ORACLE

FINANCIAL SERVICES

An Oracle White Paper
March 2010

Best Practices for Anti Money Laundering (AML): System Selection and Implementation

ORACLE

Disclaimer

The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle's products remains at the sole discretion of Oracle.

Executive Overview

The stakes are higher than ever for compliance. Money launderers are increasingly turning their attention to jurisdictions with lax Anti- Money Laundering (AML) laws as well as to mid size financial institutions. In their fight against financial crime including money laundering, compliance executives need to arm themselves with the right tools and systems. A key decision in this 'fight' is to build the business case internally for an effective compliance system that will meet the financial institution's current and future compliance needs. Inevitably, executives must determine the right system to "future-proof" their compliance spend, as well satisfy their regulators.

This white paper describes how world-class financial services companies and IT executives approach the same challenges that confront many organizations wrestling with the build versus buy decision as well as what are the optimum capabilities they should look for in a such a compliance system:

- How will the system satisfy our regulators?
- What requirements should we take into consideration so that we can future-proof our compliance spend?
- Will our compliance solution be in line with competition, more stringent, or too lax when compared to industry best practices?
- What additional compliance failure risk do we assume, if we build a custom system? Will we detect or miss potential violations?

Introduction

Now more than ever, financial industry executives are confronting complex and serious compliance challenges. How executives address these challenges determines whether a company reduces or increases the risk of experiencing costly compliance failures. Companies that stumble, often discover that they have to pay a steep price for failures: revenue drop, customer defections, stock price declines, record financial penalties, tarnished reputations,

class action suits, high legal and public relations costs, and personal damage to the careers of the executives involved.

When companies face large or small compliance failures, suddenly the costs of deploying proven and robust compliance systems look infinitesimal when compared to the costs of those compliance failures. This leaves no choice; compliance solutions must be implemented. So how do executives go about this in the right way?

Understanding AML Compliance System Requirements

The first step is to identify the core functionality necessary in an AML compliance system to avoid legal and regulatory issues. An effective AML compliance system must:

- Satisfy regulatory requirements
- Span the entire enterprise
- Detect all suspicious behavior rapidly
- Reflect industry best practices
- Be easy to use and change
- Provide long-term cost effectiveness

Satisfy Regulatory Requirements

Compliance systems need to prevent and detect potential violations. Regulators are spelling out in detail what they expect, providing you with a roadmap to successful compliance practices and a benchmark to measure your compliance capabilities.

In the area of anti-money laundering, regulators have stressed the need for firms to detect patterns of wrongdoing over time. Such patterns should be detectable in one account, households of accounts, and across all customer accounts. Lori Richards, director of the Office of Compliance Investigations and Examinations (OCIE) at the U.S. Securities and Exchange Commission, has cited best practices in this area, praising systems that can find suspicious patterns such as when two seemingly unrelated accounts sharing a common address.

Add to this the growing concerns around fraud and the opportunities for executives to use a single system to address financial crime including AML and fraud across their business.

Financial regulations and guidance increasingly direct companies to assess risks and tailor compliance systems to address the company's own risk analysis. Regulators now expect firms to report violations by themselves, saying they will look far more kindly on self-reported violations than those violations that come to the attention of regulators through tips or examinations. Regulators also expect to see clear audit trails, documenting the origin of suspicious activity, locking down the data, and outlining the steps a company takes to investigate and resolve alerts.

Span the Enterprise

It's not just regulators that want to see a unified database for compliance purposes. Top industry compliance officials recognize that getting 50 reports a day from 25 different in-house systems is a losing proposition for preventing and detecting expensive regulatory failures. Wrongdoers don't limit their schemes to one business unit, one account, or a product type.

Overtaxed compliance staff will miss hard-to-detect patterns of wrongdoing in these overgrown—often homegrown—compliance systems that silo data. Running multiple applications on a common platform reduces costs, inefficiencies, and risks. It also allows you to see what is going on from a macro or micro level throughout your organization, analyzing if you have a problem business unit, a troubled branch office, or a rogue employee. And if your enterprise is global, you'll need a system that can handle multiple currencies, time zones, and dates.

The importance of deploying enterprise-wide solutions cannot be overstated. They offer the highest assurance of meeting regulatory requirements and detecting potential violations. Robert Iati, research director for TowerGroup, has noted the key role that enterprise-wide solutions play:

- Implementing compliance systems should no longer take a "do just enough to appease the Feds" approach. Rather, forward-thinking institutions should seize this opportunity to leave their "fire-drill" tactics in the past, and build holistic systems that gaze across the enterprise to offer protection for not only the immediate regulatory concern but, more importantly, provide a solid foundation for meeting all future compliance needs.

Detect all Suspicious Behavior Quickly

Your system should find all suspicious patterns of wrongdoing. That means a system that looks at every transaction and every account all the time—a system that searches for new patterns of suspicious behavior every day or in some cases, intraday. Periodic sampling for problems leaves you, your firm, and your customers exposed. With sampling you will miss violations. If you run your batch cycle every month or quarter, you delay the discovery of mounting problems.

A system that monitors every day, needs to do so expertly, minimizing false positives so that compliance analysts do not become overwhelmed. You want to zero in on real red flags, not try to separate the real red flags waving in a sea of false ones. Expert algorithms and carefully crafted patterns of suspicious behaviors to run against your data keep false positives at a manageable level.

One hallmark of a tightly designed system is its ability to find meaningful trends and abnormal changes compared with normal account or customer behavior. For example, if some customers routinely make a large number of trades, the system should be smart enough to send you an alert only when those customers increase their trading activity by an amount that exceeds their normal trading levels.

When alerts of suspicious behavior arrive at the desks of compliance analysts, time and money will be saved if those alerts come with all the data and information that analysts need to start making decisions and recommendations on courses of action. Systems that tell only half the story and force analysts to gather additional data from other systems to begin their work, dramatically increase costs and decrease the quality of compliance systems.

Reflecting Industry Best Practices

The best compliance systems reflect the wisdom of business and compliance executives across the financial industry on what constitutes suspicious behavior and the best possible way of detecting

potential violations. Compliance systems are enriched by the experience of others, who have tested various methods to catch wrongdoers and know what works and what doesn't.

Building on the experience of others saves money and increases the likelihood that a company's system will work well and reflect the best practices in the industry. To capture and leverage that wisdom, business and compliance executives need to meet regularly with their counterparts, translate that wisdom, and apply it through algorithms and databases.

Be Easy to Use and Change

An AML compliance system needs to be flexible, easy to use, and easy to change. Who could have predicted three years ago the rapid pace of regulatory change we see today? Laws change, regulations change, and wrongdoers change. New products with new risk profiles rapidly enter the market and business culture changes just as fast. Overnight, standard business practices that were once the norm become the subject of investigations and headline-grabbing enforcement actions. In addition, regulators can send letters asking firms to produce ad hoc reports that require extensive and costly database searches on a moment's notice.

Business and compliance executives highly value compliance systems that anticipate this dynamic environment and allow business users and programmers to quickly and inexpensively change what a system can detect while simultaneously keeping a record of all changes as required by the rules. In many cases, executives are analyzing the value of systems, based on the number of changes that a business user can easily make to the system without the help of a programmer because bypassing a programmer saves time and costs.

Provide Long-term Cost Effectiveness

AML compliance systems must be cost effective over the long term. If your business is successful, the amount of data you are handling will continue to grow, but many a 'great' system with great functionality attained that standard for just a snapshot of time and then fell into disrepute as data volumes grew and technological and financial innovations passed it by. Effective systems, including compliance systems, must be easy and affordable to maintain over the years.

Key Considerations for an AML System

Key Components of an AML Compliance System

Figure 1 summarizes the key components of an AML compliance system that organizations must consider. This is helpful when estimating costs of a build versus buy decision as well.

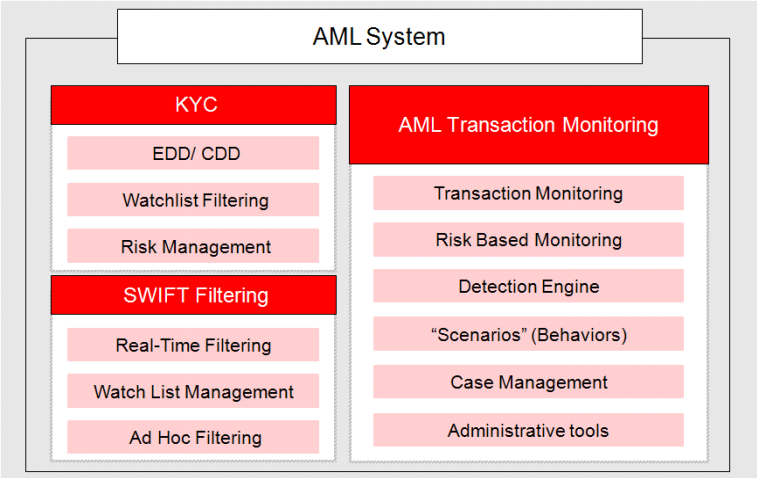

Figure 1. Typical Requirements f or an AML System

Key Questions to Ask about the Data

The following key questions need to be addressed with your business and IT staff.

What suspicious behaviors are built into the system to indicate violations or wrongdoing?

Because you need an enterprise-wide solution, start making a list of suspicious behaviors and be sure to include behaviors that cross business lines and product types. You will not only want to include obvious violations of existing laws and regulations, but you may also client behaviors that could expose your firm to financial losses.

This is an important checklist to see if the systems you are looking for address these behaviors out of the box.

How does the system detect these behaviors in the data?

Once you have identified behaviors you want to detect, you then need to identify the data that will flag the behaviors. You need to consider how data can help you separate suspicious behaviors from innocent ones.

For example, you want to know about accounts that experience a large depreciation in account worth because the losses may be caused by wrongdoing on the part of a broker assigned to that account, identity theft, or money laundering. But you'll also want to take into account these questions:

- Does it matter how the depreciation occurred? Was it a loss in the value of holdings or were funds transferred out?
- Does the destination of the funds matter? Did the funds leave the firm or were they moved into another account held by the client at the firm?
- What is a large loss? Do you want to measure it by dollars, by the percentage of loss in the account as a whole, or by both criteria?

- Does a large loss of more or less concern depend on the type of account? Is this loss in a retirement or a hedge fund account?
- Over what time period would large losses be of concern—days, weeks, months?
- Is the loss of greater concern when another account change occurs at the same time, such as another beneficial owner being added to the account?

How does the system correlate detected behaviors to find hidden and non-obvious patterns in the data?

Though, detection engines are an essential tool to detect behaviors and should be employed by financial institutions, they do generate a lot of false positives. As a result, detection engines by themselves are not sufficient and add to the compliance cost as false positives tend to reduce efficiency and increase the cost of an AML program.

But if the system has capability to correlate results of seemingly unrelated detections, it can unearth some interesting patterns and help compliance users bring out high interest and highly suspicious behaviors to the forefront for analysis and investigation.

Ability to correlate is an important functionality that compliance stakeholders should weigh in on before choosing a compliance solution.

What type of derived data is useful in detecting these behaviors?

For example, does the system allow you to aggregate activity of different types and use fuzzy name matching on watch lists?

What workflows should the system support?

- What type of actions can be taken to address the behavior?
- What information is stored to support the decision?
- What type of review of actions taken is provided?
- Is there a mechanism to rank the importance of alerts and order the sequence of investigations?
- Can the information be linked to other systems, such as a currently used case management system?
- What types of reports are generated to spot trends in the actions of analysts or customers?
- How are actions tracked for audit purposes?
- Can the alerts generated be assigned to the right analysts for review? What data is provided along with the alert to help with these reviews?

What are the commonly used reports and dashboards according to industry best practices that are necessary for management of an AML program?

An AML compliance program is going to rely on data coming in from transaction systems. However in the process of monitoring this input data stream, it is also going to generate some of its own data that will identify:

- The suspicious behaviors detected systemically and manually
- The decisions taken by the systems based on detection algorithms and correlation rules
- The decisions taken by compliance analysts and investigators on a potential suspicious activity

It is crucial for stakeholders and program managers to have access to this information for measuring the performance of the program and for identifying and addressing any process bottlenecks.

A library of industry wide accepted commonly used reports and dashboards should be defined for providing visibility into the underlying business process and measuring the effectiveness and efficiency of an AML program.

What are the reports that are unique to you due to data requirements unique to your institution?

Data in financial institutions is not the same. Hence it is impossible to meet all the reporting and information visibility requirements by providing commonly used reports and dashboards to the end users. It is vital for reporting and analytical functions in an AML system to be flexible and easy to extend so that compliance users can retrieve the information they need by:

- Defining their own reports and dashboards.
- Defining Ad Hoc queries and reports to retrieve the information they need.

What are some of the additional IT requirements that help you determine if the system fits within your organizations IT standards?

- What is the implementation environment (language, third party tools)?
- Does the system use a Web-based or desktop client?
- How does the system integrate with enterprise security?
- How much data is retained? How does it manage unretained data?
- What system maintenance is required? Are the necessary tools in scope?
- How is data from source systems integrated and loaded?
- What logging and audit controls are provided? How are they maintained?
- Can a business user be able to change the behavior detection parameters without involving a programmer? What tools will this require?

AML systems that meet these business requirements and fit into the enterprise infrastructure tend to perform efficiently, meet security requirements, and provide a comprehensive compliance solution.

Additionally the system should provide the ability to calibrate different behaviors through parameter and threshold settings.

Oracle Financial Services: A Comprehensive Financial Crime and Compliance Management System

Oracle Financial Services is the only enterprise-wide solution that enables financial services customers to deploy multiple compliance applications on a common platform. The Oracle Financial Services behavior detection platform serves as the foundation for the industry's most comprehensive suite of financial crime and compliance management applications, including

- Oracle Financial Services Anti Money Laundering
- Oracle Financial Services KYC
- Oracle Financial Services Fraud
- Oracle Financial Services Trading Compliance
- Oracle Financial Services Broker Compliance
- Oracle Financial Services Case Management

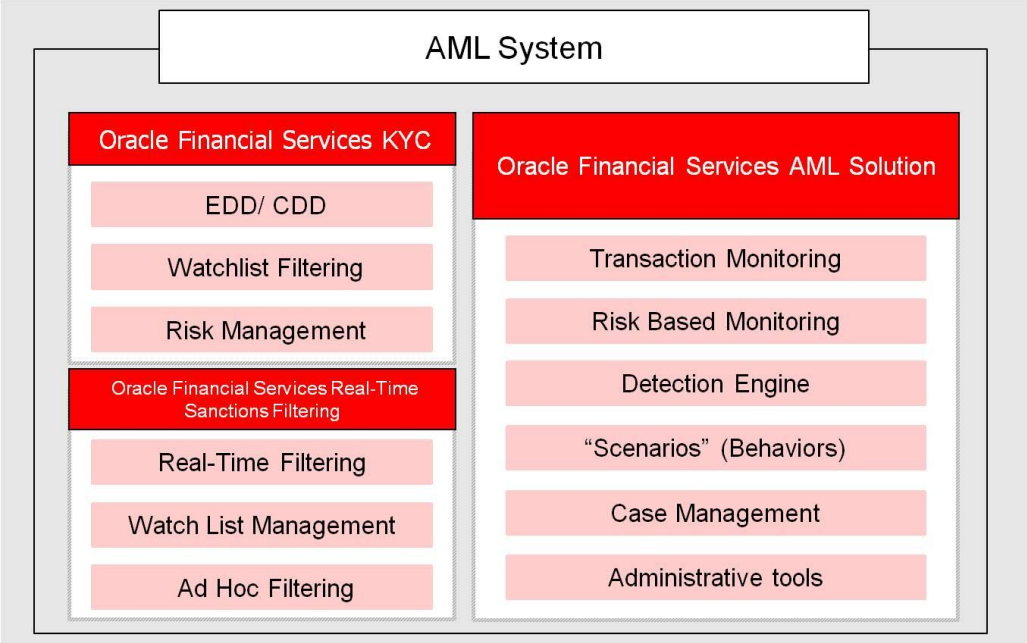

Figure 2. Oracle Financial Services Anti-Money Laundering

Oracle Financial Services suite of applications immediately delivers the benefits of improved risk management and reduced technology overhead through the adoption of one common platform for all compliance requirements, across multiple business units, client bases, and financial products.

To identify potential compliance violations and patterns of wrongdoing, Oracle Financial Services employs customizable behavior detection "scenarios" that identify and analyze hundreds of compliance

challenges—from insider trading to client suitability, from anti-money laundering to abusive squeezes, from identity fraud to mutual fund abuses.

A key innovation in the Oracle Financial Services behavior detection platform is a unified data model and analytics layer that provides "plug-n-play" scenario detection, fast and easy deployment, and the ability to enhance existing implementations with minimal disruption or downtime. This unified data model further complements a unified reporting and analytical capability to provide comprehensive business intelligence across all compliance initiatives. The platform powers all Oracle Financial Services applications, giving users greater flexibility to tailor a compliance solution to specific business needs and risks. While Oracle provides new scenarios and updates as regulatory requirements change or new types of wrongdoing evolve, the system also comes with a toolkit that allows customers' developers to create scenarios on their own. The toolkit provides an organization with complete control and the ability to customize scenarios to fit any unique circumstances or internal risk judgments.

The Oracle Financial Services behavior detection platform incorporates advanced case management functionality that allows users to manage risk alerts. It uses an integrated case management solution featuring a rich workflow and document management system. New e-mail capabilities enable automatic alert notification and alert forwarding. The platform also provides greater protection and risk management to customers through intraday ingestion, detection, and enhanced risk scoring to better identify and prioritize alert workflow. The application also supports local and global deployments with multiple language support, multiple currency support, and multiple date and time zone functionality.

Important Considerations for the AML System

The following sections examine in depth the key components of the Oracle Financial Services behavior detection platform—functionality organizations should consider as they consider whether it makes sense to create a comparable system from scratch or from other vendors.

Algorithms and Scenarios

Oracle specializes in developing sophisticated algorithms that can detect illegal behaviors quickly across several data combinations. The tools Oracle has developed—sequence matcher, link analysis, outlier detection, and rule matcher— allow firms to find potential violations that would go undetected in the simpler compliance systems developed and used by most firms.

Many firms rely on scripts to detect wrongdoing. Compliance staff at these firms are forced to review dozens of reports and unfortunately will never pick up patterns of wrongdoing that come to light only when you can combine many variables in one report or an alert.

For example, the Oracle scenario allows a firm to configure sixty different parameters to look at rapid movement of funds through wires. The scenario evaluates the flow of funds through an account, looking at relative incoming to outgoing and comparing to the retained net worth of the account. The parameters can be set separately based on whether the account is new or seasoned and based on the risk levels associated with the account and with the other parties on the wire. A single threshold set evaluates each threshold considering these dimensions in a single scenario run.

The scenario can also apply filters to include or exclude specific account types and specific transaction products. The scenario accounts for results of past investigations by allowing transactions between "trusted pairs" (i.e., relationships that have previously been investigated and cleared) to be ignored, or to be included and the ratio of trusted transactions to be used in scoring the alert.

The scenario leverages threshold sets to allow detection to be performed at different threshold settings for different client segments (e.g., use different values in monitoring your Private Client business than your retail business).

When we compare this one Oracle scenario on rapid movement of funds with scripts, it would potentially take many dozens of internally developed scripts to replicate this single scenario. Not to mention that the Oracle scenario can handle multiple currencies and be sorted by different regions, jurisdictions, or business units.

Developed, Tested, and Refined over Time

One of the primary reasons business and IT executives choose the Oracle Financial Services behavior detection platform is that its algorithms and scenarios reflect the seasoned judgments of various top business, compliance, and IT executives at global leaders in the financial industry. Additionally, its scenarios are developed by highly skilled data miners with more than seven years of experience on average. It is costly and risky to reinvent this domain expertise on your own without the benefit of the many changes and refinements that come from using a system over time across many firms.

Table 2 highlights several advantages that Oracle Financial Services scenarios hold over an organization's internally developed scripts for its solutions.

Oracle Scenarios	Internally Developed Scripts
Each scenario supports many thresholds that consider variable business conditions to reduce false positives	Creating rule sets that support many thresholds and business combinations is complex and subject to high error rate
Multiple parameters (thresholds) that can be configured on the fly	Hard-coded scripts must be opened up to change thresholds
Business users can change thresholds	Scripts can be changed by programmers only
Scenarios are tested on multiple clients to eliminate programming inaccuracies	Scripts are subject to programmers interpretation of what is correct
Scenarios include open source documentation and complete audit trail of scenario changes	Scripts are difficult to document correctly as thresholds are added and modified usually with no automated audit trail
Surveillance tiers and threshold sets allow innumerable variations on the same scenario without having to copy and edit each time	Scripts must be copied and edited each time to support variations
Algorithms, industry-standard variables, and scenario toolkit are out of the box for faster time to market	Scripts cannot easily leverage predefined, tested, and configurable algorithms and calculations

Table 1. Benefits of Oracle's scenarios compared with internally developed scripts

Data Management

Oracle Financial Services Anti Money Laundering provides a fully integrated data model, data warehouse, and data normalization covering all aspects of trading and account activity. Experienced business and IT executives see enhanced value in buying versus building the Oracle Financial Services data management solutions because the platform delivers a common and open data repository that

- Supports all Oracle Financial Services financial scenarios, from anti-money laundering and best execution to detecting broker sales practice abuses
- Supports all major asset classes (products) worldwide
- Defines a standard and comprehensive data dictionary for all financial business domains
- Ensures consistency in data quality
- Processes ever-growing data volumes efficiently and quickly to meet the reporting demands of compliance
- Incorporates best practices gained from the Oracle Financial Services user community through a defined product process
- Meets regulatory demands and requirements for data isolation and retention

Business Information Correlation

Oracle Financial Services Behavior Detection Platform includes a sophisticated business information correlation engine that is used to correlated systemically detected suspicious activity by the behavior detection engine. It supplements the behavior detection efforts by linking seemingly unrelated behaviors with each other and deriving hidden relationships and networks.

The Oracle Financial Services correlation capabilities are not limited to only behaviors that are detected by the Oracle Financial Services behavior detection engine. Oracle Financial Services supports standard interfaces for institutions to post any other suspicious and/or fraudulent behavior into the Oracle Financial Services system for consideration by the correlation engine for linking and identifying hidden relationships and networks.

The Oracle Financial Services correlation engine:

- Provides a configurable and flexible definition layer where institutions can define their own correlation rules and criteria
- Provides ability to correlate alerts and events based on similarities identified in directly or indirectly related business information associated with that event
- Supports risk based scoring of the derived correlations
- Supports the ability to take automated actions based on the derived correlation. For example, institutions can configure the system to generate automated cases based on the potential risk of an identified correlation

Enterprise Case Management

Oracle Financial Services Case Management is a comprehensive, enterprise-wide investigations platform. Compliance analysts and investigators use Oracle Financial Services Case Management to meet the increasing demand for higher productivity, when it comes to triaging alerts and investigating cases, and improved accuracy. Oracle Financial Services Case Management:

- Automates processes and reduce the cost of investigations with case management capabilities built-in for financial crime.
- Meets internal and external service level agreements while maintaining high quality investigations and analysis
- Achieves multi-channel coverage across all financial crime and compliance functions
- Supports tools and features that help improve the overall user productivity and assist in effective decision making.

Analytics

Automated monitoring of customer activity and a comprehensive investigations process is a natural first step to achieve this, but today's atmosphere also demands a 360o oversight of financial crime and compliance program activity to ensure business continuity and a high return on investment. Oracle Financial Services AML and Fraud Analytics help measure program effectiveness and show areas where enhancements could assist in meeting ongoing or future demands.

Oracle Financial Services AML and Fraud Analytics offer business intelligence and analytical reporting that provides clear operational visibility into Financial Crimes and Compliance Management program performance.

Some important capabilities of the Oracle Financial Services AML and Fraud Analytics offering are:

- Provides out of the box comprehensive data coverage for financial crime and compliance management
- Supports sophisticated analytical reporting and interactive dashboarding capability
- Built on an extensible and flexible Oracle Business Intelligence platform, delivering lower total cost of ownership

Regulatory Reporting

The accurate and timely submission and filing of regulatory reports with regulators and law enforcement officials continues to be an integral part of the war on financial crimes like fraud, money laundering, terrorist financing, and drug trafficking. Oracle Financial Services Anti-Money Laundering (AML) Regulatory Reporting and Oracle Financial Services Anti-Money Laundering (AML) Electronic Filing assist financial institutions with gathering investigation information, generating regulatory reports and filings for submission with regulatory bodies as part of an integrated financial crime and compliance management program.

Some key capabilities of the Oracle Financial Services AML Regulatory Reporting and Electronic Filing offering are:

- Provides global coverage of regulatory reporting requirements
- Provides pre-built integration with Oracle Financial Services investigation process i.e. Oracle Financial Services Case Management
- Supports comprehensive report management and report workflow capabilities

Product Components

Oracle Financial Services provides an integrated, end-to-end solution covering everything from data ingestion to case management.

- Data ingestion engine
- Alert management
- Detection and activity matching software
- Case management
- Pattern analysis logic software
- Reporting engine
- Watch list and fuzzy name matching
- Security model
- Data warehouse management and maintenance software

Risk Management

The Oracle Financial Services behavior detection platform and associated applications are already aligned with the process of testing of internal audits and regulatory examination followed by banking and securities regulators and compliance and audit staff of global leaders in the financial industry.

When it comes to accuracy, Oracle Financial Services reflects the efficiencies standards prevailing in the industry. Internal builds and other systems can produce a large number of false positive alerts that overwhelm compliance staff. Unfortunately, when faced with a large number of false positives, some internal build teams increase the risk of missing real violations by suppressing alerts by trying to reduce false positives.

Another area that bears scrutiny is considering how the system will accommodate a changing regulatory and market environment. Because regulatory and business requirements change rapidly and in some cases, unpredictably, the Oracle Financial Services platform is designed with the inevitability of change in mind. The costs of adding new scenarios, new patterns, or linkages that can detect violations

or wrongdoing are not only considerably cheaper, but once again, they reflect the considered judgments and experiences of industry leaders.

Making a Decision

Table 3 provides a checklist of actions and final cost considerations to help ensure you effectively analyze the decision of investing in an AML system.

Category and Criteria	Oracle Financial Services	Build/ Other Vendors
Intellectual property		
Scenario development	√	
Data model design and development	√	
Product components		
Data ingestion	√	
Data mining tools	√	
Detection and activity matching software	√	
Pattern analysis software	√	
Watch list and fuzzy name matching software	√	
Alert correlation and management	√	
Case management	√	
Reporting engine	√	
Advanced analytics		
Data warehouse management software	√	
Documentation	√	
Implementation		
Planning	√	
Data acquisition	√	
Testing	√	
User acceptance testing	√	
Risk management		
Regulatory expertise	√	
Reuse	√	
Accuracy	√	

Table 2. Checklist for analyzing the build versus buy decision

Cost Considerations

Whether you build or buy, achieving a best practices compliance solution takes time and money. In comparing the costs of each alternative, top business executives consider the costs, if one path exposes their firm and senior executives to a greater risk of regulatory failures, substantial fines, and reputational damage. So when choosing a solution, they consider long-term total cost of ownership, efficiency for business users, and regulatory and reputation risks as well as the near-term costs for developing and implementing compliance solutions.

Building a compliance system from scratch, or even using a toolkit approach, has a number of inherent risks that are minimized with an off-the-shelf product. Internally developed solutions and products requiring substantial build efforts can and usually do translate into a host of risks and costs:

- Longer time to market
- Lower likelihood of consistency with peers and implementing best practices
- Reduced ability to modify applications as requirements evolve
- Less centralized information
- Greater difficulty to document, maintain, and upgrade
- Higher total cost of ownership over multiple years

Anticipating and analyzing these broader risks and costs is central to correctly measuring the long-term costs of the build versus buy alternatives.

Conclusion

The choice of an AML system, and for that matter a compliance system, may be one of the most important decisions you make. This white paper helps you develop a thorough framework for analyzing the pros and cons, based on the real-world experiences of others who have traveled the same path. Whatever decision you ultimately make, we hope it adds considerable value to your analytical processes and helps your institution comply with its compliance mandates with utmost ease.

Best Practices for Anti Money Laundering (AML) System Selction and Implementation
March 2011
Author: Gaurav Handa, Gaurav Harode, Karen Van Ness

Oracle Corporation
World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065
U.S.A.

Worldwide Inquiries:
Phone: +1.650.506.7000
Fax: +1.650.506.7200

oracle.com

Oracle is committed to developing practices and products that help protect the environment

Hardware and Software, Engineered to Work Together