White paper

Revolutionizing Financial Crime Compliance: Innovative Data Products From Teradata

Manish Andhy
Senior Director of Technical Product Marketing

teradata.

Table of Contents

Introduction

"The modern world of financial crime is personalized, lucrative, and—frankly — terrifying. It is estimated that over $3 trillion dollars in illicit funds moves through the global financial system each year, meaning that financial crime proceeds exceed the annual GDP of a country the size of Canada or France. More discouraging still, it is estimated that just 1% of illicit financial activity is intercepted by law enforcement agencies."[1]

Financial institutions today face an escalating threat landscape driven by increasingly sophisticated financial crimes, alongside growing regulatory scrutiny and compliance obligations. At the same time, expectations for speed, accuracy, and transparency across financial crime programs continue to rise.

A primary impediment to effectively addressing these challenges is the persistence of siloed Anti-Money Laundering (AML) and financial crime programs. These fragmented operations frequently rely on inconsistent datasets and disconnected technologies, resulting in operational inefficiencies, elevated risk exposure, and rising costs. The outcome is often a reactive compliance posture, one that struggles to adapt to emerging threats, evolving criminal typologies, and changing regulatory expectations.

This paper makes the case that financial institutions can no longer meet modern financial crime and regulatory demands through fragmented AML systems, and that a unified data and analytics platform—operationalized through trusted, reusable data products—is essential to simultaneously improve compliance effectiveness, reduce risk, and drive measurable business value.

1. Lucas Chapin, "The Evolving Landscape of Financial Crime," Hummingbird.com, 2024, https://www.hummingbird.co/resources/the-evolving-landscape-of-financial-crime.

Financial crimes defined

To ground this discussion, the following section outlines the scope of financial crime and the regulatory mechanisms—particularly AML—that underpin financial institutions' response. Readers more familiar with these concepts may skip to the concluding paragraph of this section.

Financial crime, such as money laundering, fraud, corruption, and terrorist financing, poses a significant threat with far-reaching consequences, such as undermining financial system integrity, funding serious crimes, threatening national and global security, and causing economic harm to businesses and individuals[2][3]. Victims suffer financial and social harm, and widespread financial crime damages the public's confidence in institutions and the rule of law.

Financial crimes prevention is a collective effort involving governments, regulators, law enforcement, and financial institutions[4]. It primarily happens through robust regulatory frameworks and technology-driven processes, most notably Anti-Money Laundering (AML) and Counter-Terrorist Financing (CTF) programs[5]. Governments and international bodies, like the Financial Action Task Force (FATF), set standards and laws (e.g., the Bank Secrecy Act and USA PATRIOT Act in the U.S.) that place a wide variety of screening and monitoring obligations on financial institutions, including Customer Due Diligence (CDD) and Know Your Customer (KYC), Transaction Monitoring (TM) and Suspicious Activity Reporting (SAR). Government regulation has also introduced new risks for banks, the risk of sanctions or even of charter suspension.

Against this backdrop, AML frameworks serve as the primary operational mechanism through which financial institutions translate regulatory expectations into day-to-day controls.

Anti-money laundering (AML)

Anti-Money Laundering (AML) refers to the set of laws, regulations, and procedures designed to prevent criminals from disguising illegally obtained funds as legitimate income. Its core purpose is to stop the process of money laundering, which involves three stages: placement (introducing illegal funds into the financial system), layering (obscuring the trail of the funds), and integration (using the funds as legitimate wealth). AML programs in financial institutions utilize mechanisms like KYC, transaction monitoring, and suspicious activity reporting (SARs) to detect and report illicit financial activity, thereby protecting the integrity of the global financial system.

Customer Due Diligence & Know Your Customer

Within AML programs, Customer Due Diligence (CDD) and Know Your Customer (KYC) processes establish the foundational understanding of customer identity and risk.

"Know Your Customer" is a catch-all term addressing customer identity management that incorporates a body of regulatory requirements for financial institutions that differ slightly by jurisdiction. In the USA, the Currency and Foreign Transaction Reporting Act of 1970 established a CDD rule to improve financial transparency and deter money laundering. The CDD rule[6] requires banks to verify the identity of the beneficial owners of accounts, understand the nature of the individual customer's relationship to the account and to keep ownership records up to date. Once customer identity and risk are established, ongoing transaction monitoring becomes the primary means of detecting suspicious behavior over time.

2. Caroline Claver, et al., "Financial Crimes Hurt Economies and Must be Better Understood and Curbed," https://www.imf.org/, 2023,https://www.imf.org/en/blogs/articles/2023/12/07/financial-crimes-hurt-economies-and-must-be-better-understood-and-curbed.
3. Pierre Bardin, et al., "Money Laundering Poses a Risk to Financial Sector Stability," https://www.imf.org/en/home, 2023, https://www.imf.org/en/blogs/articles/2023/09/04/money-laundering-poses-a-risk-to-financial-sector-stability.
4. "Reducing and preventing financial crime," www.fca.org.uk, 2025, https://www.fca.org.uk/publications/corporate-documents/reducing-and-preventing-financial-crime.
5. "Anti-Money Laundering / Countering The Financing Of Terrorism (AML/CFT)," fdic.gov, 2025, https://www.fdic.gov/banker-resource-center/anti-money-laundering-countering-financing-terrorism-amlcft.
6. "Information on Complying with the Customer Due Diligence (CDD) Final Rule," finCEN.gov, 2024, https://www.fincen.gov/resources/statutes-and-regulations/cdd-final-rule.

Transaction Monitoring (TM)

Identification of Suspicious Transactions—a key component of adherence to Anti-Money Laundering—facilitates investigations into the misuse of legal persons and legal arrangements. This information can uncover patterns that match known money laundering or terrorist financing schemes[7].

A core analytical capability for banks is to determine whether any given banking transaction is suspicious, which often relies on the ability to identify transaction behavior that is "out of pattern" for a customer. Dimensions of the transaction that require evaluation to identify anomalous behavior include timing (e.g., day of the week and calendar date), dollar amount, and, most importantly, the counterparty to the transaction, especially regarding the location of the payee and nature of its business. Alerts flag potentially suspicious activity, which are then investigated by AML analysts.

Historically, most banks have responded to the expansion of regulatory oversight with expensive manual processes or developed brittle rule-based systems to flag potential issues.

Suspicious Activity Reporting (SAR)

An SAR (also referred to as a Suspicious Transaction Report, or STR) is the formal legal and communications mechanism used to support risk mitigation and collaboration with law enforcement. It is a mandatory, confidential regulatory filing through which financial institutions formally report suspected illicit financial activity to a Financial Intelligence Unit (FIU) or relevant law enforcement authorities [8][9].

SARs are the primary channel through which the financial sector provides actionable intelligence to government agencies, triggering formal investigations and enabling authorities to trace and seize illicit funds. While these AML components are well understood and widely implemented, their effectiveness is increasingly constrained by fragmented data, disconnected systems, and limited analytical cohesion. Addressing these structural limitations requires a more fundamental rethinking of how data is managed and consumed across the financial crimes lifecycle.

To revolutionize the financial crimes program, a fundamental shift is required: the adoption of a unified data and analytics platform. Such a platform serves as the indispensable foundation for a robust AML and financial crimes program. Within this transformative framework, the strategic implementation of "data products" emerges as the pivotal mechanism. Data products, defined as highly trusted, reusable, and consumable data assets, are curated collections of datasets and business-approved metadata designed to address specific domain outcomes. This approach allows financial institutions to transform disparate raw data into actionable intelligence, readily available for various AML functions.

7. "Transaction monitoring," austrac.gov.au, https://www.austrac.gov.au/business/core-guidance/amlctf-programs/transaction-monitoring.
8. "Bank Secrecy Act Forms and Filing Requirements," FinCEN.gov, https://www.fincen.gov/resources/filing-information.
9. "Suspicious Activity Reports (SAR)," occ.treas.gov, https://www.occ.treas.gov/topics/supervision-and-examination/bank-operations/financial-crime/suspicious-activity-reports/index-suspicious-activity-reports.html.

The imperative for change: addressing siloed AML programs and evolving financial crime threats

Current challenges of disconnected AML systems

Financial institutions are currently grappling with substantial inefficiencies and heightened risks stemming from their fragmented AML and financial crimes programs. These programs frequently operate in isolation, utilizing disparate technologies and inconsistent datasets, which creates a complex and costly environment. This fragmentation invariably leads to widespread data duplication, which in turn exacerbates data governance risks and complicates the establishment of a singular, reliable "golden" dataset for various AML functions.

Beyond data duplication, a critical challenge lies in the lack of real-time visibility into emerging risks. Furthermore, the comprehensiveness and overall quality of data pose a significant hurdle for financial institutions. This deficiency in data quality and timeliness severely impairs the ability to detect evolving financial crime tactics, which are becoming increasingly sophisticated. Traditional systems often generate a high volume of false positive alerts, necessitating time-consuming and costly manual reviews. This alert fatigue leads to significant resource constraints and impacts overall productivity, directly contributing to increased operational costs.

The regulatory landscape is in constant flux, with new AML regulations emerging frequently. Simultaneously, criminal methodologies are becoming more advanced and complex, making it difficult for legacy, siloed systems to adapt and identify novel typologies. The inherent rigidity and lack of integration in these older systems mean that financial institutions are often playing catch-up, exposing them to significant financial penalties and reputational damage. The proliferation of siloed systems and data fragmentation is not merely a technical challenge for IT departments; it represents a fundamental impediment to effective financial crime risk management, directly impacting regulatory adherence, operational efficiency, and the agility required to counter sophisticated threats.

Benefits of a unified data & analytics platform

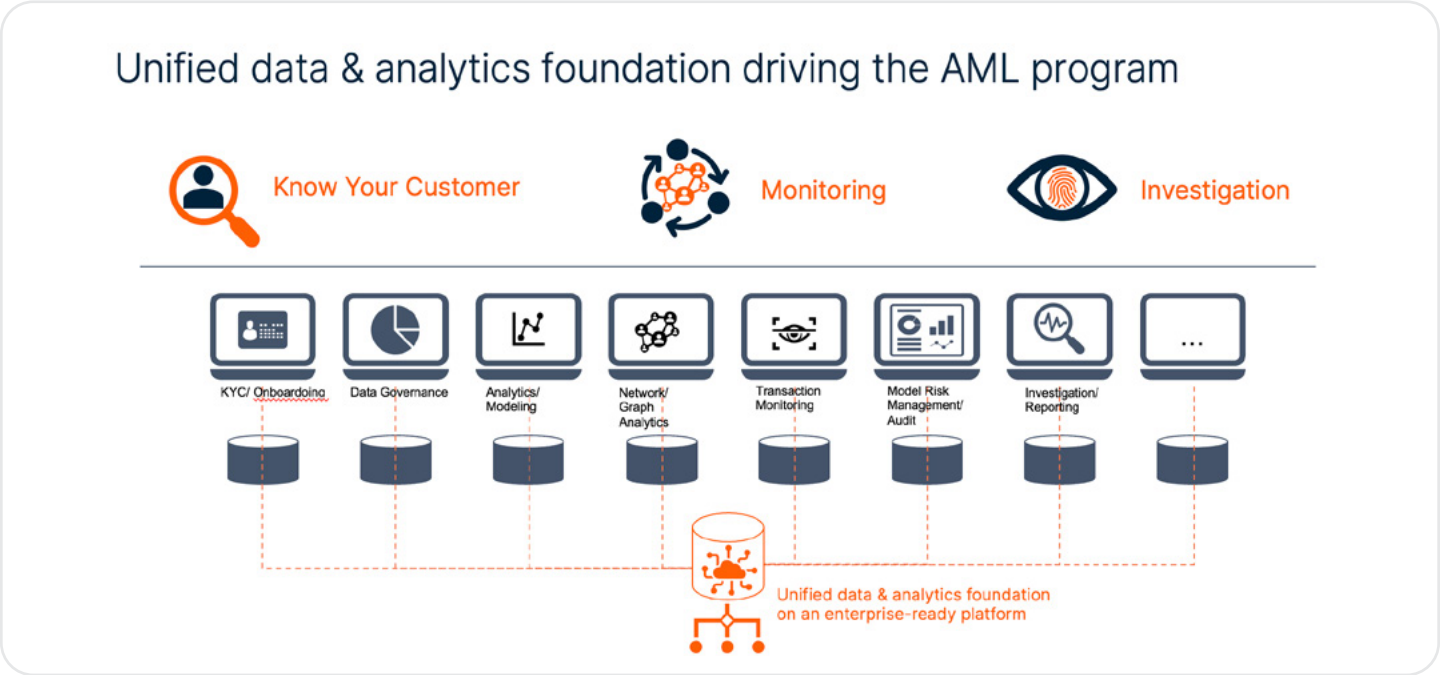
Addressing these challenges requires a unified data and analytics foundation designed to support AML end-to-end. The transition from siloed operations to a unified data and analytics platform represents a foundational shift that aligns business performance objectives with financial crime prevention and regulatory compliance goals. By transforming fragmented data into a shared, enterprise-wide asset, such a platform not only strengthens a financial institution's ability to combat financial crime, but also improves operational efficiency, cost control, and decision-making across the organization.

First, it leads to improved efficiency. By centralizing data and enabling consistent access, a unified platform significantly decreases model development time and increases overall productivity. This can accelerate the time to market or value, potentially reducing the model lifecycle from months to mere weeks. This rapid development cycle allows institutions to respond more swiftly to emerging threats and regulatory mandates.

Second, the platform offers reduced risk. Providing a single "golden" dataset across the enterprise minimizes data duplication, thereby substantially reducing data governance risk. This ensures that all pillars of the AML program—from initial customer onboarding and model development to ongoing investigations and audit—operate on the same consistent and reliable information. This consistency is crucial for accurate risk assessments and robust compliance.

Third, a unified platform enables optimized costs. The gains in efficiency and the reduction in redundant efforts translate directly into optimized and reduced expenditures across various categories, including Full-Time Equivalents (FTEs), software licenses, and hardware infrastructure. By streamlining processes and reducing manual interventions, institutions can reallocate resources more strategically.

Finally, the platform ensures scalability and enhanced data quality. An enterprise-ready data management system facilitates increased data update frequency and significantly improves data quality by establishing a single source of truth. This robust data foundation is critical for accurate reporting and effective decision-making. Furthermore, an efficient data ecosystem bolsters fraud detection and prevention measures by enabling real-time monitoring of transactions and the rapid identification of irregularities and patterns, allowing for swift intervention before financial crimes escalate. This fundamental shift transforms data from a fragmented, costly burden into a cohesive, strategic asset, enabling proactive risk management and unlocking operational efficiencies previously unattainable.



A unified data and analytics foundation supporting the different pillars of an AML program is key to the successful execution of a robust AML program

Data products for financial crime compliance

Data product defined

At their core, data products are highly trusted, reusable, and consumable data assets. More specifically, they are curated collections of productized datasets, enriched with business-approved metadata and domain logic, designed to solve specific business outcomes within the financial crime domain. This approach transforms raw, disparate data into valuable insights, actionable predictions, or clear visualizations. For AML, this means converting fragmented information into intelligence that can be directly consumed by compliance teams, investigators, and regulatory bodies.

Data product refined

The benefits of adopting a data product strategy are substantial. It has the potential to accelerate the implementation of new use cases by up to 90%[10], significantly improve decision-making processes, enhance overall data quality, and bolster regulatory compliance. Data products effectively bridge the gap between data producers and data consumers, ensuring that the right data is available to the right people in a usable format.

A key aspect of this strategy is the ability to create "sub-data products" by slicing multi-dimensional data along various axes, such as product type, specific business function, or particular risk area. For instance, a "Customer Risk Profile" topic could have sub-topics tailored for "Retail Banking Customer Risk Profiles" or "High-Risk Politically Exposed Person (PEP) Profiles." This modularity allows for highly specific data consumption while maintaining a unified underlying data foundation. This approach marks a paradigm shift from traditional data warehousing, operationalizing data governance and reusability. It transforms raw data into consumable, business-centric assets that directly address compliance challenges, rather than merely storing information. This is critical for scaling AML efforts efficiently and achieving incremental excellence by building data assets once and reusing them across multiple functions.

With this data product framework in place, the following sections illustrate how it can be applied across core AML focus areas, beginning with Customer Due Diligence and onboarding.

10. Veeral Desai, "How to unlock the full value of data? Manage it like a product," McKinsey & Company, 14 June 2022, https://www.mckinsey.com/capabilities/quantumblack/our-insights/how-to-unlock-the-full-value-of-data-manage-it-like-a-product#/.

Focus Area: Customer Due Diligence & Know Your Customer

CDD and KYC form the bedrock of AML compliance, involving the systematic collection, verification, and ongoing monitoring of customer information to accurately assess their risk profile. This foundational process includes the Customer Identification Program (CIP) for initial identity verification and Enhanced Due Diligence (EDD) for higher-risk profiles, ensuring a comprehensive understanding of each customer.

Topic: Customer risk profile & onboarding data

The purpose of this topic is to deliver a comprehensive, verified, and continuously updated view of customer identity, their associated entities, and their risk profile. It supports critical functions, from initial customer onboarding, to ongoing due diligence and enterprise-wide risk assessment. By productizing KYC/CDD data, financial institutions can move beyond static compliance checklists to a dynamic, risk-based customer intelligence hub. This enables not only efficient onboarding but also continuous, proactive risk management throughout the customer lifecycle.

By centralizing and standardizing this information, this data product becomes the "master customer data" for AML, ensuring consistency and providing accurate context for downstream processes like transaction monitoring. This significantly reduces redundant data collection and processing efforts.

As artificial intelligence—including generative AI—continues to mature and be applied at scale, onboarding new customers and meeting KYC regulatory requirements can be made significantly more efficient. Once AI distills information from new account applications using natural language processing (NLP), graph analysis can provide a deeper understanding of the entities involved and automatically identify potentially illicit transactions. The nexus of payer and payee relationships can be revealed from payment flow data using a payments network graph, with hidden patterns surfaced through graph neural network (GNN) models.

AI dramatically reduces the time and manual effort required for foundational KYC steps such as identity verification and document processing, using optical character recognition (OCR) and NLP to instantaneously scan, extract, and verify data from documents such as passports, driver's licenses, and proof of address. AI can also detect signs of forgery, deepfakes, and document tampering with far greater accuracy than manual review.

Focus Area: Transaction Monitoring

As customer risk profiles are established and maintained, transaction monitoring extends this intelligence into continuous behavioral oversight. Transaction monitoring involves continuous oversight of a customer's financial activities, including deposits, withdrawals, and transfers, with the primary objective of identifying suspicious behavior that could indicate money laundering or other financial crimes.

Historically, most banks have responded to the expansion of regulatory oversight with expensive manual processes or developed brittle rule-based systems to flag potential issues. This process is increasingly being augmented by AI and machine learning capabilities that can adapt to evolving risk patterns and detect complex, non-linear behaviors that traditional rules-based approaches often miss. Advances in model architectures now enable transaction monitoring systems to analyze large volumes of structured and unstructured data in near real time, uncovering hidden relationships, subtle anomalies, and emerging typologies of financial crime. As a result, institutions can reduce false positives, prioritize truly high-risk activity, and respond more quickly to potential threats while maintaining regulatory confidence.

Topic: Suspicious activity detection data

The identification of suspicious transactions is a foundational element of AML controls, enabling investigations into the misuse of legal persons and legal arrangements and supporting the detection of money laundering, terrorist financing, fraud, and tax evasion.

Detecting suspicious transactional activity requires timely, well-contextualized data that allows financial institutions to surface behaviors indicative of elevated risk across customers, counterparties, and transaction flows.

The purpose of this data product is to provide a comprehensive, real-time or near real-time stream of transactional activities, enriched with relevant customer and counterparty context. This enables the precise detection of unusual patterns and potential illicit financial flows. When supported by such a data product, transaction monitoring evolves from a reactive, rule-based system into a proactive, intelligence-driven engine. Integrating customer context (derived from KYC data products) and historical behavioral data significantly reduces false positives and enhances the detection of sophisticated, evolving criminal typologies.

This data product enables the crucial shift from simple rule-matching to advanced behavioral analytics and AI-driven detection, which is vital for combating the increasingly sophisticated methods employed in modern financial crime.

Focus Area: Financial crime investigations & case management

The financial crimes investigation process involves thoroughly reviewing flagged suspicious activities, meticulously gathering supporting documentation, determining the validity of an alert, and, if necessary, filing SARs with regulatory bodies. This critical function requires a comprehensive review of customer profiles, historical transaction data, and external intelligence to build a complete picture of potential illicit activity.

The AML investigation and SAR reporting process is plagued by significant inefficiencies and challenges, largely driven by reliance on legacy technology, data fragmentation, and high volumes of false alerts. The main challenges center on high false positives, fragmented data, and manual reporting.

Fragmented data spread across multiple systems often hinders investigators, who are forced to manually compile information. Up to 60% of alert triage time is spent on counterparty research due to missing consolidated historical data[11]. This lack of an integrated view hampers investigators' ability to link related alerts and spot complex criminal activity.

Furthermore, the SAR narrative is the most critical and resource-intensive component of the entire SAR form. It must clearly, concisely, and accurately answer the "who, what, when, where, why, and how" of the suspicious activity to be useful to law enforcement. In addition to the manual data collection, investigators must manually ensure all fields are correctly populated and submitted according to the specific regulations for the jurisdiction. This process is repetitive and prone to simple data entry errors. Lastly, creating a concise, coherent, and legally compliant written narrative from a large, complex body of data requires high-level human expertise and is subject to human variability and quality issues.

Generative AI (GenAI) can streamline the automated generation of SARs by synthesizing inputs from multiple data sources and supporting investigator workflows. NLP analyzes unstructured information—such as internal notes, emails, transaction memo fields, and investigator summaries—to extract key entities, including names, dates, amounts, typologies, and regulatory codes, along with the relevant suspicious context. Large language models (LLMs) then use this structured output to construct clear, coherent narrative reports that align with regulatory expectations.

Topic: Investigation & reporting intelligence

Consolidate all pertinent data points related to a suspicious activity alert or an ongoing case, providing investigators with a holistic view for efficient analysis, informed decision-making, and accurate regulatory reporting, particularly for SARs. A dedicated data product for investigations pulls together all necessary internal and external data, enabling faster, more accurate investigations and SAR filings, thereby significantly improving the efficiency and effectiveness of the compliance team.

Sub-Topics:

Suspicious Activity Reporting (SAR) filings: Contains all required fields and the supporting documentation necessary for accurate and timely SAR submissions.

- **Case history & resolution data:** Tracks the complete lifecycle of an investigation, including decisions made, actions taken, and final outcomes.
- **Network & link analysis data:** Visualizes and quantifies relationships between entities, accounts, and transactions, revealing hidden connections.
- **Adverse media & watchlist hits:** Consolidates external intelligence, including negative news and sanctions/ watchlist matches, relevant to the investigation.

Deploying all of the sub-topics above consolidates all relevant data points related to a suspicious activity alert or case, providing investigators with a holistic view for efficient analysis, decision-making, and regulatory reporting (SARs).

This approach transforms investigations from a data-gathering exercise into an analytical one, allowing investigators to focus on intelligence and decision-making rather than data reconciliation. The integration of AI capabilities to collate unstructured data further enhances this efficiency.

11. "Four Ways Data Creates Challenges for AML Investigators", Nasdaq Verafin, 14 September 2022, https://verafin.com/2022/09/data-challenges-for-aml-investigations/.

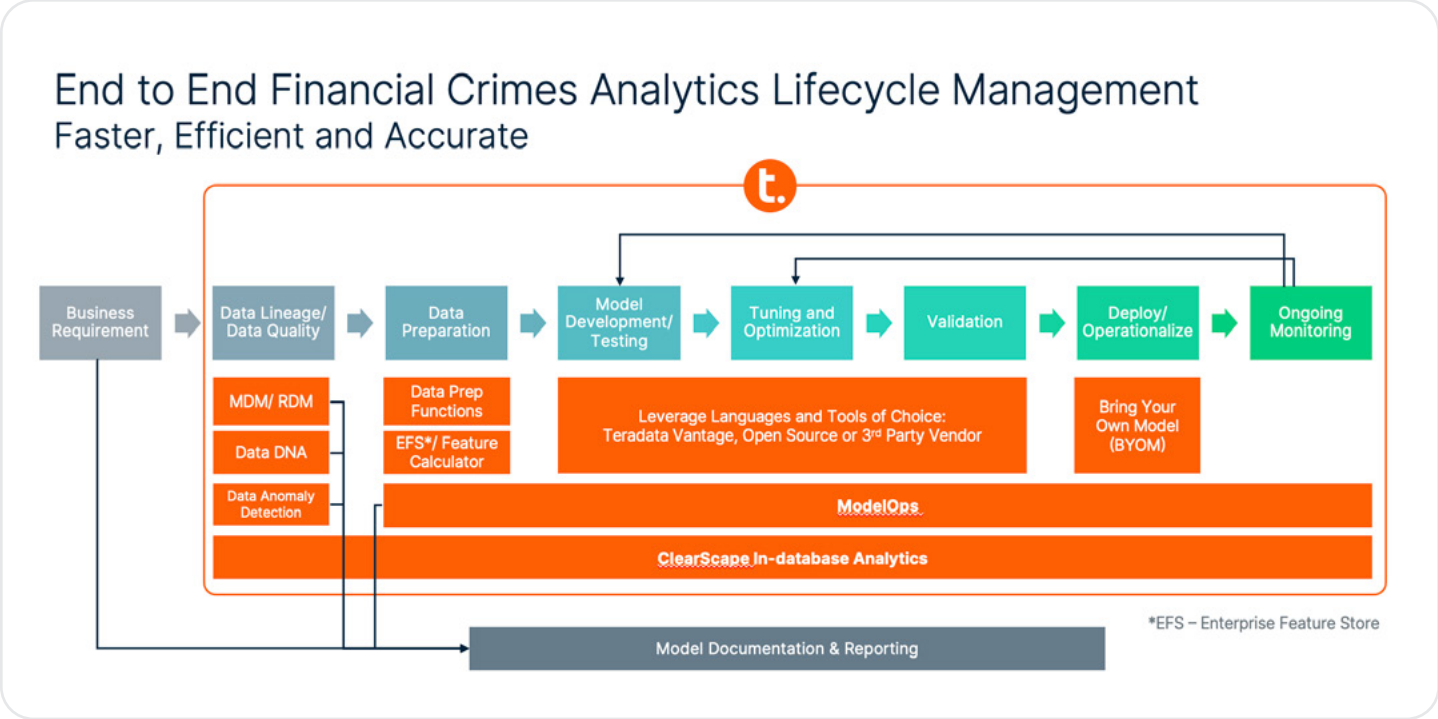
Horizontal functions: Leveraging the unified data ecosystem

While KYC/CDD/EDD, transaction monitoring, sanction screening, and investigations are distinct pillars of an AML program, several critical functions operate horizontally, cutting across and supporting all these pillars. These include model risk management (MRM), data governance, and audit. Rather than having their own specific data products in the same vein as the pillars, these functions consume and leverage the foundational data tables and the data products generated by the core AML pillars. Their effectiveness is directly tied to the quality, accessibility, and consistency of the unified data platform.

The power of data reuse: Commonality and specificity across topics

The detailed analysis of data elements across the various AML pillars clearly reveals a significant overlap in foundational data. Elements such as customer identity details (e.g., customer ID, full legal name, address), basic account information (account numbers), and core transaction attributes (transaction date, amount, type) are consistently required across KYC, transaction monitoring, investigations, model risk management, and audit functions. This pervasive commonality underscores the immense value of establishing a single "golden source" of data, a capability inherently provided by Teradata.

This commonality facilitates substantial efficiency through reuse. By building these foundational data elements once—ensuring their accuracy, cleansing them, and governing them centrally—financial institutions can drastically reduce redundant data ingestion, transformation, and storage efforts across their distinct AML functions. This direct approach contributes significantly to improved operational efficiency and optimized costs, as resources are no longer wasted on repetitive data preparation tasks. Enabling this level of integration, reuse, and analytical consistency requires an enterprise platform purpose-built for scale, governance, and advanced analytics.



ClearScape Analytics enables end-end analytic lifecycle execution, eliminating the need for multiple tools/ products and reducing tech debt and cost

Teradata: Powering the unified data product for financial crime

Teradata stands out as the premier platform for building this unified data and analytics foundation, offering unmatched capabilities essential for modern financial crime compliance. Its core strength lies in its ability to provide the "golden source" of data across the entire enterprise, supporting all critical pillars of AML and financial crimes programs. This means that instead of disparate data repositories, a single, trusted version of customer, account, and transaction data is available to all relevant functions.

Teradata's architecture is specifically designed for enterprise readiness and scalability. Financial institutions manage immense volumes of data, both structured and unstructured, a volume that continues to grow exponentially. Teradata can handle these high-volume, high-velocity data processing demands, ensuring that even real-time transaction monitoring and complex investigations can operate with optimal efficiency. This robust capability directly addresses the limitations of legacy systems, which often lack the scalability to handle large data volumes and dynamic workflows. By inherently supporting mechanisms to ensure data integrity and consistency, Teradata directly tackles the pervasive challenge of poor data quality, which is a top concern for compliance leaders and a common finding in model validation reports. This forms the non-negotiable bedrock upon which the entire data product ecosystem and advanced AML analytics are built.

Furthermore, Teradata offers an open architecture, a crucial feature in a rapidly evolving technological and regulatory landscape. This openness allows financial institutions to seamlessly integrate various AML applications, advanced AI and ML tools, and emerging RegTech solutions without suffering from vendor lock-in. This flexibility is vital for adapting to new threats and regulatory changes without incurring costly rip-and-replace cycles, which are common with rigid, legacy systems. Teradata's robust, scalable, and open architecture directly addresses the technical and strategic limitations of traditional, siloed systems, providing the necessary infrastructure for a future-proof, data-driven AML program. Much more than a data warehouse, Teradata is a strategic enabler for agility and adaptability, which is crucial for supporting the data product vision and ensuring continuous improvement in financial crime detection.

From compliance cost center to business enabler

The ultimate value proposition of Teradata's unified platform, powered by a data product approach, extends far beyond mere compliance. It enables a fundamental transformation, shifting the perception of AML from a necessary cost center to a strategic business enabler.

This transformation is achieved through incremental excellence via data reuse. By first establishing a robust, unified data foundation specifically for AML, financial institutions create a high-quality, trusted data asset. This AML data then serves as a stepping stone, providing a rich source of intelligence that can be leveraged for broader business value. For example, insights gained from analyzing customer behavior for suspicious activity can also inform customer segmentation, product development, or even fraud detection initiatives beyond traditional AML.

An efficient and effective AML program built on Teradata not only protects the institution's reputation and helps avoid substantial regulatory fines and penalties, but it also significantly improves the customer experience. By reducing the number of false positives that disrupt legitimate customer transactions and streamlining onboarding and due diligence processes, the institution can foster greater trust and drive business growth. This means that the compliance function, typically viewed as a drain on resources, becomes a source of actionable intelligence, contributing directly to competitive advantage and enhanced customer relationships across the enterprise.

Teradata stands as the optimal platform to construct this unified data foundation. Its enterprise-grade capabilities provide a singular "golden source" of data across the entire organization, supporting critical AML pillars such as KYC, transaction monitoring, data governance, analytics, investigations, model risk management, and audit. By leveraging Teradata, financial institutions can achieve substantial improvements in efficiency, significantly reduce risk exposure, and optimize operational costs. This strategic investment not only fortifies defenses against illicit financial activities but also elevates compliance from a mere cost center to a powerful business enabler, unlocking broader enterprise value from high-quality, trusted data.

About Teradata

At Teradata, we believe that people thrive when empowered with trusted information. We offer the most complete cloud analytics and data platform for AI. By delivering harmonized data and Trusted AI, we enable more confident decision-making, unlock faster innovation, and drive the impactful business results organizations need most. See how at **Teradata.com.**

17095 Via Del Campo, San Diego, CA 92127 Teradata.com

teradata.