A green and white logo

Description automatically generated

Toronto-Dominion Bank

**Final Project Report**

Presented By

A black background with white text and red squares

Description automatically generated

Table of Contents

[List of team members and responsibilities 4](#_Toc153231244)

[Executive Summary 4](#_Toc153231245)

[Overview of the selected company 5](#_Toc153231246)

[Organizational Chart: 7](#_Toc153231247)

[Competitive analysis findings 7](#_Toc153231248)

[Description of the problem to be solved 9](#_Toc153231249)

[Business Requirements 9](#_Toc153231250)

[As-is process flow: 10](#_Toc153231251)

[Transition Requirements 12](#_Toc153231252)

[Plan: 13](#_Toc153231253)

[Solution requirements (functional and non-functional) 14](#_Toc153231254)

[Functional Requirements 14](#_Toc153231255)

[Non-Functional Requirements 16](#_Toc153231256)

[Potential solution options (incl “do nothing”) 17](#_Toc153231257)

[ROI: 20](#_Toc153231258)

[Solution Recommendation (the “why”) 24](#_Toc153231259)

[An in-house AI solution 24](#_Toc153231260)

[Database design: 25](#_Toc153231261)

[Project selected: 25](#_Toc153231262)

[Evaluation criteria: 26](#_Toc153231263)

[Risks Log: 27](#_Toc153231264)

[To-be process flow: 28](#_Toc153231265)

[Implementation/deployment Strategy/approach: 30](#_Toc153231266)

[Phase 1: Initial Review and Planning 30](#_Toc153231267)

[Phase 2: Infrastructure Setup 31](#_Toc153231268)

[Phase 3: Agile Development and Iterative Enhancement 32](#_Toc153231269)

[Phase 4: Gradual Rollout and Continuous Improvement 32](#_Toc153231270)

[Test Strategy 35](#_Toc153231271)

[Revision History 35](#_Toc153231272)

[Document Approval 35](#_Toc153231273)

[Scope 35](#_Toc153231274)

[Types of Testing 35](#_Toc153231275)

[Test Approach 36](#_Toc153231276)

[Roles and Responsibilities 36](#_Toc153231277)

[Approach and Tools 36](#_Toc153231278)

[Defect Tracking 36](#_Toc153231279)

[Test Environment 37](#_Toc153231280)

[Release Control 37](#_Toc153231281)

[Risk Analysis 38](#_Toc153231282)

[Review and Approvals 39](#_Toc153231283)

[Exit Criteria 39](#_Toc153231284)

[APA References 40](#_Toc153231285)

# **List of team members and responsibilities**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Task | Responsible | Accountable | Consulted | Informed |
| Process Flow | Aiswarya, Ashna, Shashwat | Hardik | Hardik | TD |
| Updated RACI | Hardik | Hardik | Ashna | TD |
| Process Summary | Hardik | Hardik | Hardik | TD |
| SRS | Aiswarya, Saurav | Hardik | Ashna | TD |
| Feasibility Analysis | Ashna, Saurav | Hardik | Aiswarya | TD |
| Data Solution | Hardik, Shashwat | Hardik | Ashna | TD |
| Cost Benefit Analysis | Hardik, Ashna | Hardik | Aiswarya | TD |

# **Executive Summary**

Insights Consulting is providing this Request for Information (RFI) document to gain more information to improve the bank’s existing Anti Money Laundering (AML) systems in light of the recent compliance difficulties in the United States.

TD Bank is one of the most successful financial institutions with a global presence. TD has always been committed to providing excellent banking services to ensure customer satisfaction and compliance with regulatory requirements. However, the bank’s recent investments in Canadian housing, failed merger with First Horizon, and the acquisition of American firm Charles Schwab led to the bank becoming the most targeted by short sellers in the stock market. The Office of the Comptroller of the Currency (OCC) and the Federal Reserve have raised an issue with how the bank handles unusual transactions, account handling by front staff, and reporting fraudulent activities. These concerns led to the failure of the merger with First Horizon. Questions have been raised about AML compliance within the bank. Critics have drawn comparisons with some practices raised a few years ago with one of the bank’s competitors in the US, where fake accounts were created, and employees were incentivized to open these accounts and opt for overdraft protection.  
  
This RFI form aims to elicit information that can help Insights Consulting gain a thorough understanding of the bank’s existing systems and processes and how it can aid the bank in overhauling its AML processes to improve compliance with regulations.

The proposed solution will focus on detecting money laundering activities, reporting suspicious transactions, documentation, staff training, ethical behavior, customer trust, and staying committed to the bank’s mission.

# **Overview of the selected company**

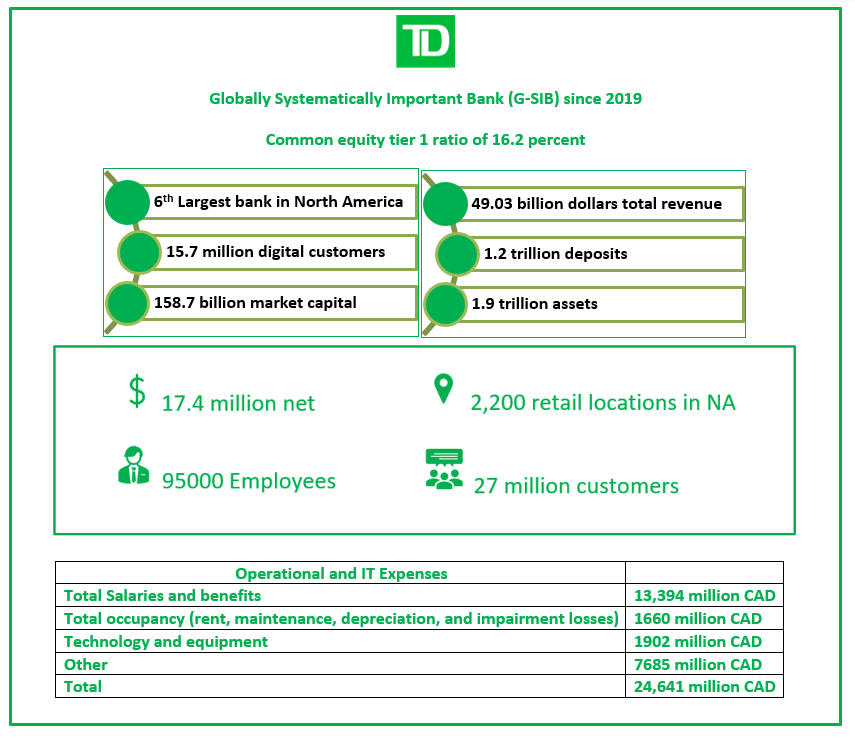
TD (Toronto-Dominion) is a leading financial institution in Canada that has been operating since 1855. TD has become a global force and provides services to a large customer base. Apart from local operations in Canada, TD is one of the few Canadian banks that has expanded into the United States market and has a significant presence. Combined success in both economies has led to the bank becoming the 6th largest bank in North America.

The bank believes in providing exceptional customer service with a proven business model, helping customers thrive in the modern world. The bank’s business model focuses on consistent growth and follows a strong risk culture. The bank wants to shape the digital future of the financial landscape—the vision – to be the better bank. The purpose is to enrich the lives of customers, communities, and colleagues. (TD, n.d.)

TD’s corporate governance (TD, 2023) structure:

A diagram of a company with University of North Texas in the background

Description automatically generated



# **Organizational Chart:**

A computer screen shot of a company structure

Description automatically generated

# **Competitive analysis findings**

**Strengths:**

1. **Financial Stability:** TD Bank is recognized as one of the financially stable banks in North America, contributing to a strong foundation for operations and growth.
2. **Diverse Financial Services:** TD Bank offers a wide range of financial services, providing customers with various options for banking, investment, and wealth management needs.
3. **Large Customer Base:** The bank is accessible to a large customer base, with over 27 million customers, indicating a significant market presence and potential for cross-selling.
4. **Digital Banking Platforms:** TD Bank has strong digital banking platforms, aligning with the trend towards digital transformation in the banking industry.
5. **Reputation:** The bank has a strong reputation, being recognized as the 'best Canadian bank,' which can positively influence customer trust and loyalty.

**Weaknesses:**

1. **Customer Service Concerns:** Issues with improper customer service could impact customer satisfaction and loyalty, highlighting an area for improvement.
2. **Limited Global Presence:** TD Bank lacks a proper global presence, which may limit its reach compared to competitors with more extensive international networks.
3. **Technology Investment Needs:** The need for increased investment in new technologies suggests potential challenges in keeping up with advancements and maintaining a competitive edge.
4. **Cash Flow Problems:** Identified cash flow problems can pose risks to the bank's financial health and ability to invest in growth opportunities.

**Opportunities:**

1. **Digital Mediums:** TD Bank can leverage digital mediums to attract new customers and enhance its market share by focusing on digital acquisition and engagement strategies.
2. **Wealth and Retirement Planning Services:** The opportunity to expand into wealth and retirement planning services aligns with evolving customer needs and provides avenues for revenue diversification.
3. **Financial Technology Investments:** Investing in financial technologies can attract a larger customer base and ensure the bank remains competitive in the rapidly evolving fintech landscape.
4. **Global Expansion:** Exploring opportunities for global expansion can help TD Bank tap into new markets and diversify its revenue streams.
5. **ESG Focus:** The focus on Environmental, Social, and Governance (ESG) issues allows TD Bank to concentrate on sustainable financial products, catering to the growing demand for responsible banking.

**Threats:**

1. **Increasing Competition:** The banking industry faces increasing competition, requiring TD Bank to continuously innovate and differentiate itself to maintain or improve market share.
2. **Regulatory Compliance Challenges:** Stringent rules and regulations pose challenges to remaining profitable while ensuring compliance, requiring ongoing efforts to navigate the regulatory landscape.
3. **Currency Fluctuation Risks:** As a bank with international operations, currency fluctuation issues can impact TD Bank's financial performance and risk management strategies.
4. **Technological Advancements by Competitors:** Competitors with advanced features and emerging technologies may attract customers seeking innovative and convenient banking solutions.

In summary, TD Bank's strengths lie in its financial stability, diverse services, and large customer base, while opportunities exist in digital transformation, wealth management, and global expansion. However, addressing weaknesses such as customer service concerns and the need for technology investment is crucial to mitigating threats and staying competitive in the dynamic banking industry.

# **Description of the problem to be solved**

TD bank in 2023 possesses the highest short interest among stocks as of April and it is due to a variety of reasons. Firstly, because of the bank’s acquisition of American firm Charles Schwab and its failures in the market lately and its failed acquisition of another firm called First Horizons. Second reason is since being a Canadian bank, TD has a lot of investment in Canadian Real Estate which is going through a difficult period as of now, and short sellers predict TD’s market strength will decrease as a result. The third and most important reason that concerns this project is that the US Department of Justice has ordered a probe into the Anti Money Laundering Practices at TD, and it faces several fines for failing to live up to regulations set by the US government. This has resulted in a loss of faith among many stockholders. The company is in dire need to re-evaluate and reform its AML compliance program.

The planned acquisition of First Horizon Bank faced regulatory hurdles due to concerns over TD Bank's anti-money laundering practices. Regulators, including the Office of the Comptroller of the Currency (OCC) and the Federal Reserve, have expressed worries about TD Bank's handling of suspicious transactions and delays in reporting such activities and the DOJ has ordered a probe. A major concern has also been around accusations around account practices like Wells Fargo in 2016 (Paymnts, 2022), with customer facing workers incentivized to open customer accounts and opt into Overdraft protection with threats of losing employment otherwise. This is a major concern that needs internal investigation into employee training with respect to AML compliance laws. Despite TD Bank's assertions of actively fortifying risk management, the uncertainty surrounding regulatory approval prompted the mutual termination of the merger agreement. This development represents a setback for TD Bank's expansion plans in the Southeastern United States and highlights the regulatory scrutiny emphasizing the need to improve AML compliance at TD to avoid paying any further penalties and to ethically uphold the highest standards of regulatory compliance, communication, and a healthy relationship with American regulators.

# **Business Requirements**

The business requires an Anti-Money Laundering (AML) solution which can monitor the bank transactions and promptly detect any suspicious activities.

The suspicious activity should be triggered and alerted to the concerned team within the quickest time span for further analysis and mitigations.

The solution should be able to handle any future increase in transaction volumes without any compromise in the speed and accuracy of suspicious activity detection.

The solution should completely adhere to the U.S governments AML rules and regulations and update the compliance policies in case of any amendments. The solutions should be transparent and collaborative with law enforcement, regulatory bodies.

The business also focuses on the importance of employee training of money laundering threats; thus, the solution should also offer comprehensive training programs for the TD bank employees.

# **As-is process flow:**

  
  
As-Is Process Summary

**Statement**

This as-is process flow depicts the current Anti-Money Laundering Process at TD. It complies with to the concepts outlined in the bank's AML statement. TD is dedicated to adhering to economic sanctions laws and regulations. (TD, 2020)

**Policies for Leadership**

The policies and procedures are developed after an examination of the bank's processes and their interdependence. These policies are documented. It is mandatory to educate all levels of the organization about AML awareness.

**Customer Onboarding**

Employees are trained to verify customer information and KYC.

**Processing of Transactions**

If an account is compromised, it must be monitored further, and data is compared against watchlists. If the customer is verified, their records are maintained and updated as usual, and their transactions continue as usual. If any transactions are flagged during monitoring, they will be compared to the watchlist.

**Reporting**

If suspicious activity is discovered, a risk assessment is performed, and higher authorities are notified. If such activities are not discovered or are reduced, evaluation studies to investigate the effectiveness of the AML program are required.

Legal and compliance, customer-facing staff, regional management, and risk management teams are the most affected business areas. Improving the AML process at TD to improve compliance in the US will necessitate functional changes in some or all of these areas.

# **Transition Requirements**

**Current State:**

TD Bank’s market capitalization has reduced for the last two years (fig 1). TD’s stock happens to be the most shorted as of April 2023, partly due to its investments in Charles Schwab, an American firm, a failed acquisition of another American company called First Horizon, and investments tied to Canadian Housing, which is presently expected to hit a downturn. The US Department of Justice has ordered a probe into the bank’s Anti Money Laundering (AML) Compliance Programs. This is concerning since TD Bank has a huge presence in the United States out of all Canadian Banks. (fig 2)

Net income as of 2023 is 10.6 billion dollars, dropped by 5.71 percent from the previous year ↓

TD has an AML compliance team responsible for identifying trends, being aware of new legislation, and ensuring compliance with regulatory requirements. However, there is a growing need to improve the current methods for detecting money laundering, such as using modern technology and infrastructure. Recent developments in technology have made AI tools accessible to everyone, and with it come both good and bad consequences. So, it is also important that companies stay up to date as well.

**Future State:**

AI technology, including Machine learning and predictive analysis, Deep Learning, Neural Networks, Generative AI, and Large Language Models, has improved the probability of detecting fraud and money laundering. Advanced techniques help discover criminal behavior at a larger rate, which might otherwise go undetected when using old-school conventional methods.

Higher detection rate of money laundering cases, frauds, and identity theft. This reduces the fines and penalties the bank would have to pay.

Reduce corporate malfeasance, thus making TD financially stronger as a business.

Ensures the bank’s AML arm stays compliant with regulations set by the US government.

**Transitional State:**

While TD, as a bank, has been strong for years, it has competed and fallen short against one of its major competitors. The advantage, however, is that they have a huge presence in the US. The high number of short positions is not just based on the investments in the US market but also because of the bank's ties to the Canadian housing market. So, it is crucial that the bank ensures they have a diversified portfolio, and one way to make sure is to increase their US presence in the form of growing their business, which is something that TD is already doing but, in the process, their AML compliance processes leave a lot be desired. This gap needs to be addressed using modern tools and techniques.

Research: Finding out what is the best way to go about in terms of improving AML processes.

Is a high-tech solution necessary to begin with? Market research and industry trends would say yes.

There are various methods and techniques to solve this problem that need to be explored. Some involve traditional statistical techniques and manpower, technology-based solutions involving AML software programs by third-party vendors, in-house AI solutions, or outsource work to develop an AI product to detect money laundering or a combination of both. The existing AML team needs to be provided with more training and resources to better identify and distinguish individual cases. The transition involves looking inward into past data and past company policies, as well as keeping up with US regulations. The project leans heavily and favors the use of AI in detecting money laundering practices.

## **Plan:**

1. Analyzing current processes

2. Review Regulations

3. Risk Analysis

4. Analyze Customer Behaviour

5. Provide AML training to internal employees

6. Implement advanced AML technology (Generative AI, Machine Learning, AML vendors, or alternatives)

7. Maintain documentation

8. Vendor assessment (if applicable)

9. Internal Audits

10. Co-operation with US regulators

11. Continually review and improve processes (flexibility)

# **Solution requirements (functional and non-functional)**

## **Functional Requirements**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Req. ID | Req. Description | Priority | Dependencies | Acceptance Criteria |
| FR01 | The system shall continuously monitor real-time transactions and detect any suspicious activities, triggering immediate alerts or reports. | High | None | The system must detect and alert on any suspicious transaction within 5 seconds. |
| FR02 | The system shall categorize the money laundering activity based on its severity and priority | High | None | The system must categorize suspicious activities in a structured manner for further action. |
| FR03 | The system shall integrate with the current system to access customer transaction and data. | High | None | The system must seamlessly integrate with the existing bank systems without disrupting operations. |
| FR04 | The system shall generate a detailed report on identified suspicious transactions and facilitate sharing with the desired team for further analysis. | High | None | The system must generate and share a detailed activity report when suspicious activity is confirmed. |
| FR05 | The system shall implement data breach protection measures to safeguard sensitive information. | High | FR03 | The system must have safeguards to prevent data breaches |
| FR06 | The system shall feature a generative AI interface with machine learning algorithms trained on company-specific data in detecting potential money laundering activities. | Medium | FR03 | The system should incorporate generative AI and ML models using relevant company data. |
| FR07 | The system shall support comprehensive training modules for staff based on the designation or area of expertise. | High | None | The system should identify employee roles and provide role-specific training. |
| FR08 | They system shall dynamically update training modules based on recent money laundering activity to update employees about emerging threats. | Medium | FR07 | The system should update training materials when new money laundering activity means are identified |
| FR09 | The system shall assess employee knowledge with assessments, quizzes, and simulations. | Medium | FR07 | The system should evaluate employee knowledge through assessments, quizzes, and simulations based on the training. |
| FR10 | The system shall maintain records of employee training programs and assessment scores to evaluate their proficiency. | Low | None | The system must keep records of training programs and associated assessment scores |
| FR11 | The system shall ensure strict adherence to AML laws and regulations in the U.S. | High | None | The training modules must fully comply with AML laws and regulations in the U.S. |
| FR12 | The system shall external collaboration with AML vendors considering the performance and security factors. | High | FR11 | The bank must select an AML vendor known for its success and reliability. |
| FR13 | The system shall be scalable to handle increasing volume without any performance issues. | High | None | The system must be scalable to accommodate growing transaction volumes. |
| FR14 | The system shall require the vendor to maintain compliance, audit trails and risk assessments. | Medium | FR04 | The selected AML vendor must maintain audit trails for compliance and accountability. |

## **Non-Functional Requirements**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Req. ID | Req. Description | Priority | Dependencies | Acceptance Criteria |
| INFR01 | The system shall alert any suspicious activity within 1 seconds | High | FR01 | The system should promptly alert of any suspicious activity within 1 seconds. |
| INFR02 | The system shall retrieve the customer details of suspicious activity within 10 seconds | Medium | FR01 | The system should access and provide customer details for suspicious activity within 10 seconds. |
| INFR03 | The system shall be accessible for all employees including those with disabilities as per the WCAG 2.1 standard. | Low | None | The solution must adhere to WCAG 2.1 standards to ensure accessibility for employees with disabilities. |
| INFR04 | The system shall include the multilingual training modules with subtitles, transcripts. | Medium | None | The training modules should be available in multiple languages with subtitles. |
| INFR05 | The system shall be available 24/7 with a vendor support. | High | FR12 | The selected AML vendor should provide 24/7 support for assistance and issue resolution. |

# **Potential solution options (incl “do nothing”)**

**Solution 1: In-House AI Solution**

Implementation Roadmap:

Develop a phased implementation plan to roll out the generative AI interface and synthetic data generation tools.

Start with transaction monitoring and reporting, then expand to suspicious activity reporting (SAR) and employee training.

Regularly update and refine the AI models based on feedback and emerging trends.

Technology Stack:

Select AI frameworks such as TensorFlow or PyTorch for model development.

Integrate the solution with existing AML systems for a seamless workflow.

Implement a robust data management system for handling synthetic data and training simulations.

Compliance Enhancement:

Ensure that AI models adhere to regulatory requirements and compliance standards.

Conduct periodic audits to validate the accuracy and fairness of the AI models.

Keep the AML analysts updated with continuous training on the evolving landscape of AML regulations.

**Solution 2: Outsourced AML Compliance**

Vendor Selection Criteria:

Establish a comprehensive checklist for selecting a third-party vendor, considering their compliance track record, experience, and security measures.

Implement a rigorous due diligence process to ensure the chosen vendor aligns with TD Bank's AML requirements.

Integration and Training:

Develop a structured knowledge transfer program to seamlessly integrate the outsourced solution with existing systems.

Implement real-time monitoring tools and dashboards for quick identification of suspicious activities.

Continuous Improvement:

Establish regular communication channels with the vendor to address any issues promptly.

Periodically review and update security measures to align with the evolving threat landscape.

Implement a feedback loop for TD Bank staff to provide insights into the effectiveness of the outsourced solution.

**Solution 3: Maintaining Current AML Procedures**

Continuous Training and Development:

Institute a regular training schedule for AML analysts to stay updated on the latest compliance guidelines and regulatory changes.

Utilize a Learning Management System (LMS) to provide online courses, ensuring continuous learning for staff.

Enhanced Manual Investigation Processes:

Invest in advanced tools and technologies to support manual investigations, improving efficiency and accuracy.

Implement AI-assisted tools for data analysis to complement manual efforts.

Automation for Routine Tasks:

Identify routine and repetitive AML tasks suitable for automation to enhance operational efficiency.

Implement automated reporting tools for compliance and regulatory reporting.

Regular Compliance Audits:

Conduct regular internal audits to ensure adherence to AML procedures and identify areas for improvement.

Collaborate with external auditors to validate the effectiveness of existing processes.

Investment in Technology:

Explore and invest in new technologies that can augment current AML procedures, such as advanced analytics and machine learning models for improved risk assessment.

Adaptive Risk Management:

Develop a dynamic risk management strategy that adapts to changing business environments and emerging AML risks.

Implement a feedback loop to gather insights from analysts for continuous improvement of AML processes.

Ultimately, the choice between these options would depend on TD Bank's specific needs, resources, and strategic goals. A combination of elements from each solution might also be considered to create a tailored approach that best suits the bank's AML compliance requirements.

# **ROI:**

Return of investment(ROI) for the solution 1 is as follows:

**Income Tax Rate**: 23.48%

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **Year 1** | **Year 2** | **Year 3** | **Year 4** | **Year 5** |
| **Net Gain** |  |  |  |  |  |
| Reduction in Fines / Penalties | 3,000,000 | 9,000,000 | 12,000,000 | 18,000,000 | 27,000,000 |
| Financial loss prevention | 2,500,000 | 5,000,000 | 9,500,000 | 15,000,000 | 24,500,000 |
| New customer base | 500,000 | 1,000,000 | 1,500,000 | 2,000,000 | 2,500,000 |
| **Total Revenue** | 6,000,000 | 15,000,000 | 23,000,000 | 35,000,000 | 54,000,000 |
| **Expense** |  | | | | |
| Development Team | 8,000,000 | 4,000,000 | 4,000,000 | 3,600,000 | 2,700,000 |
| Maintenance & Support | 3,500,000 | 2,600,000 | 1,700,000 | 1,500,000 | 1,500,000 |
| Technology and Infrastructure | 200,000 | 250,000 | 300,000 | 350,000 | 400,000 |
| Data security | 500,000 | 600,000 | 700,000 | 800,000 | 900,000 |
| Integration | 500,000 | 350,000 | 250,000 | 250,000 | 100,000 |
| Audit | 300,000 | 450,000 | 600,000 | 650,000 | 700,000 |
| Risk management | 1,000,000 | 800,000 | 770,000 | 690,000 | 630,000 |
| Training | 120,000 | 50,000 | 50,000 | 50,000 | 50,000 |
| Contingency | 5,000,000 | 3,000,000 | 2,000,000 | 2,000,000 | 2,000,000 |
| Legal | 1,000,000 | 1,200,000 | 1,400,000 | 1,600,000 | 1,800,000 |
| **Total Expense** | 20,120,000 | 13,300,000 | 11,770,000 | 11,490,000 | 10,780,000 |
|  | | | | | |
| **Gross Profit** | (14,120,000) | 1,700,000 | 11,230,000 | 23,510,000 | 43,220,000 |
|  | | | | | |
| **Tax** | (3,315,376) | 399,160 | 2,636,804 | 5,520,148 | 10,148,056 |
|  | | | | | |
| **Net Profit** | (10,804,624) | 1,300,840 | 8,593,196 | 17,989,852 | 33,071,944 |
| **ROI** | **-53.70%** | **9.78%** | **73.01%** | **156.57%** | **306.79%** |

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 of investment(ROI) for the solution 2 is as follows:

**Income Tax Rate:** 23.48%

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **Year 1** | **Year 2** | **Year 3** | **Year 4** | **Year 5** |
| **Net Gain** |  |  |  |  |  |
| Reduction in Fines / Penalities | 5,000,000 | 5,500,000 | 6,000,000 | 6,500,000 | 7,000,000 |
| Financial loss prevention | 2,500,000 | 3,000,000 | 3,500,000 | 4,000,000 | 4,500,000 |
| New customer base | 500,000 | 1,000,000 | 1,500,000 | 2,000,000 | 2,500,000 |
| **Total Revenue** | 8,000,000 | 9,500,000 | 11,000,000 | 12,500,000 | 14,000,000 |
| **Expense** |  | | | | |
| AML vendor service | 3,000,000 | 3,200,000 | 3,400,000 | 3,600,000 | 3,800,000 |
| Maintenance & Support | 500,000 | 600,000 | 700,000 | 800,000 | 900,000 |
| Employee Training | 200,000 | 250,000 | 300,000 | 350,000 | 400,000 |
| Data security | 500,000 | 600,000 | 700,000 | 800,000 | 900,000 |
| Integration | 500,000 | 600,000 | 700,000 | 800,000 | 900,000 |
| Downtime during integration | 1,000,000 | 1,200,000 | 1,400,000 | 1,600,000 | 1,800,000 |
| **Total Expense** | 5,700,000 | 6,450,000 | 7,200,000 | 7,950,000 | 8,700,000 |
|  |  |  |  |  |  |
| **Gross Profit** | 2,300,000 | 3,050,000 | 3,800,000 | 4,550,000 | 5,300,000 |
|  | | | | | |
| **Tax** | 540,040 | 716,140 | 892,240 | 1,068,340 | 1,244,440 |
|  | | | | | |
| **Net Profit** | 1,759,960 | 2,333,860 | 2,907,760 | 3,481,660 | 4,055,560 |
|  | | | | | |
| **ROI** | **30.88%** | **36.18%** | **40.39%** | **43.79%** | **46.62%** |

**Avg Income tax rate:** 23.48

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.

# **Solution Recommendation (the “why”)**

## **An in-house AI solution**

Why: Because AI is the future of technology. Large Language Models which are the basis of generative AI have changed the tech landscape and are akin to the industrial revolution in 21st century. It will change the nature of employment for many jobs in the future. Becoming a financial institution that leverages the use of AI will ensure TD’s leadership, since it will be the first to market as an early adopter of AI. There are competitors that are already looking into the tech market by advertising future employment roles in generative AI research to get some of the best talent. Here, however, we have a plan and solution ready addressing requirements with an effective implementation plan. This solution provides with the highest return on investment as displayed in the ROI section. Also, retaining control over the entire infrastructure provides TD with more insights and helps them make predictions to assist in business decision making.

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.

# **Database design:**

Database for both the possible solutions will have following tables:

1. Alerts

2. AI Model

3. Employee

4. Audit Log

5. Sanction List

6. Customer

7. Training

8. Transactions

# **Project selected****:**

To develop an in-house AI- driven anti-money laundering application is best option available of the three proposed solution. The alignment of future technology, and impact of AI makes this solution standout from the rest. Additionally, developing an in-house solution has advantages when it comes to data protection of bank and customizing the product. This solution not only addressed the AML issues but also gives a comprehensive, scalable, and ethical approach to the bank. The aim to stay committed to the regulatory compliance and fraud prevention will enhance the reputation of TD bank.

# **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.

1. **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.

1. **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.

1. **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.

1. **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.

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.

# **Risks 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** |

# **To-be process flow:**

The To-Be diagram represents an upgraded and proactive Anti-Money Laundering system. It incorporates advanced technologies, such as machine learning, NLP, and scenario simulation, to improve detection accuracy, response time, and overall compliance with global AML standards. Continuous monitoring, employee training, and legal oversight contribute to an adaptive and robust AML program that is responsive to evolving risks and regulatory requirements.



**Employee Training and AML Awareness**

Develops adaptive learning modules using machine learning techniques to enhance employee proficiency in AML compliance and utilizes AI-driven scenarios for diverse training, continuous learning feedback loops, and multilingual support.

**Alert Generation Using NLP Techniques**

The solution employs natural language processing (NLP) techniques for alert generation, improving the accuracy and informativeness of alerts through advanced language analysis. If suspicious activity is detected, the system triggers immediate alerts to AML analysts for further investigation. If a high level of suspicion is identified, the system escalates the case to higher authorities within the AML department for further investigation and action.

**Behavioral Analysis & Scenario Simulation**

The system utilizes unsupervised learning techniques for behavioral analysis, simulating diverse money laundering scenarios. It Integrates user profile simulation, anomaly detection, and ML-based scenario models.

**Real time monitoring**

The solution also implements real-time monitoring using advanced machine learning algorithms to enhance the accuracy and efficiency of transaction monitoring. It involves continuous monitoring of accounts flagged as suspicious to detect any changes in behavior or transactions.

# **Implementation/deployment Strategy/approach:**

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.

## **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.

## **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.

**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.

**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 | Test Strategy Document |

## **Document Approval**

|  |  |  |
| --- | --- | --- |
| **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 |

## **Scope**

Testing Activities:

* Requirement Analysis (Functional & Non-functional)
* Test planning
* Test Design
* Test environment setup
* Test executions
* Defect reporting and tracking
* Production deployment
* Test closure

## **Types of Testing**

* Unit Testing
* Integration Testing
* System Testing
* Smoke Test
* Load Test/ Performance Testing
* Security Test
* Scalability Test
* User Acceptance Testing

## **Test Approach**

Project Management: Agile Methodology

Module development: Sprints of 2 weeks

Sequence of testing: As mentioned under the “types of testing”.

## **Roles and Responsibilities**

|  |  |  |
| --- | --- | --- |
| **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 |

## **Approach and Tools**

The testing team will follow agile methodology to complete this project. The testing activities will be iterative with feedback loops. The project will follow the shift left approach thus the testers will closely collaborate with the develops from the initial stage of development for defect prevention and early testing.

**Tools:**

* Test management tool: Azure DevOps
* Functional testing: Selenium
* Non-functional testing: LoadRunner, HP Performance Center, Wireshark

## **Defect Tracking**

Defects or bugs identified in the software testing process should be documented as user stories and assigned to the development team using the defect tracking system. The testing team will conduct tests to verify that the issues are resolved once the development team addresses these concerns and deploys new code. A signoff document will be prepared at the end of each testing phase, outlining the tested features, reported bugs, and any optimizations made during the process.

## **Test Environment**

The proposed solution will be tested in the Azure could environment due to its security and speed. Backups of test data will be created and stored in cloud after each test phase for potential restoration.

* 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.

## **Release Control**

**Objective:** To Ensure systematic releases, with effective test execution and continuous enhancement.

**Major Activities:**

1. **Bi-Weekly Releases**:

* Schedule releases every two weeks that include 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 backwards compatible.
* PATCH version for bug fixes that are backwards compatible.

1. **Change History:**

* For each release, keep a detailed change log.
* Include a list of 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.

## **Risk Analysis**

**Potential risks:**

* Data breach: Unauthorized access or security breaches
* Inadequate training: Misuse of the AML system by employees due to insufficient training.
* Scalability Issues: Failure to scale up according to the increasing transaction volumes.

**Impact:**

* Legal consequence
* Financial loss
* Increased false positives
* Performance issues
* System downtime

**Mitigation plan**

* Regular security audits and update encryption protocols.
* Implement a comprehensive training program, regularly update training materials and conduct assessments.
* Investment in scalable infrastructure, routine load testing, and continuous tracking of performance metrics.

**Contingency plan:**

* Immediate activation of an incident response team.
* Communicate openly with affected parties and put corrective measures in place.
* Conduct post-incident investigation.
* Conduct regular assessments to identify gaps.

## **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**

The test phase can be closed successfully of the following criteria is met:

1. Functional test executions are successful.
2. Critical defects are fixed and verified.
3. Performance and security requirements are met.
4. Risk mitigations and business continuity plan is developed.
5. All test artifacts are reviewed, approved, and signed off by the stake holders.

# **APA References**

* TD. (2022). TD Bank and First Horizon Scrap $13.4 Billion Merger

<https://www.pymnts.com/news/partnerships-acquisitions/2023/td-bank-first-horizon-scrap-13-billion-dollar-merger/>

* TD. (2020). AML Statement

<https://www.td.com/document/PDF/ESG/2020-AML-ATF-Sanctions-Statement.pdf>

* TD. (n.d.). *About TD – TD Canada Trust*.

<https://www.td.com/ca/en/about-td>

* TD. (2023). Corporate Governance Structure

<https://www.td.com/ca/en/about-td/corporate-profile/corporate-governance-structure>

* Financial Crimes Enforcement Network. (n.d.)

<https://www.fincen.gov>

* Scrum.org. (n.d.)

<https://www.scrum.org>

* Financial Post. (2023) *TD could face penalties in probe of Anti Money Laundering Compliance in US.* <https://financialpost.com/fp-finance/banking/td-penalties-anti-money-laundering-compliance-us>
* Financial Post. (2023) *Short positions against TD Bank climb to $6.1 billion, data shows*  
  <https://financialpost.com/fp-finance/banking/td-bank-short-positions-rise-6-1billion-data>
* RBC. (n.d.). *RBC Wealth Management*.

<https://www.rbcwealthmanagement.com/en-ca/>

* TD. (2022). *Annual Report 2022*

<https://www.td.com/document/PDF/ar2022/ar2022-Complete-Report.pdf>

* TD. (n.d.). *Environmental-social-governance-reporting*.

<https://www.td.com/content/dam/tdcom/canada/about-td/pdf/esg/2022-esg-report.pdf>

* RBC. (2018). *About RBC*

<https://www.rbc.com/about-rbc.html>

* Scotiabank. (2023). *Investor Presentation*.

<https://www.scotiabank.com/content/dam/scotiabank/corporate/quarterly-reports/2023/q3/Q323_Investor_Marketing_Presentation.pdf>

* Canadian Imperial Bank of Commerce. (2019). *Personal Banking.*

<https://www.cibc.com/en/personal-banking.html>

* Quarterly Results Presentation. (n.d.). Retrieved September 14, 2023, from

<https://www.cibc.com/content/dam/cibc-public-assets/about-cibc/investor-relations/pdfs/quarterly-results/2023/q323presentation-en.pdf>

* CIBC. (n.d.). *Sustainability*

<https://www.cibc.com/en/about-cibc/corporate-responsibility.html>

* CIBC. (n.d.). History

<https://www.cibc.com/en/about-cibc/corporate-profile/history.html>

* Royal Bank of Canada (RBC) Review 2023: What To Expect From Canada’s Largest Bank. (2023, July 7). *Forbes Advisor Canada.*

<https://www.forbes.com/advisor/ca/banking/royal-bank-of-canada-review/#:~:text=The%20primary%20downsides%20of%20banking>

* PESTEL Analysis of TD Bank Group Building an Effective Enterprise Data Management Policy. (n.d.). *247caseanalysis*.

[https://www.247caseanalysis.com/case/TD-Bank-Group-Building-an-Effective-Enterprise-Data-Management-Policy-21412-Pestel-Analysis](https://www.247caseanalysis.com/case/TD-Bank-Group-Building-an-Effective-Enterprise-Data-Management-Policy-21412-Pestel-Analysis  )

* The Toronto-Dominion Bank Number of Employees 1991-2022. (n.d.). *Stock Analysis.* Retrieved September 14, 2023, from

<https://stockanalysis.com/stocks/td/employees/>

* TD Bank Group—Org Chart, Teams, Culture & Jobs. (n.d.). *THE ORG*. Retrieved September 14, 2023, from

<https://theorg.com/org/td-bank>

* TD Canada Trust Organizational Structure [Interactive Chart]. (n.d.). *Organimi*. Retrieved December 11, 2023, from

<https://www.organimi.com/organizational-structures/td-canada-trust/>