that no significant transactions are omitted.

Please refer to “**Argo OASIS Data Lineage and Data Reconciliation Testing Plan**” for detail.

### Model Backup

Provide the model backup procedures, including parties involved and frequency, and describe how the model owner has determined that the procedures are functioning correctly.

Model Owner:

The bank's Network Operations Center (NOC) scheduled OASIS for both primary (PRVIPOA102W) and secondary (PRVIPOA202W) application server’s backup frequency which is once a week on Saturday holding this backup up to three weeks and once a month on the first day of the month holding this backup up to three months.

All databases are automatically backed up in accordance with the identified Disaster Recovery Plan (DRP) Tier.

OASIS is rated as Tier 2 in the banks’ business continuity tool Castellan (Riskonnect) and a Recovery Point Objective (RTO) of less than one day (up to 4 hours)

Automated scheduled Microsoft SQL database backup

Production database full and differential backup occur Monday Through Saturday at 3AM and retained for three days. Production database transaction log (incremental) backup for database in full recovery mode occur daily.

For more details regarding SQL database backup please see “**ITDBA-Automated Database Backups.pdf**”

## Contingency Plans

### Disaster Recovery Plan

Provide a reference to the disaster recovery plan or describe the plan here.

Model Owner:

A Disaster Recovery Plan (DRP) is part of the bank’s Business Continuity Office program. DRP is to guide the bank’s personnel through the steps necessary to recover the OASIS from a disruption or data center impacting incident. DRP for OASIS is stored within the bank’s business continuity tool Castellan (Riskonnect)

DRP focus areas included:

1. Recovery Team – team members (IT Application Support, IT Systems Engineering and IT DBA) are responsible for failover or recovery for Argo OASIS

2. Team Communication - methods of communication (Microsoft Team and Direct Communication via Phone)

3. Application Failover/Recovery Procedures – steps to execute for failover to Disaster Recovery (DR) in an actual recovery situation

4. Technical Validation Procedures – steps execute to validate the failover to DR worked as intended

5. Application Failback / Return Home Procedures – steps executed to failback to return to primary data center following an actual recovery situation.

The detail of DRP for OASIS can be found within **“OASIS Application Disaster Recovery Plan.pdf.”**

Lowest Requested Recovery Time Objective (RTO) – Tier 2 (Up to 1 day)

Lowest Requested Recovery Point Objective (RPO) – Tier 1 (Up to 4 hours)

### Business Continuity Plan

Provide a reference to the business continuity plan or describe the plan here. For a vendor model, provide the plan for how the model will be supported or replaced if the external vendor is no longer available to support the model or the vendor’s level of service is unsatisfactory.

Model Owner:

A Business Continuity Plan (BCP) is a strategic framework designed by the bank’s Business Continuity Office program to ensure that the bank can continue its essential function during and after a disaster or disruption. The plan includes procedures for maintaining and restoring business operations, minimizing the impact of disruptions, and ensuring the safety of bank employees.

Risk & Operations department is responsible for completing Business Impact Analysis (BIA) and then BCP in the bank’s business continuity tool Castellan (Riskonnect).

Objective to complete the BIA first to assess the potential impact of disruption on critical business functions, including financial, operational and reputation effects.

Key BIA objectives included:

Maximum Allowable Downtime (MAD) – maximum acceptable of time that a business process can be down, and the Risk & Operations department can tolerate in the event of disruption.

Application Dependencies Requested Recovery Time Objective (RTO) – maximum acceptable amount of time that a dependent application can be down following a disruption.

Application Dependencies Data Loss Tolerance Recovery Point Objective (RPO) – maximum acceptable of time of data loss measured in time that a business can tolerate in the event of a disruption. It indicates how far in time the department must recover data from backups to normal operations.

The detail of BIA for Risk & Operations department can be found within **“****Risk Operations Department BIA.pdf.”**

MAD: Tier 1 (up to 4 hours)

Requested RTO: Tier 2 (up to 1 day)

Data Loss Tolerance (RPO): Tier 1 (up to 4 hours)

BCP focus areas included:

Department Recovery Team – defines the roles and responsibilities of the recovery team members.

Department Meeting Location – alternative work location in the event of disruption.

Workaround Details for each Dependency Type – list workaround for disruption on application, location, third-party and department dependency

The detail of BCP for Risk & Operations can be found within the “**Risk Operations Department BC Plan.pdf**”

## Operating Procedures / User’s Guide

Provide step-by-step procedures for running the model, which may include:

1. Input data extraction and preparation, including data cleaning and transformations.
2. Checking the correctness of input data.
3. Setting/updating/checking model settings, assumptions, and parameter values.
4. Checking the correctness of the settings, assumptions, and parameter values.
5. Initiating the processing component of the model.
6. Checking successful completion of the model execution.
7. Extracting model outputs.
8. Checking that model outputs are valid.
9. Producing standard reports.
10. Distributing standard reports.

Note: if there is a separate operating procedural document (or User’s Guide), please list the document name below and share the document with MRM.

Model Owner:

The vendor has provided **“MD.06 Model Solution Guides Oasis.pdf”**which contain user procedures.

Refer to section 4.2.2 Data and Process Flow Diagram on the flow from source VisionIP and ingested by OASIS.

Refer to section 2.1.2.3 Data Extraction Process on the data load jobs for VisionIP and OASIS sub process.

Refer to section 1.2.6 Process Flow Diagram on OASIS alerts and handled by the model user.

# ONGOING MODEL GOVERNANCE & OUTCOME ANALYSIS

**Reference Document List**

Please list all the documents referred to in this section.

|  |  |  |
| --- | --- | --- |
| **#** | **Reference Document Name** | **High Level Description and purpose of the Document** |
| 1 | Monthly Risk Focused Meeting – Dec 23 Xceed & Oasis Slides.pdf | Evidence of metric presentation in December 2023 to senior management |
| 2 | Monthly OASIS Performance Report.pdf | Snapshot monthly OASIS model performance for May and June 2024 |
| 3 | Queue Performance Report – June 2024 | OASIS queue performance report for June 2024 |

## Ongoing Risk & Performance Monitoring Plan

**Part 1** - provide an overview of the performance monitoring process, including:

1. Frequency of monitoring activities.
2. Titles/positions of individuals/teams responsible for executing performance monitoring analyses.
3. Individuals responsible for evaluating the resulting reports and documenting conclusions.
4. Stakeholders responsible for reviewing the performance reports and initiating required actions in the event that new risks or performance weaknesses are detected.

**Part 2** - provide the details of the **ongoing risk and performance monitoring plan (together, ongoing monitoring plan)** for this model. Ongoing monitoring plans should generally cover the following two types of periodic monitoring activities:

1. Model Risk Monitoring – Reassessment of the model’s risk profile. This includes but is not limited to reassessment of model weaknesses and limitations, as well as the associated risk mitigants in light of any changes in the model use, Company’s strategy, market conditions, and regulatory environment, among other things.
2. Model Performance Monitoring – Analysis of the model’s **predictive performance** and **identification of emerging model performance weakness**.

Specifically, for Model Performance Monitoring design, it is expected that all models should have some type of outcomes-based performance monitoring process in place to evaluate whether the model is meetings its designed objectives. The Model Owners must specify, as appropriate and feasible for the specific model and its individual uses, detailed plans to monitor model performance through **some combination of the following** four methods:

* Comparison of predicted outcomes to actual values (i.e., back-testing).
* Benchmarking model outputs against comparable external data points, such as observable market information, or outputs of alternative models.
* Analysis of sensitivity of model outputs to variations in model inputs, parameters, and assumptions.
* Stress testing of model predictions to extreme changes in model inputs and assumptions.

The Model Owner should define performance thresholds which, if breached, would require the Model Owner to take corresponding actions. Performance thresholds may be set based on business unit policies or procedures, judgmentally, or based on statistical methodology utilizing model performance over the development sample. In all cases, the approach for setting performance thresholds should be established during development and documented in this section.

**Guidelines** for Risk & Performance Monitoring Plan details:

* Risk Monitoring Plan Details: The risk monitoring plan should list the internal and external factors that should be considered when evaluating model risks. This may include, as applicable:
  + - * Changes in the model use.
      * Changes in the portfolio composition or characteristics of the portfolio/asset/liability/transactions to which the model is being applied.
      * Changes in the Company's strategy.
      * Industry and economic environment changes.
      * Regulatory environment changes.
      * New regulatory findings, independent model validation findings, internal audit findings, external audit findings etc. The plan should include a list of internal and external stakeholders, groups, and committees that may identify, either directly or indirectly, model-related risks through their own “ordinary course of business” activities. It is expected that the Model Owner will establish and maintain periodic communications with these stakeholders to monitor emerging risks.
    - Performance Monitoring Plan Details: The performance monitoring plan should include:
* The source(s) of data used in the performance monitoring process.
* The list of key performance metrics that will be calculated and reported along with their technical specifications.
* Description of the performance analysis that will be performed consistent with the requirements.
* Acceptable performance thresholds for each key metric, if applicable. If a specific threshold is not defined, the Model Owners should document the justification for the lack of threshold. The Model Owners’ rationale for selecting particular performance thresholds must be adequately documented. If, as is sometimes the case, an oversight committee is required by the Business Unit/Line of Business to approve model performance thresholds, then this fact must be reflected in the monitoring plan and the Model Owners must retain evidence of such approvals. Finally, the frequency of the re-evaluation of the performance thresholds should be documented.
* Procedures for communicating and escalating performance issues to appropriate stakeholders (committees, upper management, etc.).
* Procedures for responding to performance threshold breaches.
* The list of stakeholders (individuals and committees) responsible for the review of the risk and performance reports.

Part 1 – Overview

|  |  |
| --- | --- |
| Frequency of monitoring activities (e.g., monthly, quarterly, etc.) | Monthly |
| Titles/positions of individuals/teams responsible for executing performance monitoring analyses | Fraud Strategy, in collaboration with the Enterprise Risk Management |
| Individuals responsible for evaluating the resulting reports and documenting conclusions | Fraud Strategy, in collaboration with the Enterprise Risk Management |
| Stakeholders responsible for reviewing the performance reports and initiating required actions in the event that new risks or performance weaknesses are detected | Senior Management of Risk and Operations (R&O) |

Part 2 – Risk & Performance Monitoring Plan

Model Risk Monitoring Plan Details:

Model Owner:

A check fraud model operates without a predefined threshold for reasons related to the dynamic and evolving nature of check fraud. In practice, instead of a fixed performance threshold, the model is using features with a probabilistic approach.

Risk Scoring: Each check item is assigned a score based on various features (tests)

Queues: actions are taken based on the features in combination of transactional analysis (TA) and image analysis (IA) to flag check for review

Feedback loop: The model learned form added reference image, continuously refining its image analysis assessment criteria for check stock and signature.

By foregoing a performance threshold breach, check fraud model can leverage fraud risk assessment and different risk tolerance based on the specific risk appetite and policies of the bank. Using a structured methodology based on enterprise risk management guidance, the current fraud risk assessment identified an increasing trend in external fraud risk in the industry. This approach ensure that model robust and align with the bank risk appetite while minimizing disruption to legitimate transactions.

Model Performance Monitoring Plan Details:

Model Owner:

The Bank fraud strategy team holds a monthly risk-focused meeting to review model performance and investigate fraudulent items. They analyze the Forgery Affidavit Claims Log (FAC log) which tracks all fraudulent items where the bank is liable for loss. They then research strategies to minimize loss. Refer to **“Monthly Risk Focused Meeting - Dec 23 Xceed & Oasis Slides.pdf”** for the metrics reviewed in the meeting. The key stakeholder and approval responsibilities are with Sr. Management R&O.

Fraud Strategy uses multiple reports and metrics to monitor the effectiveness of OASIS. The following section will outline the various reports that are being leveraged to monitor OASIS accordingly.

**Monthly Risk Focused Meeting OASIS Slide**

Monthly, as part of preparation for the Monthly Risk Focused Meeting, Fraud Strategy works to produce an OASIS-specific metrics slide. Slide contains Quarterly breakdown by Alerts & Losses, including the following data:

• Total # of Analyst Reviewed Checks

• Total # of Auto Closed Checks

• Total # of Checks (Auto closed + Analyst Reviewed)

• Total Amount of Bank Loss

• Total Amount of Loss Exposure

• Total Amount of Counterfeit Alert Exposure

• Total Amount of Forged Maker Alert Exposure

**Monthly OASIS Performance Report**

Fraud Strategy, in collaboration with the Enterprise Risk Management team, is defining enhanced monthly metrics for OASIS. The intent is to establish key metrics to gauge the overall performance of the OASIS system. The reporting includes the following metrics:

• Total # of Items Processed in OASIS

• Total # of Alerts Generated across all Defined Queues

• Suspect Rate as a % (detection rate)

• Total # of True Positives – Reason Code 11 (Fraud/Counterfeit tag)

• Total # of False Positives – Remaining alerts not tagged with Reason Code 11

• Total # of False Negatives – Reason Code 10 (Forgery tag)

• False Positive Rate as a %

• Precision as a % - True positive rate/total # of alerts

• Recall as a % - False negative/True positive + False negative

**Queue Performance Report**

Fraud Strategy, in collaboration with the Enterprise Risk Management team, has defined reporting to give insights into the performance of the specific queues we have defined. The reporting includes the following metrics:

• Queue Name

• Queue Criteria

• Total # of Items Processed in OASIS (monthly)

• Total # of Alerts Created by each Queue

• Suspect Rate as a % (detection rate)

• False Positive Rate as a %

• Total # of OASIS Reason Code 11 – Fraud/Counterfeit (true positive) per queue

• True Positive Rate as a %

These reports are manually refreshed by using SQL queries daily (business days). The longer-term goal is to migrate this manual reporting into a PowerBI dashboard.

## Model Approval and Change Management Process

In this section, discuss the aspects of the model approval and change management process that are specific to this model.

### Model Approval Process

Provide the names of the individuals (or a committee) involved in the approval process for this model.

Model Owner:

All changes to the OASIS model must follow the change management process outlined below. Changes are divided into technical changes and business changes. Only queue modifications are considered business changes; all other changes are considered technical changes. The change management process is as follows:

1. The Fraud Strategy team presents potential changes to the Senior Management of Risk & Operations for approval. The change request must include, at minimum a description of the change. For modifications to queues, the description of the change must be presented with forecasted changes in alert volumes and evidence of forecast testing. To conduct forecast testing, IT Application Support creates a copy of production data and loads it into a lower, non-production environment. Queue parameter changes will be made in this environment to determine effect of the change on alert quality and volume. Effects on alert quality and volume will be include in the change request.
2. Once approval is received, the Fraud Strategy either implements the change for business changes or informs IT that the change has been approved and works together with the IT team to schedule deployment for technical changes.
3. The IT team is then responsible for completing the requested technical changes in the model.
4. Once a technical change has been implemented, IT notifies the Deposit Fraud team who then performs a post-implementation validation of the change and presents the findings to the Fraud Strategy team for review. Once reviewed, the Fraud Strategy team then sends the review to IT.
5. Using the post-implementation validation results, the IT team closes out the change deployment process and updates the OASIS log of changes with the requested change.
6. All supporting artifacts and approvals must be stored electronically after the change management process has completed. Storage in E-mail is sufficient.

### Model Change Log

Provide a reference to the model Change Log. Please refer to the Bank’s 1st Line Model Risk Management Guidelines (MRM-PnP05), the MRM Procedure (MRM-PnP02), and Model Change Log Template v01.docx for detailed requirements.

Model Owner:

Adopted the MRM model change log template to capture the nature model changes, reasons for the model changes, and potential model impacts. Using this model change log template to ensure modifications are managed in a framework, minimizing risks, maintaining model integrity to align with MRM quarterly model change certification process. Added risk impact column in the log to provide transparency in the potential impacts.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Change Date** | **High-Level Description of Change** | **Change Impact** | **Category of Change** | **Responsible Party** | **Supporting Documents & Location** | **Communication and Approval** | **Additional Comments** |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

The proposed changes are prompted by changes in fraud patterns, inherent risks, regulatory requirements, business strategies or technical advancements. Each category of change will have different levels of model risk impact.

# APPENDICES

## Appendix A

List and describe references to additional model-related files that have not already been referenced in the Template.

1. OASIS-2-5\_Release Notes.pdf

Description: Information on the newest model upgrade implemented at the Bank in 2020

1. Output Review – OASIS Check Fraud Verification.pdf

Description: The Bank’s OASIS Check Fraud Verification procedures

Model Owner:

All additional model-related files are referenced in within the above sections and provided as supporting artifacts to this document.

## Appendix B

For vendor models, provide high level description of the vendor company background, qualifications, and services provided, especially relating to EWB’s purchase. In addition, please reference MRM procedure MRM-PnP04, MRM-PnP04 EWBC MRM Vendor Model Onboarding Process v01.pdf, for detailed onboarding and documentation requirements.

Model Owner:

Argo OASIS was implemented in 2007, some updates within the past few years have helped the bank capture more fraudulent activity and new enhancements that help the overall functionality.  The vendor was vetted through Third Party Risk Management (TPRM) Risk Assessment, see Vendor Management System (VMS) for responses ([VMS - Vendor Detail (ewbc.net)](https://vendormanagement.ewbc.net/Vendor/Index/3358).