A green and white logo

Description automatically generated

**Solution Implementation Strategy**

A black background with white text and red squares

Description automatically generated

Table of Contents

[**Introduction** 3](#_Toc152367013)

[**Summary of Recommended Solutions** 3](#_Toc152367014)

[**Evaluation Criteria** 4](#_Toc152367015)

[**Return On Investment (ROI)** 5](#_Toc152367016)

[**Recommendation** 6](#_Toc152367017)

[**Risks** 7](#_Toc152367018)

[**Implementation Strategy** 9](#_Toc152367019)

[**Test Strategy** 15](#_Toc152367020)

# **Introduction**

In our pursuit of analyzing the challenges at TD bank and designing solutions to improve AML compliance, we have identified three possible solution plans which have been discussed in previous documents namely:  
1. In house AI solution  
2. External vendor  
3. Status Quo

There are advantages and disadvantages to each, and this document further explores and analyzes each solution, recommends the most beneficial solution, and presents ROI information for each solution, presents a risk log with mitigation steps, implementation and testing strategies.

# **Summary of Recommended Solutions**

**Solution 1:** An in-house AI solution that leverages a combination of a generative AI interface which assists AML analysts in their day-to-day, generates synthetic data, training simulations. This solution covers aspects of AML such as transaction monitoring and reporting, Suspicious activity reporting (SAR), Employee Training, Data generation and management and Compliance and regulatory reporting. Supervised and unsupervised learning models, selecting appropriate algorithms for prediction, classification, clustering, and trend analysis to enhance detection accuracy and operational efficiency.

**Solution 2:** The outsourced solution is working with a third-party vendor specializing in AML compliance. It entails careful vendor selection based on background, track record of compliance, and familiarity with AML laws. Encryption, access controls, and stringent regulations are just a few of the data security measures to ensure safe data handling and transfer. Key elements include knowledge transfer through training programs, integration with current systems, and real-time monitoring tools to spot suspicious activity quickly. Predetermined rules, automated alert systems, data mapping modules, dashboards for real-time visualization, validation checks, and performance monitoring tools are described in detail. An LMS that provides online courses on AML regulations and system operations is used to emphasize continuous learning.

**Solution 3:** Maintaining current AML procedures means carrying on with compliance, risk management, transaction monitoring, customer due diligence, and manual investigations as needed. As they currently exist, the task assignment and human resource allocation processes are not to be altered by this solution. The plan, in its entirety, calls for conducting training regularly, closely following current compliance guidelines, and basing analysis on accepted data management procedures.

# **Evaluation Criteria**

1. **Effectiveness in AML Compliance:**
   * **Solution 1:** Utilizes a combination of supervised and unsupervised learning models, NLP techniques, and continuous improvement through big data. It covers various aspects of AML compliance, including transaction monitoring, employee training, behavior analysis, alert generation, and legal considerations.
   * **Solution 2:** Outsourcing to a third-party vendor with a focus on effective vendor selection, data security, integration, and real-time monitoring.
   * **Solution 3:** Maintains existing AML procedures with limited technology integration.
2. **Cost and Resource Implications:**
   * **Solution 1:** Requires a significant investment in developing an in-house AI solution, including hiring skilled personnel, implementing infrastructure, and ongoing maintenance costs.
   * **Solution 2:** May involve initial setup costs and ongoing fees to the third-party vendor. The long-term costs depend on the terms of the agreement.
   * **Solution 3:** Likely has lower initial costs as it maintains the current procedures but may incur higher long-term costs due to limited scalability.
3. **Scalability:**
   * **Solution 1:** Designed with scalability in mind, leveraging big data and cloud solutions for continuous improvement and accommodating future customer growth.
   * **Solution 2:** Can be scalable depending on the capabilities of the chosen vendor and the scalability of their solution.
   * **Solution 3:** Limited scalability due to reliance on existing manual procedures.
4. **Integration Complexity:**
   * **Solution 1:** Involves developing and integrating various AI models, which could be complex but provides flexibility in customization.
   * **Solution 2:** Requires integration with existing systems, which may pose challenges in data mapping and system compatibility.
   * **Solution 3:** Involves continuing with existing processes, minimizing integration complexities.
5. **Risk Mitigation:**
   * **Solution 1:** Comprehensive risk analysis and mitigation strategies for data privacy, system integration, compliance, resistance to change, and unexpected challenges.
   * **Solution 2:** Mitigations include data security measures, vendor selection, integration planning, and regular audits.
   * **Solution 3:** Risks include lack of integration, compliance issues, and a reactive approach, with mitigation strategies primarily relying on continuous improvement.

**Evaluation Criteria**

1. **Flexibility and Adaptability:**
   * **Solution 1:** Offers flexibility through continuous improvement and the ability to adapt to evolving AML regulations.
   * **Solution 2:** Depends on the flexibility of the chosen vendor's solution and the ability to adapt to changing AML requirements.
   * **Solution 3:** Limited flexibility due to maintaining the status quo with existing procedures.

# **Return On Investment (ROI)**

Solution 1.

The Return on Investment (ROI) for the AI solution in Year 1 is negative at -53.70%. This negative ROI indicates that the expenses incurred surpass the generated revenue and benefits, leading to a loss. However, as the solution progresses, there's a notable improvement in the ROI. By Year 2, the ROI becomes positive at 9.78%, a modest return. This trend continues to improve in subsequent years. By the fifth year, the ROI goes up to 306.79%, showing substantial returns and profitability.

**Return On Investment (ROI)**Solution 2.

For the first year, the outsourced vendor solution's Return on Investment (ROI) is computed to be 30.88%. Year 5 of the solution continues to demonstrate growth, with a final value of 46.62%. A steady return on the investment made in the outsourced vendor solution is indicated by the ROI's upward trend over time. The steady rise in ROI indicates that the outsourced solution is profitable for the company.

## **Recommendation**

**Solution 1** is a comprehensive and strategic approach covering various aspects of AML compliance, scalability, and risk mitigation. In summary, Solution 1 not only addresses the specific criterion of effectively reducing false positives but also provides a comprehensive, scalable, and ethically sound solution for AML compliance. The in-house AI-based approach offers a strategic first-to-market advantage, positioning the organization as a leader in the market with a strong commitment to regulatory compliance and fraud prevention.

# **Risks**

1. **Data Quality and Bias:**

Risk: Inaccurate outcomes due to biased or poor-quality training data.

Mitigation: Regularly audit and cleanse data, implement bias detection, and ensure diverse representation in training data.

1. **Model Interpretability:**

Risk: Challenges in explaining complex AI model decisions.

Mitigation: Use interpretable models, implement explanation techniques, and document assumptions and limitations.

1. **Regulatory Compliance:**

Risk: Legal consequences and reputational damage from non-compliance.

Mitigation: Stay informed, adapt processes to regulations, engage legal experts, and implement compliance monitoring.

1. **Overreliance on AI:**

Risk: Potential for false positives or negatives without human oversight.

Mitigation: Balance AI with human expertise, establish a robust system for human review, and provide ongoing employee training.

1. **Operational Risks:**

Risk: Disruption due to technical failures or system downtimes.

Mitigation: Implement redundancy, conduct regular testing and maintenance, and have a comprehensive business continuity plan.

1. **Scalability Challenges:**

Risk: Struggles in processing growing data volumes in real time.

Mitigation: Design with scalability in mind, regularly evaluate and upgrade infrastructure, and implement load testing.

**Risk Log**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Risk name | Impact | Impact Level | Probability Level | Priority Level | Owner |
| Biased Data | **Inaccurate Outcomes** | **High** | **Low** | **Medium** | **Data Scientist** |
| Model Interpretability | **Challenging to Explain model** | **Low** | **Low** | **Low** | **Project Manager** |
| Operational Risk | **System failures and downtime** | **High** | **Low** | **Medium** | **DevOps Team** |
| Regulatory Compliance | **Legal Consequences** | **High** | **Medium** | **High** | **Legal Team** |
| Malfunction of AI | **Potentially false result** | **Medium** | **Low** | **Low** | **Software Team** |
| Scalability | **Misuse of AML Data** | **Low** | **Low** | **Low** | **Human Resource** |

# **Implementation Strategy**

The implementation strategy will follow an agile and iterative approach for solution development and a phased deployment approach eventually expanding into other branches.

**Phase 1: Initial Review and Planning**

**AML Aspects Validation:**

Initially, the critical aspects of AML solutions that are necessary to improve compliance at the bank are validated. Past Compliance records with recurrent issues and shortcomings.

The current performance is evaluated against the existing AML regulations. Transaction monitoring systems and their performance are evaluated to assess their effectiveness and identify inefficiencies in detecting and reporting transactions.

**Branch Risk Assessment:**

Analyzing historical AML performance metrics for each branch to identify high performers and areas needing improvement. Assessing risk factors associated with branches, such as location, client profile, transaction volume, and historical compliance issues. Strategic Branch Selection to select a subset of branches that have demonstrated strong AML performance and those identified as high-risk due to various factors (clientele, location, etc.).

Establishing a priority order based on the level of risk, compliance history, and strategic importance of branches in the network.

**Version Control Implementation Plan:**

**Versioning Framework**  
Establish a versioning system to track changes, enhancements, and updates across the deployment lifecycle.  
**Change Management Strategy**  
Define protocols for managing changes, ensuring traceability, and facilitating efficient rollback procedures if necessary.  
**Collaboration Framework**: Establish a framework for collaboration among development, testing, and deployment teams to maintain version control standards.  
**Documentation Protocol**: Set up documentation practices to capture changes, iterations, and enhancements during each phase.

**Implementation Strategy**

**Phase 2: Infrastructure Setup**

This phase will require collaboration between the Development team, Testing team and DevOps team. Security team will be consulted to identify vulnerabilities.

**Cloud-Based Infrastructure:**

Carefully choosing the cloud service provider (e.g., Azure, AWS) based on security, scalability, compliance, and compatibility with the bank's systems. Integrating the solution with the bank's databases to ensure seamless data access and transaction monitoring. Designing the infrastructure to accommodate potential future growth and increased data processing demands. Implementing robust security protocols to safeguard sensitive data and comply with industry standards and regulations.

**AI Solution Architecture:**

Create a scalable, adaptable, and efficient architectural framework to support the AI-driven components and their integration with existing systems. Design the structure and features of the generative AI interface, ensuring it covers essential AML aspects and supports interactive analysis and training. Define integration protocols and data pipeline to ensure smooth communication between the AI solution, generative AI interface, and existing bank database systems.

**Synthetic Data Generation:**

Developing AI models capable of generating synthetic data mimicking real-world AML scenarios and transaction patterns.Creating synthetic datasets representing various AML scenarios enables comprehensive training and analysis simulations.Setting up virtual testing environments to validate the effectiveness of the generated synthetic data.

**Implementation Strategy**

**Phase 3: Agile Development and Iterative Enhancement**

**Agile Development Implementation**Breaking down solution development into iterative sprints for continuous improvement. Biweekly sprints on JIRA, Trello and Microsoft Planner. Knowledge base implementation on SharePoint.Forming dedicated teams comprising Software Developers, Testers, Data Scientists, Machine Learning Engineers, Analysts, and Security Specialists.Embracing adaptability to incorporate feedback and incremental improvements after each sprint.

**Generative AI Interface Development**Building core features within the interface focusing on real-time transaction monitoring, behavior analysis, and alert generation.Designing an AI assistant tool for assisting employees in monitoring and flagging transactions and automating certain manual work. The interface will then interact with other analytical models depending on the use cases.

**Employee Training Tools Development:**Training Module Creation: Developing modules covering AML regulations, software utilization, and scenario-based simulations for training purposes.

Interactive Learning via simulations: Designing tools for employees to practice identifying suspicious activities using simulated scenarios.

Training Staff will ensure staff ability is elevated to expected newer standards.

**Phase 4: Gradual Rollout and Continuous Improvement**Deploying the solution in selected branches based on priority and readiness. Upon successful implementation and performance evaluation, the solution will be gradually distributed across local, state, and national regions. Coordinating deployment schedules, resources, and teams for smooth implementation. Conducting on-site training sessions for branch employees on best practices and how to integrate the new AI system into their workflow.

Providing ongoing support and assistance to branches during initial usage phases. Gathering feedback from branches, end-users, and AML experts to identify areas for improvement.

Analyzing feedback to prioritize enhancements and iterate on existing functionalities. Implementing continuous enhancements based on feedback to improve solution effectiveness.

**Implementation Strategy**

**Backout Strategy**

Trigger Points Identification:

* **Performance Failure**
* **Security Breach**
* **Regulatory Non-Compliance**
* **Operational Disruption**.

Backout Procedures:

1. **Immediate Halt and Assessment**:

Stop deployment activities immediately upon trigger point identification. Convene a designated team of experts for assessment and analysis.

1. **Issue Isolation and Rollback**: Isolate and analyze the issue causing the trigger point. Execute a structured rollback plan to revert to the stable pre-deployment state.
2. **Communication and Reporting**: Notify stakeholders about the backout decision and its reasons. Prepare detailed incident reports highlighting causes and steps taken.

Testing and Validation:

1. **Post-Backout Validation**: Rigorous testing to ensure the system returns to a stable state. Validate critical functionalities impacted by the backout.
2. **Learning and Improvement**: Analyze root causes and derive lessons for future improvements. Implement enhancements to prevent similar issues in subsequent deployments.

**Implementation Strategy**

**Backout Strategy**

Revision:

1. **Decision-Making**: Assess if issues are resolvable or if deployment needs delay or reconsideration. Decide on continuation with revised plans or postponement based on assessment.
2. **Adjusted Deployment Plan**: Revise deployment plans incorporating lessons learned and issue resolutions. Implement necessary adjustments for more successful future deployment attempts.

**Key Considerations:**

* **Timely Decision-Making**: Promptly decide upon trigger point detection to minimize impacts.
* **Clear Communication**: Maintain transparent communication among stakeholders throughout the backout process.
* **Documentation**: Thoroughly document all steps, decisions, and outcomes for reference and improvement.

**Summary Of Deployment**

|  |  |  |
| --- | --- | --- |
| Phase | Deliverable | Responsibility |
| 1 | AML Aspects Review Report | AML Team |
| 1 | Branch Risk Assessment Report | Risk Analysts |
| 1 | Version Control Plan | DevOps, Software Dev Team |
| 2 | Cloud-Based Infrastructure Setup | DevOps, IT Security |
| 2 | AI Solution Architecture Design and Execution | AI Architects, AI Team, Software Dev Team |
| 2 | Synthetic Data Generation | AI Team, Analysts |
| 3 | Agile Development Plan | Project Manager |
| 3 | Generative AI Interface Development | AI Team, UI/UX, Software Dev Team |
| 3 | Employee Training Tools Development | Training Team, Analysts, Software Dev Team |
| 4 | Initial Branch Deployment | Deployment Team |
| 4 | Feedback Integration Report | Project Manager |

# **Test Strategy**

**Revision History**

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Author | Description |
| 1-Dec-2023 | Version 1.0 | Insights Consulting |  |
|  |  |  |  |

**Scope**

|  |  |  |
| --- | --- | --- |
| Document | Reviewed by | Approved by |
| Test Strategy Document | Business Team | Project Manager/ Delivery Head/Business Analyst |
| Development Team |
| Functional Testing Team |
| Non-functional Testing Team |
| Business Continuity Team |

Testing activities included within the scope of this project:

* Unit Testing
* Integration Testing
* System Testing
* Performance Testing
* Security Testing
* Disaster Recovery Testing
* User Acceptance Testing

**Test Approach**

The project will follow an agile methodology approach for testing. Each module will be developed and tested in sprints of 2 weeks. The sequence of testing will be sequential order as mentioned in the scope of this document.

|  |  |  |
| --- | --- | --- |
| Roles | Responsibility | Test to be completed |
| Developer | Develop, test, and optimize code for all modules | Unit Testing |
| Functional Tester | Develop the test cases, test scripts, and prepare test data for SIT environment. | Integration, System, User Acceptance testing |
| Non-functional Tester | Develop test scripts, load distribution scenarios and test data for pre-production environment. | Performance, Security |

**Test Strategy**

**Approach and Tools**:

The project will follow automation testing methods for both functional and non-functional testing. Azure DevOps will be used for agile project management.

**Defect Tracking:**

* Any defects or bugs identified in the testing process should be addressed as a user story and assigned to the development team through the defect tracking system.
* After the new code deployment, the testing team will execute testing to ensure the resolution.
* Each testing phase will have a separate signoff detailing the features or components tested, bugs reported, optimizations.

**Test Environment**

The solution will be hosted in Azure cloud environment as it ensures high security and speed. Also considering the future demands and scalability, Azure is one of the best options. Backup for test data will be taken after each test phase and pushed to the cloud for restoration in case of data corruption. The testing environments for each of the tests are listed below:

Functional Testing: SIT (System integration testing) environment.

Performance Testing: Pre-production environment, i.e., copy of production environment.

Security Testing: Pre-production environment, i.e., copy of production environment.

UAT Testing: Production environment.

**Testing Tools**

Tools required for testing are listed below:

* Functional testing: Selenium
* Non-functional testing: LoadRunner, HP Performance Center, Wireshark

**Test Strategy**

**Release Control**

**Objective**

Ensure systematic release processes, including version history, for effective test execution and continuous enhancement.

**Major Activities**

1. **Bi-Weekly Releases**:

* Schedule releases every two weeks, including new features, enhancements, or bug fixes.
* Hold release planning meetings to prioritize and plan upcoming features.

1. **Versioning**

* MAJOR version for API changes that are incompatible.
* MINOR version for adding features while remaining backward compatible.
* PATCH version for bug fixes that are backward compatible.

1. **Change History:**

* For each release, keep a detailed change log.
* Include new features, enhancements, bug fixes, and other changes.

1. **Execution of Tests:**

* For each release, run the entire test suite.
* Include regression testing to ensure that existing functionality is not jeopardized.

**Version History**

|  |  |
| --- | --- |
| **Version** | **Change** |
| 1.0.0 | Initial Release |
| 1.1.0 | Add real-time transaction monitoring |
|  | Integrated generative AI and ML algorithms |
| 1.1.1 | Bug fix: data breach issues |
| 1.2.0 | Enhancement for user training |
| 1.2.1 | Bug fix: AI performance issues |
| 1.3.0 | Introduction to personalized training |
|  | Recent training modules updating. |

**Test Strategy**

**Review and Approvals**

|  |  |  |  |
| --- | --- | --- | --- |
| **Activity** | **Reviewer** | **Approver** | **Comments** |
| Test Strategy Document Review | QA Lead, Project Manager, Business Analyst | Project Manager, Stakeholders | Ensure alignment with project goals and requirements |
| Test Approach Review | QA Lead, Test Engineers | Project Manager, Business Analyst | Validate testing process, levels, and approach |
| Test Environment Review | QA Lead, Test Engineers | Project Manager, IT Team | Confirm environment readiness and data backup strategy |
| Testing Tools Review | QA Lead, Automation Engineers | Project Manager, IT Team | Assess the suitability of testing tools and automation approach |
| Release Control Review | QA Lead, Project Manager | Project Manager, Stakeholders | Verify the release plan, versioning, and change log |
| Risk Analysis Review | QA Lead, Project Manager | Project Manager | Evaluate identified risks, mitigation plans, and contingency measures |
| Document Approval | QA Lead, Project Manager | Project Manager, Stakeholders | Confirm acceptance and approval of the complete test strategy |

**Exit Criteria**

* All the functional test executions are completed successfully.
* All critical defects have been fixed and verified.
* All the performance requirements, such as response time, scalability, etc., are satisfied.
* All the security test cases have been tested, and the issues identified are fixed.
* Risk mitigations are identified, and business continuity measures are planned.
* All the test artifacts, such as test plans, test cases, and test reports, have been reviewed and signed off.
* All the stakeholders have reviewed and approved the test results.