



FinScan®

Special Guide for Insurance Companies

Risky Business: Five Key Parts of Your Compliance Program You Should Evaluate Now

Why insurers need to step up their AML compliance

Did you know you have the same sanctions responsibilities as your bank? And if you operate in the US, failing to comply can have serious consequences. But staying vigilant isn't just about avoiding penalties – it's about protecting your business. Legacy systems and incomplete data often plague insurance companies, leaving you vulnerable to money laundering and financial crimes.

Here's why ignoring AML compliance is a gamble you can't afford:



Your bank won't tolerate non-compliance: Your bank adheres to strict sanctions regulations, and so should you. Falling outside their risk appetite could jeopardize your relationship and access to essential financial services.



Data gaps are a vulnerability: Many insurers underestimate the importance of complete and accurate customer data. Not knowing your customers and their business networks creates major exposure points for money laundering activities.



Financial crimes aren't distant threats: Insurance premiums and cancellations offer easy access for laundering illicit funds. Without proper AML solutions, such activities can go undetected for weeks or months, causing significant financial losses.



Trade finance harbors hidden risks: The complex world of trade finance presents a breeding ground for fraud and sanctions violations. A robust AML strategy is crucial to mitigate these risks and protect your business interests.

Understanding your current state

The first step to successfully selecting and adopting a new solution, platform, tool-set, 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.

Here are the five key areas to examine to fully understand the relationship between your current state and your desired improvements and outcomes.

Questions to ask yourself:

01

Data Quality

Bad data hurts compliance beyond IT: it wastes resources reviewing false matches and masks risks with inaccurate information. While IT can help, their focus may not align with compliance needs. To truly combat these risks, collaborate with your vendor or IT team to target data quality issues specific to your business, such as inconsistent formats, missing elements, and duplicate entries. This tailored approach can significantly improve efficiency and risk detection.

Questions to ask yourself:



Are you 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 you screening for risk?



How does each of these source systems rank on various dimensions of data quality such as accuracy, completeness, consistency, and uniqueness?



Do you know exactly what data errors are feeding false positives such as noise words, titles, and dummy data?



How can you stop these errors from getting into the screening system?



How many duplicate customers do you have?



Do you screen and remediate the same alert multiple times?



How can you apply remediation decisions to the same customer when they appear in multiple alerts – and improve productivity?



What productivity gains can you achieve with such a feature?

02

False Positives

Frustrated by false positives drowning your AML compliance team? Most companies switch systems due to bad data leading to inaccurate results. While minimizing them completely is unrealistic, advanced technology can make a drastic difference. Track your current false positives to showcase improvement and justify a new solution's ROI.

Questions to ask yourself:



How many hits are you receiving each day?



What level of hit rate would you consider optimal?



What's your typical level (ratio) of false positives on a daily, weekly, or monthly basis?



What's the desired ratio you'd like to achieve (recognizing that there will always be some false positives)?



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 you have the tools or resources to improve data quickly and effectively?



Do you know exactly why you are getting certain types of alerts?



03

Manual Processes

If you're drowning in manual tasks, then it's time to ditch the bottlenecks. Analyze your team's daily grind – are inefficient systems slowing them down? Identify manual processes, track time spent, and uncover hidden roadblocks. Streamline workflows and free up your team to tackle real risks effectively.

Questions to ask yourself:



Which of your current processes are inefficient?



What are your 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 much time are you spending clearing all the hits?



Is your team able to multitask on different processes, enabling staff to review and report hits more rapidly?



Which steps are creating bottlenecks in your process?



Which steps do you wish were automated?



04 Risk & Coverage

Don't just meet compliance, exceed it. Screen beyond basic legal requirements with comprehensive third-party lists. Get wider coverage of politically exposed persons (PEPs), news, and more to stay compliant and avoid reputational risks.

Questions to ask yourself:

For the compliance lists you use today:



Do they adequately address what you 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 your vendor?



Are there any additional internal lists or block lists that need to be automatically populated into your system?



If yes, then how are they maintained and uploaded to the system?



Are you able to easily see and review all necessary information on the compliance profiles to clear your alerts?



Can different divisions in your organization screen against different sets of lists based on their needs?



05

Reporting

AML compliance goes beyond initial screening. Auditors and regulators demand proof of efficiency and effectiveness. Trustworthy reports are key – accurate, complete, and easily customized to showcase your robust compliance efforts. Empower your team for success with timely and effective reporting.

Questions to ask yourself:



Is your system able to generate reports?



If so, are you building and formatting your reports manually?



What types of reports do you need that you cannot get today?



Are you 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 you export the reports in various formats?



Can you save frequently-used reports to save time and improve consistency?







Can you export data to Business Intelligence (BI) systems for detailed analysis?

Safeguarding your future

By examining your current state across these five key areas – data quality, false positives, manual processes, risk & coverage, and reporting – you've gained invaluable insights into the strengths and weaknesses of your AML compliance program.

This self-assessment serves as a critical first step toward building a more efficient, effective, and risk-mitigating program.

The good news is, you don't have to navigate this journey alone. By leveraging advanced technology, partnering with industry experts, and implementing tailored solutions, you can:

-  Eliminate the noise of false positives, freeing your team to focus on real risks.
-  Streamline manual processes, boosting productivity and efficiency.
-  Expand your risk coverage with comprehensive data sources, ensuring maximum protection.
-  Generate robust, accurate, and easily accessible reports, demonstrating compliance and exceeding expectations.

Don't wait until it's too late – taking a proactive approach to AML compliance is vital to securing your business and upholding its integrity. It's not just about avoiding penalties, it's about safeguarding your business reputation, protecting financial assets, and fostering trust with your stakeholders.

Take action today to elevate your AML compliance program, and empower your team to tackle emerging threats with confidence.

FinScan[®]

Locations

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

finscan.com