A green and white logo

Description automatically generated

**Solution Design**

A black background with white text and red squares

Description automatically generated

Table of Contents

[**Introduction** 3](#_Toc150552899)

[**Summary of Existing Functionality** 3](#_Toc150552900)

[**REQUIREMENT DETAILS** 3](#_Toc150552901)

[**ASSUMPTIONS AND PREREQUISITES** 4](#_Toc150552902)

[**5.0 Possible Solution #1 – Developing an In-house AI-based solution** 6](#_Toc150552903)

[**5.1 High-Level Design** 6](#_Toc150552904)

[**5.2 Low-Level Design** 7](#_Toc150552905)

[**5.3 Impact Analysis** 7](#_Toc150552906)

[**5.4 Out of Scope** 7](#_Toc150552907)

[**5.5 Risk and Mitigation** 8](#_Toc150552908)

[**6.0 Possible Solution #2 – Outsourcing to third-party vendor** 9](#_Toc150552909)

[**6.1 High-Level Design** 9](#_Toc150552910)

[**7.0 Possible Solution #3 – Maintaining the Status Quo** 12](#_Toc150552911)

[**7.1** **High-Level Design** 12](#_Toc150552912)

[**7.2 Low-Level Design** 12](#_Toc150552913)

[**7.3 Impact Analysis** 12](#_Toc150552914)

[**7.4 Out of Scope** 12](#_Toc150552915)

[**7.5 Risk and Mitigation** 13](#_Toc150552916)

# **Introduction**

TD Bank seeks to improve its existing AML process to improve compliance following a US probe. The bank wants to ensure financial integrity and maintain strong relationship with the US government regulators. The company is focused on seeking innovative technological solutions, ensuring regulatory compliance and maintain itself as a trustworthy financial institution in North America.

# **Summary of Existing Functionality**

TD bank has existing AML procedures in place, but the existing setup has room for improvement as per US compliance standards. The AML activities in transaction monitoring, customer diligence, employee training, reporting need to comply with rules set by the Federal Reserve and Office of the Comptroller of the Currency (OCC). The bank currently uses a combination of inhouse analysis and monitoring techniques along with AML vendors but the bank struggled to invest into certain American properties and risks penalties over compliance issues.

# **REQUIREMENT DETAILS**

1. **Enhanced Transaction Monitoring:**
   * Implement advanced machine learning algorithms for real-time transaction monitoring to detect and prevent suspicious activities.
   * Predictive modeling, anomaly detection, and integration with generative AI for enhanced alert narratives.
2. **Optimized Employee Training:**
   * Develop adaptive learning modules using machine learning techniques to enhance employee proficiency in AML compliance.
   * AI-driven scenarios for diverse training, continuous learning feedback loops, and multilingual support.
3. **Behavioral Analysis and Scenario Simulation:**
   * Utilize unsupervised learning techniques for behavioral analysis for simulating diverse money laundering scenarios.
   * User profile simulation, anomaly detection, and integration with ML-based scenario models.
4. **Advanced Alert Generation with NLP:**
   * Implement natural language processing (NLP) techniques for alert generation to improve the accuracy and informativeness of alerts.
   * NLP-driven alert text analysis, generative AI for language enhancement, and real-time reporting.
5. **Continuous Improvement Mechanism:**
   * Leverage big data and cloud technologies to maintain large repositories for continuous training and improvement.
   * Reinforcement learning, ML-based feedback loops, and scalability for future customer growth.

# **ASSUMPTIONS AND PREREQUISITES**

1. **Access to Comprehensive Data:**
   * TD Bank has access to comprehensive and accurate data for implementing advanced machine learning models.
   * Establish secure data management protocols and ensure seamless integration with existing systems.
2. **Commitment to Technological Integration:**
   * TD Bank is committed to integrating advanced technologies seamlessly into its existing AML infrastructure.
   * Establish a dedicated technology integration team, foster innovation culture, and ensure robust change management practices.
3. **Regulatory Collaboration:**
   * TD Bank collaborates closely with regulatory bodies to align its AML solutions with evolving compliance requirements.
   * Strengthen partnerships with regulatory experts, engage in proactive communication, and participate in industry forums.
4. **Investment in Technology Infrastructure:**
   * TD Bank is willing to invest in advanced technology infrastructure for seamless implementation of machine learning and generative AI.
   * Conduct a comprehensive cost-benefit analysis, allocate budgets accordingly, and ensure scalability for future enhancements.

# **5.0 Possible Solution #1 – Developing an In-house AI-based solution**

# **5.1 High-Level Design**

1. **Transaction monitoring**

Use supervised learning models for prediction and classification use cases in terms of predicting, classifying, and categorizing suspicious transactions and accounts. Use a generative AI front interface to communicate with the machine learning models and create an interactive environment for AML employees to leverage.

1. **Employee Training**

Use reinforcement learning techniques to create training modules and simulations based on employee performance.  
Using generative AI to create practice datasets for employees to analyze.

1. **Behaviour Analysis**

Use unsupervised techniques to cluster customer profiles. Generative AI can be used to generate synthetic profiles for testing.

1. **Alert Generation**

Use NLP techniques for alert generation and reporting once a behaviour pattern, illegal activity has been identified.

1. **Continuous Improvement**

Leverage big data and cloud to maintain large data repositories. The idea is to continuously keep training the AI models to improve model performance and establish a feedback loop.

1. **Legal**

Significant investment needed in legal department to ensure the solution is ethical and complies with international laws including Canadian and American.

# **5.2 Low-Level Design**

* Select appropriate algorithms for the right problem statement. Predictive models such as Regression and Gradient Boosting, Support Vector Machines and other Ensemble methods for prediction use cases such as predicting the amount of money that might be laundered at a certain time from now.
* Select classification algorithms such as Decision Trees, Random Forest and Naïve Bayes to classify customer datasets and identify suspicious accounts.
* Use clustering techniques such as K-Nearest Neighbours to create different profiles and Neural Networks and Isolation Forests to detect complicated behaviour patterns.
* Use Time Series Analysis to detect trends over time.

# **5.3 Impact Analysis**

* Better detection techniques with higher accuracy eliminates dirty money and leads to financial strength in turn leading to reduced penalties and positive relations with regulators.
* First to market advantage.
* Operational efficiency and employee productivity.
* Scalability of solution to accommodate future customer growth.
* Reduced manual effort for employees so that they can work productively.

# **5.4 Out of Scope**

* Marketing activities.
* Cybersecurity practices beside the scope of AML while crucial, form a broader scope and will not be a part of the solution.
* Training modules or workshops that are not related to AML compliance.
* PR activities or regulatory advocacy.

# **5.5 Risk and Mitigation**

**Risk Factors:**

* Data privacy
* System Integration
* Compliance risk
* Resistance to Change
* Unexpected Challenges

**Mitigations:**

* Authorization and authentication techniques in place to protect sensitive data.
* Develop solutions concurrent to the existing process with a plan to integrate them gradually with agile techniques and establish version control and rollback procedures.
* Ensure the solution is up to date with new regulations with audits.
* Prepare the employees with comprehensive programs and change management strategies and a learning culture.
* Establish support teams and contingency plans with its own budget in case of unforeseen problems.

# **6.0 Possible Solution #2 – Outsourcing to third-party vendor**

# **High-Level Design**

1. **Effective Vendor selection**

Evaluate all the potential vendors carefully to make sure they are reputable, have experience with AML compliance, and follow all applicable rules and regulations. Verify that the chosen vendor has current knowledge of AML legislation and a proven track record of successfully implementing compliance.

1. **Data Security**

Usage of effective encryption procedures for all data transferred between our company and the vendor to product sensitive data.

Establish stringent access controls to restrict who within the vendor organization has access to your data and make sure that access is authorized in accordance with the least privilege principle. Establish strict regulations to give authorization to handle and view these data within the vendor side.

1. **Integration with the existing systems**

To prevent data redundancies and inconsistencies, make sure that the systems and the vendor's platform have the appropriate data field mapping.

1. **Knowledge transfer**

To make sure that the employees are proficient in using the outsourced AML solution, work with the provider to create training plans. Arrange information exchange meetings between the company and the vendor to improve communication and comprehension of changing anti-money laundering circumstances.

1. **Real time monitoring**

Usage real-time monitoring features to spot suspicious activity fast and take appropriate action along with real time transaction monitoring.

**6.2 Low-Level Design**

* Set up predefined rules and thresholds for identifying suspicious activities. Establish automatic alerting mechanisms to inform authorized staff members of possible AML violations.
* Create a dashboard for real-time visualization of monitoring results and alerts.
* To minimize duplication and inconsistencies and to guarantee accurate field mapping between systems, create a data mapping module.
* To identify and correct any inconsistencies as soon as they arise, do data validation checks during integration.
* Provide a dashboard where users may track errors and check the status of integration.
* Verify the vendor's performance history and compliance history by integrating with external databases. If the vendor's compliance status changes, set up an automated notification mechanism.
* Create a Learning Management System (LMS) to oversee employee training initiatives.
* Provide engaging online courses on AML laws, system operation, and upgrades.
  1. **Impact Analysis**
* Reduced financial risk of penalty due to AML compliance and regulatory issues.
* Enhanced reputation, increased sales, and improved business performance.
* Competitive advantage of using emerging technology solution
* New customer base due to transparency and trust.
* Scalability of solution to accommodate future customer growth.
* Reduced manual effort for employees so that the employees can work productively.
  1. **Out of Scope**
* The bank will not provide legal service and handle legal action against the AML solution.
* Customization and integration beyond the AML implementation.
* Marketing or branding activities that are not related to AML compliance.
* Training modules or workshops that are not related to AML compliance.
* Cyber security measures to enhance the solution beyond the AML activities.

**6.5 Risk and Mitigation**

**Risk Factors:**

* Data privacy
* Reliable vendor
* Integration issues with existing system
* Compliance risk

**Mitigations:**

* Implement different authorization, access controls and encryption methods should be used to ensure data privacy. Execute security testing for the solution if required.
* Choosing the reputed and experienced vendor in AML solutioning and set clear expectation in service level agreement.
* Implement the solution in phases and complete unit test at end of each phase. Roll back any functionality that violates or disrupts the existing system.
* Back up the entire data to prevent any data loss during the integration. Also, develop a business continuity plan to overcome any unexpected downtime.
* Perform regular vendor audits and ensure the legal regulations are followed.

# **7.0 Possible Solution #3 – Maintaining the Status Quo**

# **High-Level Design**

1. Continue existing AML procedures that are currently in place for customer due diligence, transaction monitoring, reporting, compliance, risk management.
2. Execute manual investigations and generation of suspicious activity reports as needed.
3. Continue using human resources and assigning tasks as they are now without making any changes.

# **7.2 Low-Level Design**

1. Conduct periodic training as usual.
2. Stick to existing compliance protocols.
3. Rely on existing data management practices for analysis.

# **7.3 Impact Analysis**

1. The technology integration will be limited and it will lead to limited AML use cases.
2. Reactive approach to incident handling which will lead to higher costs.
3. Higher penalties and limited scope of expansion in American Market.
4. Lack of scalability in the existing process.

# **7.4 Out of Scope**

* Customer Due Diligence processes.
* Automated real time transaction monitoring.
* Limited adoption of Data Analysis.

# **7.5 Risk and Mitigation**

**Risk Factors:**

* Lack of Integration
* Compliance risk
* Reactive approach
* Lack of expansion opportunities

**Mitigations:**

* Improve technology over time to improve detection of money laundering.
* Improve reporting activity to comply with regulators.
* Implement pro active techniques by using agile processes.
* Co-ordinate and comply with US government.