FinScan®

The Compliance Officer's
Complete Success Guide to

EVALUATING AND SELECTING AML COMPLIANCE SYSTEMS

Table of Contents

Preparing for the Change **1**

Evaluating Your Current Compliance Program Identifying Challenges **2**

Data Quality 3

False Positives 5

Manual Processes 7

Risk & Coverage 9

Reporting 11

Exploring Alternative Systems Evaluation Criteria **13**

Accuracy 15

Efficiency/Workflows 18

Automation & Batch Processing 20

Migration Methodology 22

Performance & Scalability 24

Training 25

Data Agnostic 26

Are You Ready? **36**

Preparing for the Change

To ensure your organization's success in this complicated compliance environment, you must be armed with an innovative, efficient, and multifaceted compliance screening solution. Such a system would be so advanced that, as the regulators become stricter and the regulations surrounding compliance continue to grow in number and complexity, you, your compliance team, and your organization will be well positioned to meet the risks and needs you face now and in the future.

Because you are reading this guide, the assumption is that you are contemplating the idea of or are actively searching for a new anti-money laundering (AML) compliance screening system. While migrating to a new system can be a daunting and challenging task for any compliance team, reading this guide means you have taken the first step in ensuring your team's survival through the regulatory jungle.

This guide will bring to light the many questions you should be asking yourself regarding your current tools and applications and whether you have the capabilities required to stay on top of today's regulatory compliance demands.

This guide to evaluating compliance systems will prepare and show you how to:

- Assess your current compliance program
- Determine the gaps in your current system and identify your needs
- Evaluate and compare alternative systems

Evaluating Your Current Compliance Program Identifying Challenges

The first step to successfully selecting and adopting a new solution, platform, toolset, or application begins with an evaluation of your current processes and system. Before you can choose a new approach, you should have a complete understanding of what capabilities and components you'll need to improve your outcomes from what they are today. The following four sections will assist you and your compliance team in identifying the problem areas and unmet needs in your current processes and systems.

We will explore the common challenges of:

- Data Quality
- False Positives
- Manual Processes
- Risk & Coverage
- Reporting

Challenge: Data Quality

Most organizations know that poor data quality can have devastating consequences not just for IT, but for compliance operations from both efficiency and risk detection perspectives. While poorly structured data and inconsistent formats can create questionable matches requiring significant investment in personnel to manually review them, even more potentially serious impacts are reputational risks and financial penalties when sanctioned entities go unnoticed due to inaccurate data and matching.

To address the data quality issue, compliance professionals typically seek help from their internal IT teams. If the resources are available, IT can offer some preliminary improvements, but even then, they typically fall short on delivering data that is fit for compliance screening. Organizations maintain customer or product centric databases that fail to consider joint names, duplicates, names in address lines, missing data elements, and inconsistent formats – all of which can have a considerable impact on uncovering risk. Therefore, it is vitally important that you work with your vendor or IT team to identify the data quality issues that are specific to your business.

Questions to ask yourself:

- ✓ Are we screening all the individuals and entities in our system even when they are mentioned as joint accounts or in non-name lines such as address lines?

- ✓ What is the cost of missing a true hit?

- ✓ How many data sources are we screening for risk? How does each of these source systems rank on data quality such as accuracy, completeness, consistency, and uniqueness?

- ✓ Do we know exactly what data errors are feeding false positives such as noise words, titles, and dummy data? How can we stop these errors from getting into the screening system?

- ✓ How many duplicate customers do we have? Do we screen and remediate the same alert multiple times? How can we apply remediation decisions to the same customer when they appear in multiple alerts – and improve productivity? What productivity gains can we achieve with such a feature?

Challenge: False Positives

The largest single catalyst triggering most organizations to search for a new AML compliance system is a desire to reduce the number of false positive results bogging down compliance teams. Our decades of experience have shown that the most common challenges with existing compliance software programs are data quality issues that lead to inaccurate outcomes.

Of course, a reduction of false positives must be achieved without increasing the risk of missing true hits. Although false positives can be frustrating, some level is unavoidable, though advanced technology can help minimize them significantly. It is vitally important that you identify the baseline number of false positives your current solution is producing to demonstrate the need for improvement and, later, the return on investment (ROI) of your new solution.

Questions to ask yourself:

- How many hits are we receiving each day? What level of hit rate would we consider optimal?
- What's our typical level (ratio) of false positives on a daily, weekly, or monthly basis? What's the desired ratio we'd like to achieve (recognizing that there will always be some)?
- What level of staffing is currently deployed to clear matches on a daily basis?
- To what extent are matches cleared fully each day? If less than 100%, then what's the typical backlog remaining from one day to the next? What is the condition of the input data? Do we have the tools or resources to improve data quickly and effectively?
- Do we know exactly why we are getting certain types of alerts?

Challenge: Manual Processes

Manual processes are time consuming and prevent compliance teams from doing their jobs and responding to risk efficiently. Therefore, it is crucial to identify the bottlenecks in your current process.

- What does your team currently do manually?
- How much time do your people spend on tasks due to the inefficiencies of your system?

Evaluating what your team does on a daily basis can often pinpoint processes created to work around a problem but are not the most efficient ways to accomplish a task. Review all your workflows and the processes you use to review and clear hits.

Questions to ask yourself:

- ✓ Which of our current processes are inefficient?
- ✓ What are our current manual processes and tasks? Can those processes be completed in a different workflow?
- ✓ How long does it take to review and clear one potential hit? How long are we spending clearing all the hits?
- ✓ Is our team able to multitask on different processes, enabling people to review and report hits more rapidly?
- ✓ Which steps are creating bottlenecks in our process? Which steps do we wish were automated?

Challenge: Risk & Coverage

What lists are you screening against today? Your legal team can advise you on requirements based on your jurisdiction which you can incorporate into your risk-based approach. But you may need or want to screen beyond just what is required and screen against more comprehensive lists from a third-party data provider. These lists give you significantly greater coverage of Politically Exposed Persons (PEPs) and their associates, negative news, and other information that can keep you compliant and off the front page of any newspaper.

Questions to ask yourself:

For the compliance lists we use today:

- Do they adequately address what we need to screen against?
- Are they updated frequently enough? If not, how often are they currently updated and what frequency would be ideal?
- Are list updates automatically managed and maintained by the vendor?
- Are there any additional internal lists or block lists that need to be automatically populated into our system? If yes, then how are they maintained and uploaded to the system?
- Are we able to easily see and review all necessary information on the compliance profiles to clear our alerts?
- Can different divisions in our organization screen against different sets of lists based on their needs?

Challenge: Reporting

As you know, screening your customers, partners, and vendors and reviewing the resulting hits is only part of your job when it comes to your AML compliance program. You also need to show internal auditors and external regulators that your compliance screening processes are efficient and effective.

Your team should be able to rely on the accuracy and completeness of reports generated by your compliance system, and they should be able to generate, with little effort, customized reports of exactly what they need to see.

Questions to ask yourself:

- ✓ Is our system able to generate reports? If so, are we building and formatting our reports manually?
- ✓ What types of reports do we need that we cannot get today?
- ✓ Are we able to generate reports on more than just the compliance outcomes, for internal use, such as productivity monitoring?
- ✓ How about reports for external use, such as audit logs? How easily are these reports created and accessed?
- ✓ Can we export the reports in various formats?
- ✓ Can we retain frequently used reports to save time and improve consistency?
- ✓ Can we export data to BI systems for detailed analysis?

Exploring Alternative Systems: Evaluation Criteria

Now that you have a clear understanding of the gaps in your current compliance program, you are ready to evaluate your options.

Before you jump in with both feet and choose a new system to battle your way through myriad compliance standards and regulations, it is imperative to thoroughly evaluate potential new systems to identify the one that best fits your needs.

This step is often overlooked, as some companies quickly adopt an inexpensive “out-of-the-box” solution and hope (and expect) it will solve their problems. While they might find a solution that looks like it will work – and it might for the first few months – many firms and their compliance teams face the issue of a system that “breaks down in the middle of the road.”

Whether it was because the system wasn’t scalable or configurable, couldn’t fully integrate with their existing infrastructure, or didn’t offer an efficient way to review matches, compliance teams that jump the gun without fully evaluating their current and growing needs end up having to start the entire search process over again.

Much advancement in compliance screening has been achieved over the last few years. Your organization requires an effective solution that accurately and efficiently identifies possible risk while providing intuitive tools to review, track, and report on results. The compliance solution provider should also offer ways to improve your data quality, the expertise to advise you on the latest regulations, scalability, and many more critical features.

Here, we provide seven primary criteria on which you should evaluate potential compliance screening systems. This will also arm you with the tough questions your potential provider should be able to answer.

We will explore the following evaluation criteria:

- Accuracy
- Efficiency/Workflows
- Automation & Batch Processing
- Migration Methodology
- Performance & Scalability
- Training
- Data Agnostic

Evaluation Criteria: Accuracy

Accuracy is the primary consideration when evaluating potential compliance systems. The question on every compliance officer's mind is, "How do I make sure I don't miss any critical hits while minimizing the number of manual reviews?" The answer to that question is to choose a compliance system that uses a sophisticated, modern matching methodology that leverages the strengths and avoids the weaknesses of your customer data.

Because your customer data is different than every other organization, so should your matching criteria and approach. To be optimally effective, the algorithm must allow you to match on any reliable fields you have in your records that are also present in the compliance lists.

Nearly every modern compliance system enables "fuzzy matching" logic (e.g., Jhon Smith matching John Smith, dates of birth within x years of each other), but that alone does not make them comparable. One common approach uses a weighted scoring method, where each field (last name, nationality, date of birth, etc.) is given a weight based on its importance and a score based on its match quality.

However, this approach does not account for the specific context of how or why certain records matched. Further, sets of matched records could be assigned the same aggregate scores even when different fields triggered the alert. This "black box" approach lacks transparency which can make it challenging to explain to a regulator the rationale for your decision (i.e., you will want to provide better reasoning than the matches being under or over a certain score).

An **alternative matching approach** enables you to determine match quality based on the contextual differences between two records for each individual field used for matching, and not aggregate scores. This allows you to build a highly granular screening system that considers existing data conditions and provides transparent reasons for a match. It also drastically reduces your number of false positives and false negatives by giving you much more control over your matching logic.

In addition, it greatly enhances your ability to demonstrate your control framework and explain your decisions to regulators who will be pleased to hear "We didn't file a report because the customer had exact matches on first name and nationality, but only a close date of birth and unequal last name."

Additionally, advanced compliance systems offer sophisticated **data quality solutions** that can analyze, cleanse, de-duplicate, and identify hidden names in joint accounts and address lines within your customer records. Better data quality can also illuminate inconsistencies and identify potentially fraudulent customers within your database. This will reduce the number of records being screened while increasing the quality of those records, ultimately lowering the number of potential hits that will need to be reviewed by your team.

Be sure to evaluate the strengths of a potential provider's matching methodology. Make sure it can be tailored to your specific data and your risk-based approach and that it can be explained to a regulator. Doing so will eliminate risk and reduce costs.

Questions to ask a potential provider:

- ✓ What is your matching methodology and how is it different from that of your competitors?
- ✓ Do you provide documentation of your matching methodology so that we can easily explain it to auditors and regulators?
- ✓ Upon which fields other than “Name” are we able to match?
- ✓ What level of accuracy does your system provide in both missed hits and false positives? How does this level compare to that of competitive systems?
- ✓ To what extent can we customize the rules that govern matching, such as loose rules vs. tight rules, or something more granular?
- ✓ In what way are different matching rules able to be applied by compliance list and internal data source?
- ✓ In what ways can your product predict the volume of hits by match type to enable stepwise control of our risk against our review resources?
- ✓ How do you identify and eliminate duplicate records that exist across our databases?
- ✓ How do you identify sanctions risk in records where the customer name is in a non-name line?
- ✓ How does your product deal with different naming conventions in non-English languages and character sets such as Cyrillic, Arabic, Chinese, etc.? Does it incorporate culturally sensitive matching technology or does it rely on a transliteration function?

Evaluation Criteria: Efficiency/Workflows

In most organizations, it's likely that processes within your current program require manual effort. Such manual steps not only increase the potential of error, but they also increase your operating costs unnecessarily. The right compliance screening toolset should decrease risk, manual interventions, and their associated costs within your overall compliance screening, reviewing, and reporting program.

When seeking a new system, focus on a solution that has an efficient and comprehensive tool for reviewing and reporting potential hits. The optimal solution should enable your compliance workforce to quickly process matches without error, decreasing the time and resources required for reviewing.

Many out-of-the-box systems and homegrown solutions require external storage of results and reports in spreadsheets and PDFs, all of which can cause significant issues for your team. Not only does this create an unwieldy system that is difficult to work with, but when auditors or regulators request certain information, these manual processes significantly slow down response time and potentially lead to incorrect reports.

Manual processes steal resources from your necessary day-to-day compliance work. Your compliance solution should allow for easy reporting at the click of a button and storage of additional/backup materials within the solution.

Questions to ask a potential provider:

- ✓ How do you help reduce or eliminate our manual processes?
- ✓ What types of reporting options do you offer, and how easily does your system generate them?
- ✓ How will your review tools reduce review time?
- ✓ What specific functionalities or capabilities are included in your review tool to increase efficiency?
- ✓ To what extent can you customize your workflow and case review tool?
- ✓ Aside from screening reports, are we able to generate reports on the review process for management dashboards?
- ✓ How do we access match history and audit logs?
- ✓ Do you have an estimated ROI of how your system will improve our bottom line?

Evaluation Criteria: Automation & Batch Processing

Automated screening has become the expected norm in AML compliance. The integration of real-time screening into customer onboarding or payment processing systems typically reduces risk. Accurate results are imperative, as false positives during real-time transactions can have a negative impact on your customer interactions.

Also, for companies with large data files of customer records, an AML compliance screening system must be able to run the records in a batch process. It should also be able to perform the task relatively quickly within your required processing window without increasing risk or unnecessary downtime.

Questions to ask a potential provider:

- ✓ How does your system allow for automated screening via APIs/web service calls?
- ✓ What systems or software can be integrated into your compliance system, e.g., a CRM or customer onboarding system?
- ✓ How does your product process real-time or ad-hoc screening to ensure it does not slow down our business operations?
- ✓ Does your system support batch screening of our records?
- ✓ What are the various ways we can process our screening data? (e.g., batch, real-time, via API, etc.)
- ✓ What are our options for processing platform deployment? (SaaS, on-premise, etc.)

Evaluation Criteria: Migration Methodology

When evaluating new systems, making your selection is only half the challenge. It's essential to evaluate a solution provider that has a wealth of experience performing implementations and system migrations. Find out if the provider can smoothly migrate your existing data and systems.

Regardless of how long you've had your current system, you're going to have a history you can't afford to lose. Your new solution provider must be able to integrate all the work you have already done, saving you the redundant effort of re-reviewing previously resolved matches. It is also critical to understand how historical data will be maintained and accessed to comply with regulatory requirements for record retention.

Before choosing a new system, it is imperative that you receive a project plan that lays out the detailed steps of the implementation and migration. The system provider should also be able to provide you with an estimated ROI of migrating to the new system based on costs and benefits, such as fewer false positives, speed and efficiency of screening, and integration with your existing processes and internal systems.

Questions to ask a potential provider:

- ✓ What experience do you bring to the table related to migrations?
- ✓ What tools do you have in place to help automate our conversion to the new application?
- ✓ What is your plan to migrate our existing system to the new solution?
- ✓ How do you enable us to migrate our historical data to the new solution?
- ✓ What's the pro forma implementation project plan?
  How is the workload divided between our staff and your implementation team?
- ✓ How do you support archiving prior data and decisions?
- ✓ Do you support our current AML data partner within your product? If not, would you consider such an integration on your roadmap?

Evaluation Criteria: Performance & Scalability

Another important aspect of the solution's performance is whether the system is scalable; that is, whether it can handle your screening needs as the number of records in your database grows.

While it may seem like a good idea to purchase a less costly system that can address your current needs, it may not be. When that solution begins to falter under the growing volume of records, you will have to begin this entire process again and find a new solution that can accommodate your growth. Make sure you ask the right questions to prevent this scenario.

Questions to ask a potential provider:

- ✓ What is the maximum number of records your system can handle?
- ✓ What percentage of your clients process the daily volumes we have, and how does this capacity translate into annual processing volume?
- ✓ Can your solution screen multiple client lists simultaneously?

Evaluation Criteria: Training

A new, modern compliance system with streamlined tools will require some training to get your team quickly up to speed so they can take full advantage of its capabilities. Your provider should offer both initial training during the implementation of your new system and advanced training for power users and administrators in whatever form is convenient for your team. This advanced training should allow your own employees to train new hires.

Questions to ask a potential provider:

- ✓ What training do you offer as a standard part of your solution?
- ✓ What advanced training options are available?
- ✓ Do you have a certification program for our internal users, enabling them to act as subject matter experts within our organization?
- ✓ How do you enable our internal team to train and upskill new employees without having to come back to you as the vendor?

Evaluation Criteria: Data Agnostic

Today's regulatory environment often requires organizations to screen beyond standard lists such as OFAC SDN, HM Treasury, or OSFI. As a result, many solution providers have partnered with data providers. Your solution provider should be able to offer a wide range of compliance lists and support a variety of enhanced third-party data sets.

Your new system should efficiently position you to keep up with constantly expanding and evolving compliance regulations. Additionally, the solution should be able to automatically feed any updates to compliance data into the system so that you are always screening against the most up-to-date data.

It is important to consider all aspects of your data provider, including coverage, cost, and accuracy.

Questions to ask a potential provider:

These questions depend significantly on your organization's screening obligations and requirements. You should adapt them to the types of screening you need.

- ✓ Can your solution support the screening of:
  - **Sanctions?**
  - **PEPs and RCAs?**
  - **Negative news?**
  - **Internal custom or block lists?**
- ✓ External proprietary lists? (e.g., Social Security Death Master File, healthcare and ESG exclusion lists, marijuana-related businesses, or other high-risk factors)
- ✓ What enhanced private risk databases does your system support? (e.g., LSEG Risk Intelligence, Dow Jones, Orbis Database, etc.)
- ✓ What compliance lists do you offer?
- ✓ How does your system screen multiple compliance lists simultaneously?

- ✓ In what ways do you support beneficial owner information?
- ✓ What’s required to integrate any other lists we want to use within your product?
- ✓ Can your solution utilize all our client record secondary identifiers, such as date of birth and national ID number?
- ✓ How does your solution apply different matching rules by list and source database?
- ✓ Does your solution support native character screening?

Additional Questions to Ask a Provider

Supplemental to the primary categories of evaluation are five additional areas you should question a potential provider about.

1 Hosted/SaaS Solution vs. Licensed/ On-Premise Deployment

Based on your scalability, cost, security, data privacy requirements, and national and regional regulations, your solution provider should have a highly experienced team to work with you to develop a flexible deployment strategy that fits your needs.

A hosted compliance system, also referred to as a Software as a Service (SaaS) solution, is when the software resides in a server environment maintained and controlled by the software provider. Hosted systems typically are quicker to implement and can be easier to maintain than installed software. Today's hosted systems are very secure, reliable, and should be able to support your data privacy regulations.

A licensed compliance system (also known as on-premise or installed) is when the software is installed behind your firewall and controlled and maintained by your own IT staff. Licensed systems are sometimes required by your Information Security team, so they should be consulted before you engage with a provider. On-premise systems can also be deployed in a private or public cloud as a "hybrid" deployment option.

Questions to ask a potential provider:

- ✓ Can your solution be installed on-site behind our firewall?
- ✓ Is your solution available as a hosted solution in a secure environment to meet our data protection requirements for certain countries?
- ✓ How is data protected internally on your hosted solution?
- ✓ To meet my regulatory and contractual needs, can you offer your solution in multiple instances?
- ✓ Can you offer hosted and licensed (on-premise) solutions at the same time?

2 Reporting

A system with built-in reporting functionality is an absolute must. Users and administrators should easily be able to generate any reports needed. The system should also be able to produce a full audit log of every action that takes place within the system.

Questions to ask a potential provider:

- ✓ What reports are available as a part of your solution?
- ✓ How can we customize the reports to perfectly suit our needs?
- ✓ Do you have dashboards to track internal productivity and statistics for our internal reporting?
- ✓ Does your system maintain an audit trail of all data and actions within your system to easily show to auditors and regulators?

3 Case Management/Review Tool

The solution should include an intuitive and easily navigable case review tool to enhance the accuracy of reviewing hits while facilitating efficient workflows.

Questions to ask a potential provider:

- ✓ How customizable is your case review tool?
- ✓ How customizable are the workflows?
- ✓ Can your system handle escalation notifications through multiple channels including email?
- ✓ Can you segment groups of individual or organizational data within the same system and screen them against different lists or via different processes?
- ✓ In what languages is your case review tool offered?

4 Support

The solution provider should offer ongoing support for the system and respond to questions or requests in a timely manner.

Questions to ask a potential provider:

- What support is provided during implementation and ongoing?
- Do you provide global support and coverage?
- Are your support staff technical experts in your product?
- Do you provide regular enhancements to your product?

5 Additional Capabilities to Look for and Questions to Ask

- Can your solution automatically capture a customer ID, validate it, and simultaneously screen it against any watchlist for an efficient and accurate onboarding process?

- Does your solution support document upload and storage under the client profile for easy access, sharing, and maintaining an audit trail?

- Can your solution provide an automated beneficial ownership due diligence capability that incorporates beneficial owner identification (BOI), verification, and screening against watchlists into a seamless, integrated process?

- Does your solution support real-time payment/transaction screening to automatically screen relevant information, including free text fields, against any watchlists?

- ✓ Does your solution provide AML-specific data quality processing, such as data standardization, deduplication, identification of hidden names in non-name lines, and extended relationships and networks, prior to screening to significantly enhance matching accuracy and reduce false positives?

- ✓ Does your solution enable an enhanced due diligence (EDD) capability from within the solution by integrating with a public records database (e.g., CLEAR)?

- ✓ Do you provide assistance in migrating to new policies and procedures brought about by a new system implementation?

- ✓ Can you help update or develop model configuration documentation to support regulatory requirements and expectations?

Are You Ready?

This guide has armed you with information you will need to successfully find and evaluate a new AML compliance system. Know that there is a solution that can efficiently address your needs and meet the rigorous requirements that have been identified here. A proven provider should be able to successfully guide you through this process.

FinScan is a comprehensive, enterprise AML compliance screening solution used by leading organizations worldwide. Let us show you why.

Contact us for a free consultation & demo of FinScan's features and capabilities:

finscan.com

About FinScan

FinScan, an Innovative Group solution, offers advanced Anti-Money Laundering (AML) and Know Your Customer (KYC) compliance software and consulting solutions trusted by over 300 leading organizations worldwide. Built on decades of experience in data quality and cognitive matching technologies, FinScan provides a data-first approach to ensure unparalleled accuracy in identifying risk, minimizing false positives, and reducing the risk of missing true hits. FinScan's comprehensive offerings include sanctions, PEP, and adverse media screening, UBO due diligence and screening, Swift/transaction screening and monitoring, ID authentication, data enrichment, and advisory services for implementing a holistic compliance program. FinScan offers flexible deployment including SaaS, on-premise, and hybrid options. FinScan's SaaS customers are screening more than 300 billion names a year. Learn more at **www.finscan.com**.

FinScan®

finscan.com

Locations

Pittsburgh | London | Dubai | Frankfurt | Mexico City | São Paulo | Singapore | Sydney | Toronto