KYC3

Know Your Customer, Counterparty & Competition
Big Data Technology for Risk Management

White Paper

Setting Up a Robust and Automated Compliance Program

Setting Up a Robust and Automated Compliance Program

Asset managers have a significant opportunity to enhance their investor experience, avoid costly compliance fines, and increase their bottom line by 5-10%. However, many struggle to achieve these goals due to a lack of emphasis on a holistic approach to compliance within their organizations. Teams are often overwhelmed with complex onboarding processes, extensive customer due diligence, intricate risk assessments, and labor-intensive audits that require extensive manual checks and double-checking.

The reliance on manual processes, lack of integration, document overload, and the use of disparate evaluation tools, along with heavy reliance on emails, manual checklists, and spot reviews, further exacerbate the challenges faced by asset managers in achieving effective compliance.

Implementing an effective anti-money laundering (AML) program is crucial for asset managers, as it not only prevents them from incurring fines but also safeguards the reputation of their company from being tarnished. A robust AML compliance program encompasses five major functions, each with numerous activities that are essential for ensuring regulatory adherence and mitigating financial crime risks.

By addressing these challenges and implementing a comprehensive AML compliance program, asset managers can streamline their operations, enhance the investor experience, and ultimately improve their financial performance. This proactive approach to compliance not only protects the organization from potential penalties but also fosters a culture of trust and integrity, which is essential for long-term success in the asset management industry.

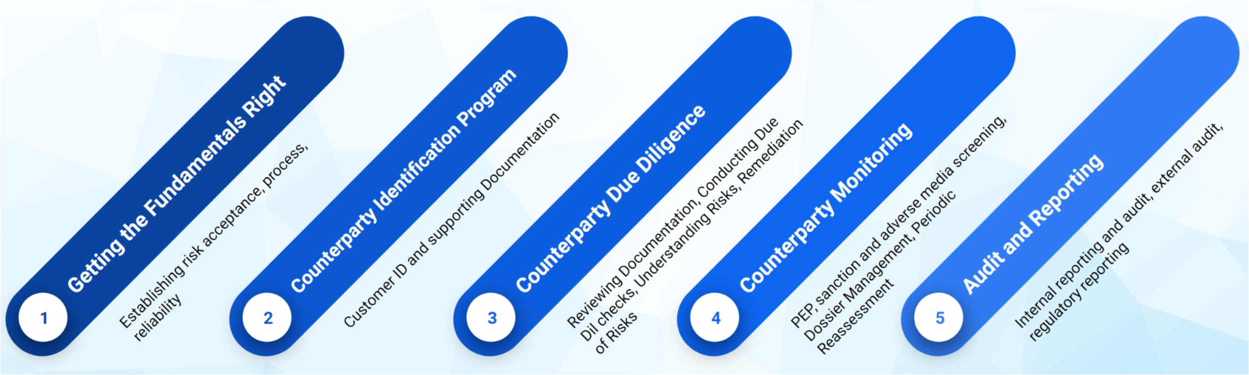

1
Getting the Fundamentals Right
Establishing risk acceptance, process, reliability
2
Counterparty Identification Program
Customer ID and supporting Documentation
3
Counterparty Due Diligence
Reviewing Documentation, Conducting Due Dil checks, Understanding Risks, Remediation of Risks
4
Counterparty Monitoring
PEP, sanction and adverse media screening, Dossier Management, Periodic Reassessment
5
Audit and Reporting
Internal reporting and audit, external audit, regulatory reporting

Figure 1: The 5 pillars of a successful counterparty compliance program.

Pillar 1: Getting The Fundamentals Right

In order to get the fundamentals right, you will have to elaborate your policies, procedures and controls.

This part involves developing and implementing policies, procedures, and controls to mitigate and manage the identified risks. This includes policies on customer due diligence, ongoing monitoring, and reporting of suspicious activities.

The procedures should include a training and awareness workstream. Providing training to employees to ensure they understand their AML responsibilities and are aware of the latest AML regulations and best practices.

Your policies need to include independent testing and audit of your program. Conducting regular independent testing and audit of the AML program to ensure its effectiveness and compliance with regulations.

And last, but not least, you will have to appoint a Designated AML Compliance Officer (CO) and Money Laundering Reporting Officer (MLRO). Appointing a designated AML compliance officer who is responsible for overseeing the AML program and ensuring its effectiveness.

By effectively implementing these policies, asset managers can position their organization for success, improve their investor experience, avoid compliance fines, and boost their bottom line.

Once the framework and roles and responsibilities are clear, it will be time to decide, at board level and with formal records, what risks your organization is ready to accept and manage. Based on this Risk Appetite Statement (RAS), your program of compliance risk management policies and procedures can be implemented. This means you must decide which counterparties are potentially acceptable for you to engage within the scope of products and transactions in your business. To state the obvious, this isn’t about defining any illegal activity - those are already outside your risk tolerance by definition.

The Risk Acceptance Statement defines the level of risk in legal activity that you are able to manage, knowing that when things go wrong, it is usually an apparently legal activity of a counterparty that is actually carrying higher risk than anticipated. It could be covering something more sinister and illegal or simply be the result of negligence or incompetence.

Often, limited Risk Management capability constrains the Risk Acceptance scope, the resulting policy and procedures, and creates a poor customer experience. With a digital process, the scope can be reviewed, the ability to handle clients effectively can be augmented and the overall customer experience can be improved, resulting in a much more effective business for you.

Step 1: Your Risk Acceptance Statement (RAS)

The Old Way	**The New Way**
Review business capabilities and expected market, estimate risks and define a RAS	Define your RAS based on empirical review of clients using automated capabilities and real-time reporting
The Old Result	**The New Result**
A RAS based on assumptions about the organization, the market and risks that may not match operational realities	A RAS based on measurable parameters from your clients, products and markets.
Using an automated and fully digital risk assessment system, you can validate the accuracy of and your adherence to your RAS.	

Every risk management program starts with a Risk Acceptance Statement (RAS). This should be up to date, in line with your risk management capabilities and board approved. The traditional method for determining your risk tolerance is to assess your business assumptions and review your manual process capacity in order to develop a Risk Acceptance Statement based on these assumptions. This results in a risk policy that is limited by the assumptions about your business.

The new way of reviewing your risk tolerance is to get a real-time look-through at your risk profile and a better understanding of your actual accepted risk versus your risk management capabilities. With a fully digital system, you can compare your actual risk to your Risk Acceptance Statement at any time instantly. This results in faster, clearer and more accurate risk acceptance and risk mitigation.

Step 2: Defining Your Compliance Process

The Old Way	**The New Way**
Develop procedures and checklists that enable the RAS to be implemented in your organization	Configure your compliance process based on the limits of a dynamic and integrated digital system
The Old Result	**The New Result**
An operating manual detailing a system of elaborate procedures and checklists, usually managed with tools such as Excel, Word and Email	Digitalization delivers a standardized compliance process that is leaner and more agile.
Using an automated and fully digital risk assessment system, you can do more with less and you can adapt to regulatory changes quickly and inexpensively.	

Once the RAS is approved, the procedures for managing risk are established or adapted to the RAS. The old way of doing this is to develop detailed procedures with forms and checklists to be followed. This results in an elaborate and complicated process with manual steps and decision points.

The new way of managing this process is with workflow management techniques. This results in a leaner compliance process with fewer steps. Using a fully digital, dynamic and integrated system you can do more with less and can adapt your risk management processes to new regulatory and business requirements quickly and inexpensively.

Step 3: Ensuring your Risk Assessment Process is reliable

The Old Way	**The New Way**
Review the risk assessments to ensure that they are consistent and that risks are properly accounted for	Configure the risk assessment engine directly in the system and begin using it. Dynamically adjust the parameters so that the risk results filter into the correct risk level automatically.
The Old Result	**The New Result**
Manual review of test or real cases in order to determine if the risk assessment process is correctly categorizing risks	Once tuned, there is no need to review the risk assessment process as a standardized digital process delivers provably consistent results.
Using an automated and fully digital risk assessment system, you get a standardized, automated and fully auditable risk assessment process.	

After establishing your processes, they need to be reviewed in order to ensure that the checks and balances are working as intended. The old way of doing this is to conduct manual reviews of “spot check” cases in order to determine if the risk assessment process is correctly categorizing and assessing risks.

The new way of doing this is with automated risk assessment techniques, involving the use of linked algorithmic risk calculations. Digitalization of the risk assessment process delivers a standard, automated and fully audible risk assessment process with no need to conduct further spot checks.

Pillar 2: Identifying and Assessing your Customers and Counterparties

You need to identify who your counterparty is. In short, you need to know if the investor with a large ticket for your fund is a political slush fund that may be the proceeds of corruption or if it's a family fortune gained from the sale of a business. The individual you deal with may be identified. However, you need to know if they represent themselves or they represent something else, such as another individual or an organization. If they represent an organization, you need to know who owns and who controls that organization all the way to the Ultimate Beneficial Owner.

This is much harder than it sounds as the UBO may not even be a shareholder. High net worth individuals and private equity structures sometimes use "nominee" shareholders and directors to represent them in official records. This often isn't done for nefarious reasons, it is rather to maintain a high level of discretion and keep a lower profile as part of a sensible personal risk management strategy that many high net worth individuals require. A Counterparty Identification Program involves deciding what kinds of questions and documentation you will request from your counterparts based on your assessment of the apparent risk they represent.

In a traditional setting, identifying your counterparty involves meeting the people face-to-face, having them present government documents for identification and to demonstrate their role and partners in any legal entity that they represent. This is the traditional "account opening".

In a digital world, this becomes a new process. You need to identify the individual sitting behind the internet connected device, to collect relevant information from them and to ensure that the information is true and valid to the best of your ability. You can do this by using video conferencing tools, collecting documents electronically and having clients send additional information in with legally binding signatures.

Step 1: Customer identification

The Old Way	**The New Way**
Speak to customers and ask have them provide identity documents	Let customers complete a digital identification process on a secure portal
The Old Result	**The New Result**
Compliance office receives documents and certifies the ID of the customer	Customers can onboard any-time, any-day and faster
Using a digital customer identity portal improves both the quantity and quality of your customers experience while reducing fraud and data protection risks for you.	

In the past, the process of identifying customers involved speaking to them directly and asking them to provide identity documents. This method was time-consuming and required customers to physically present their documents.

However, with the introduction of a new way, customers can now complete a digital identification process on a secure portal. This new method allows customers to onboard at their convenience, anytime and any day, resulting in a faster and more efficient process.

Instead of relying on a compliance office to receive and certify the customer's ID documents, the digital customer identity portal streamlines the process, improving both the quantity and quality of the customer's experience. Additionally, this new method reduces the risks of fraud and data protection, providing a more secure environment for both the customers and the company.

Step 2: Gathering additional documentation

The Old Way	**The New Way**
Customers are asked to send in documents by email and/or by postal service	Allow customers to digitally upload documents via a secure customer portal
The Old Result	**The New Result**
Compliance officer receives documents in various channels, bit by bit and must manually check, organize and review them	Faster onboarding, document requirements are clear, customers are happy = more business
Using a digital customer identity portal, customers upload all documents using a clear and automated “ToDo” list and you all get deals done faster and more securely.	

In the old way of gathering additional documentation, customers were required to send in their documents either by email or through the postal service. This process was time-consuming and inefficient. Compliance officers would receive these documents through various channels, bit by bit, and had to manually check, organize, and review them. This resulted in a slow onboarding process and increased the risk of errors or missing information.

However, with the new way of gathering additional documentation, customers are now able to digitally upload their documents via a secure customer portal. This streamlined process allows for faster onboarding as document requirements are clearly communicated to customers. The use of a digital customer identity portal also provides an automated "ToDo" list, making it easier for customers to upload all necessary documents. This not only speeds up the process but also ensures that all required information is provided, reducing the risk of errors. As a result, customers are happier with the improved efficiency and security, leading to increased business opportunities.

Pillar 3: Conducting Customer Due Diligence

You need to verify that what your counterparty has claimed is valid and represents a true and accurate depiction of what and who you're dealing with. This means that you must review the documentation provided in order to assess its relevance and authenticity. You must cross check to a reasonable level of effort that the claims of your counterparty make sense. This can involve doing Google searches, using specialized databases and resources, conducting meetings with involved and related individuals or even sending private investigators to collect first hand information. Your due diligence should result in you knowing the risk level of your counterparts and treating them accordingly.

Conducting due diligence involves the verification of the information provided by your prospective client as well as cross checking the client identity against government lists and available public media in order to conduct a money laundering risk assessment of your customer. Traditionally, this involves scrutinizing the documents provided by the client, analyzing the client’s statements and using public sources, such as trade registries and press archives, to verify the client’s background and claims. This also involves checking to be sure that the prospective client isn’t a wanted criminal or terrorist by referring to a multitude of lists issued by national and supra-national law enforcement organizations.

In a digital world, this becomes a much more complex task, as there are a large number of data sources and data changes very quickly. You can use search engines and public access government databases to do much of this checking. With these sources, you gather information, analyze it in context, and compile reports summarizing the identified risks and their likelihood of posing a threat to your business from compliance, AML and reputational perspectives.

Additionally, you can utilize specialized software and tools that are designed to monitor and analyze data for potential risks. These tools can help automate the process of gathering and analyzing data, making it more efficient and accurate.

When conducting risk assessments in a digital world, it is important to consider various factors such as the type of data being analyzed, the sources of the data, and the specific risks that are relevant to your business. For example, if your business deals with financial transactions, you may need to focus on compliance and anti-money laundering (AML) risks.

To gather information, you can use search engines to find relevant news articles, social media posts, and other online sources that may contain information about potential risks. Public access government databases can provide information on regulatory requirements and compliance issues.

Once you have gathered the information, it is important to analyze it in context. This means considering the relevance and reliability of the sources, as well as the potential impact of the identified risks on your business. For example, a negative news article about a competitor may not pose a direct threat to your business, but it could impact your reputation.

After analyzing the data, you can compile reports summarizing the identified risks and their likelihood of posing a threat to your business. These reports can help you prioritize and address the most significant risks. It is important to regularly update and review these reports, as the digital landscape is constantly evolving and new risks may emerge.

Overall, conducting risk assessments in a digital world requires a combination of technology, data analysis, and critical thinking. By utilizing the right tools and approaches, you can effectively identify and manage potential risks to your business from compliance, AML, and reputational perspectives.

Step 1: Reviewing Customer Documentation

The Old Way	**The New Way**
Documents are dumped into a folder and reviewed against the checklist	Organize documents in a "smart" system that knows the dossier requirements and can be quickly reviewed using a fast and efficient "Tinder for compliance" approach.
The Old Result	**The New Result**
Checklist is completed manually and deficiencies are noted in time consuming process	Faster onboarding, document requirements are clear, customers are happy and you can handle more business
Using an integrated digital compliance platform makes review fast and easy and gives immediate visibility on remediation requirements, making the whole process 10x faster.	

In the old way of reviewing customer documentation, documents would be dumped into a folder and then reviewed against a checklist. This process was time-consuming and inefficient. The old result of this manual checklist completion was a slow process with deficiencies noted in a time-consuming manner.

However, with the new way, documents are organized in a "smart" system that understands the dossier requirements. This allows for a quick and efficient review using a "Tinder for compliance" approach. The new result is a faster onboarding process with clear document requirements. This leads to happier customers and the ability to handle more business. By utilizing an integrated digital compliance platform, the review process becomes fast and easy.

Additionally, it provides immediate visibility on any remediation requirements, ultimately making the entire process 10 times faster.

Step 2: Conducting Due Diligence Checks

The Old Way	**The New Way**
Customer data is entered into a due diligence system and results are checked by the compliance analyst.	Screen customers against PEP, sanctions, adverse media and search engines *as soon as a customer data is captured* and immediately add results to the dossier.
The Old Result	**The New Result**
Results are "copy/pasted" or downloaded and integrated into a customer risk report document that is added to the dossier. Manual work is error prone and lacks full audit trials	Real-time customer due dil available quickly and easily without switching systems and with a full audit trail of risk assessment and analyst review
Using an integrated digital compliance platform makes the due diligence process error-free and 10x faster.	

In the past, conducting due diligence checks on customer data was a time-consuming and manual process. Compliance analysts would enter the customer data into a due diligence system and then manually check the results. This process was prone to errors and lacked a comprehensive audit trail. The results would then be copied and pasted or downloaded and integrated into a customer risk report document, which would be added to the dossier.

However, with the new way of conducting due diligence checks, the process has become much more efficient. As soon as customer data is captured, it is screened against various sources such as politically exposed persons (PEP), sanctions lists, adverse media, and search engines. The results are immediately added to the dossier, providing real-time customer due diligence. This eliminates the need to switch between systems and ensures that the risk assessment and analyst review have a full audit trail.

The use of an integrated digital compliance platform has revolutionized the due diligence process. It has made the process error-free and 10 times faster.

Step 3: Understanding the Risks of the Customer Structure and Activity

The Old Way	**The New Way**
Customer provided structure charts and business descriptions are reviewed, if questions arise, clarification is requested	Assess risks using all the inputs from the customer, such as roles and organizational relations. Quickly review dynamic and automatic structure charts and business risk flags.
The Old Result	**The New Result**
Charts of various formats and data quality are included in customer files for reference, along with Q&A notes	Standardized structure charts are generated automatically. They are dynamic and easy to manage. Structures are reflected "as is" in real time based on available information and can be merged and split with a single click. Risks are calculated and updated “on-the-fly” based on the latest information.
Using an integrated digital compliance platform with entity-relationship data makes structure changes and risks automatically visible and up-to-date in real-time.	

In the old way of understanding the risks of the customer structure and activity, customer provided structure charts and business descriptions were reviewed, and if any questions arose, clarification was requested. The result was that charts of various formats and data quality were included in customer files for reference, along with Q&A notes.

However, in the new way, risks are assessed using all the inputs from the customer, such as roles and organizational relations. This is done by quickly reviewing dynamic and automatic structure charts and business risk flags. The new result is that standardized structure charts are generated automatically, making them dynamic and easy to manage. These structures are reflected "as is" in real time based on available information and can be merged and split with a single click. Risks are calculated and updated "on-the-fly" based on the latest information.

By using an integrated digital compliance platform with entity-relationship data, structure changes and risks are automatically visible and up-to-date in real-time. This new approach streamlines the process, improves accuracy, and ensures that all relevant information is easily accessible.

Step 4: Remediation of Identified Risks

The Old Way	The New Way
Based on the evaluation of customer inputs and risk assessments, additional information may be required from the customer by email or telephone	During automated risk assessments and structure review, compliance can send an invitation to the customer to upload additional information directly
The Old Result	**The New Result**
Compliance sends an email to customer and awaits the response	Customers can provide additional documents any time of day quickly and analysts can confirm them immediately
Using an integrated digital customer portal reduces the time to close information gaps by an order of magnitude and better secures the exchange of sensitive information.	

In Step 4 of the process, which focuses on the remediation of identified risks, there has been a significant improvement from the old way to the new way. Previously, when additional information was required from the customer based on customer inputs and risk assessments, compliance would have to send an email or make a phone call to request the information. This process was time-consuming and relied on the customer's prompt response.

However, with the new approach, automated risk assessments and structure reviews allow compliance to send an invitation to the customer to directly upload the required information. This not only saves time but also allows customers to provide the documents at any time of the day, ensuring a quicker response. Furthermore, analysts can immediately confirm the received documents, streamlining the process even further.

The implementation of an integrated digital customer portal has not only reduced the time to close information gaps by a significant amount but also enhanced the security of sensitive information exchange. Overall, this new method has greatly improved efficiency and effectiveness in the remediation of identified risks.

Pillar 4: Monitoring Your Customers and Counterparties

You need to continually monitor your counterparty risk levels and take appropriate action if the risk level of a counterparty changes. This means you need to screen your counterparts against official lists of wanted and known criminals and terrorists, such as the OFAC, Interpol, UN, EU, FBI and other published lists. This also means you need to know if your counterparty is or becomes politically exposed - meaning they are in a position of political power that may be conducive to corruption. Finally, you need to make sure your counterparties are not engaging in behavior that could be damaging to your reputation as their service provider. The media is full of regretful financiers making excuses that they were unaware that Jeffrey Epstein was a sadistic pedophile yet this information was in the public media for nearly a decade before the scandal became front-page news.

There are many sanctions lists published by various governmental and international bodies around the world. While not all are legally applied in any specific jurisdiction, it is very important to be aware of them all. Even if an entity is not sanctioned on lists legislated for your jurisdiction, finding the entity sanctioned on an extra-jurisdictional list that does not necessarily apply to your organization is still a very strong sign of potential wrongdoing or risk. Such hits must absolutely be investigated and taken into consideration. Occasionally, entities are listed on national sanctions lists for political purposes, in these rare cases, one may decide to engage with the entity despite this negative information. In any case, you should ensure that there is a detailed audit trail of the decision making process for such decisions.

Monitoring of client risk involves keeping tabs on your clients, as one would do with a traditional press clipping service. This means scanning the press each day for negative information about your clients. Also, this means scanning all official lists of wanted criminals and terrorists to ensure that your client is not added to one of these lists.

Because of the volume of information and the multitude of sources, it is no longer feasible to connect directly with each official source and with search engines to review each client each day. In a digital world, you will need a client screening solution. In general, you will have to purchase access to a consolidated data source that makes all of this information available in a single search. Still, with such a data source, there are several ways to screen your clients.

First, you can purchase access to a web tool in which you will screen each of your clients manually each day, possibly by uploading them in batches once per day and checking them against the data. This approach keeps all of your customer data private to your company at the expense of a daily intervention that involves collection and review of the same results each day, so that you can check for new data points.

Second, you can share your client data with a third party who will screen your clients each day and send you notification of any new negative information arising about your clients. This approach reduces your workload at the expense of sharing all of your customer data with a third party who becomes a legal custodian of that data.

The third option, and one that combines the benefits of both keeping your client data private and fully automating your workload, involves running the screening in your systems so that your client data stays with you and your nightly screening records are also kept with you so that old results are remembered and new results can be handled with a minimum of work.

Step 1: Customer PEP, Sanctions and Adverse Media Screening

The Old Way	**The New Way**
The compliance team will upload a list of customers to a screening service in order to check them, or the compliance team will give the customer list to a third party for nightly screening	Operate everything automatically and in-house. Get risk alerts and review them directly in the system. A secure system downloads risk data from the data providers and screens the customers every night in-house.
The Old Result	**The New Result**
Customer data is handled every day by third parties and potential hits are provided to and assessed by the compliance analysts	Customer data stays in your company, results and assessments are collected and reviewed in a couple clicks with a full audit trail.
Using an integrated digital compliance platform, it's possible to keep your customer data private, screen them every day, and easily handle the results 10x faster than before.	

In the old way of conducting customer PEP, sanctions, and adverse media screening, the compliance team would upload a list of customers to a screening service or give the list to a third party for nightly screening. This process involved relying on external parties to handle customer data and assess potential hits.

However, with the new way, everything is operated automatically and in-house. A secure system downloads risk data from data providers and screens the customers every night within the company. This not only ensures the privacy of customer data but also allows for risk alerts to be received and reviewed directly in the system. The results and assessments are collected and reviewed with just a couple of clicks, providing a full audit trail.

This integrated digital compliance platform has revolutionized the screening process, making it 10 times faster than before. Now, customer data stays within the company, eliminating the need for third-party involvement and streamlining the entire process.

Step 2: Customer Dossier Management

The Old Way	**The New Way**
Periodically, the compliance analyst will review the dossiers and ensure that all required documents are included	The analyst is notified whenever a dossier is deficient and can trigger a remediation request via a secure portal. An automated system knows all required documents and tracks their expirations.
The Old Result	**The New Result**
Regular periodic spot checks reveal missing or expired documents. Customers are asked to remediate the situation via email, phone or letter	Customers receive immediate notification of missing or expired documents and the analyst can review them on the spot when they are uploaded
Digitalization makes remediation a continual and automatic process. Dossier status is visible at all times and spot checks aren't required, saving many man-days of work per year.	

In the past, customer dossier management was a time-consuming and manual process. Compliance analysts would periodically review the dossiers and manually check if all the required documents were included. If any documents were missing or expired, the analyst would have to contact the customer via email, phone, or letter and request remediation. This process was not only inefficient but also prone to errors and delays.

However, with the implementation of the new system, customer dossier management has been revolutionized. Now, an automated system tracks all the required documents and their expirations. Whenever a dossier is deficient, the analyst is immediately notified through a secure portal. This allows for immediate action to be taken, as the analyst can review the missing or expired documents as soon as they are uploaded.

The benefits of this new system are numerous. Firstly, customers receive immediate notification of any missing or expired documents, ensuring that they are aware of the situation and can take prompt action. Secondly, the digitalization of the process makes remediation a continual and automatic process. There is no longer a need for regular spot checks, saving a significant amount of time and manpower. Additionally, the dossier status is visible at all times, providing transparency and ease of access for both the analyst and the customer.

Overall, the implementation of the new customer dossier management system has greatly improved efficiency, accuracy, and customer satisfaction. The streamlined process and automated tracking have eliminated the need for manual checks and remediation requests, saving valuable time and resources. This positive change ensures that all required documents are always up to date, reducing compliance risks and enhancing the overall customer experience.

Step 3: Periodic Refresh and Reassessment

The Old Way	**The New Way**
Based on their risk level, customer dossiers must be reviewed periodically.	Receive automatic notification on any specific dossier review date and quickly check the file for any changes of risk status.
The Old Result	**The New Result**
On an annual, biannual or tri-annual basis, dossiers are assessed to ensure that the assessed risk level has not changed	Digital dossiers become "smart dossiers”. No dossier will be forgotten and the remediation workload is evenly distributed over the year.
Using an integrated digital compliance platform with digital dossiers, makes reassessment into a holistic step in a continual process, saves time and improves reliability.	

Step 3 of the process involves periodic refresh and reassessment, which is a crucial step in ensuring the accuracy and reliability of customer dossiers. In the old way, dossiers were reviewed periodically based on their risk level. However, this process was time-consuming and there was a risk of forgetting to reassess certain dossiers.

But now, with the new way, things have become much more efficient and streamlined. Thanks to an integrated digital compliance platform, automatic notifications are received on specific dossier review dates. This allows for a quick and easy check of the file to identify any changes in risk status.

The old result of reassessment was done on an annual, biannual, or tri-annual basis to ensure that the assessed risk level had not changed. However, this approach had its limitations and was not as reliable as desired.

With the new result, digital dossiers have transformed into "smart dossiers". This means that no dossier will be forgotten and the workload for remediation is evenly distributed throughout the year. The integration of digital dossiers into the reassessment process has made it a holistic step in a continual process. This not only saves time but also improves the reliability of the reassessment process.

Overall, the implementation of an integrated digital compliance platform has revolutionized the way reassessment is conducted. It has made the process more efficient, reliable, and user-friendly. By ensuring that dossiers are regularly refreshed and reassessed, businesses can maintain an accurate and up-to-date understanding of their customers' risk levels.

Pillar 5: Audits and Reporting

You need to be prepared to confirm the efficacy of your risk management program to your board, to your auditors and to your regulator. To do this, you need to track and assess your performance across all elements of your program. You need a reliable audit trail and easy to produce reports. Ideally you can produce up to the minute reviews quickly and efficiently on any counterparty, product or transaction in your business. Not only will your board, auditors and regulator appreciate these reports, you will sleep better at night knowing that your system is well monitored and everything can be proven to be in order.

Typically your reporting program will involve reporting for several different purposes, including board reporting, internal audit reporting, external audit reporting, and regulatory reporting.

These reports are usually developed as templates ahead of time that are regularly completed and provided to the relevant authority. Board reporting may be bi-monthly, monthly or quarterly, internal audit may be monthly or quarterly, external and regulatory reporting may be quarterly or annual. When all combined, these responsibilities create a very busy reporting calendar. Each report needs to be prepared by its deadline and delivered to the appropriate authority. The preparation of reports involves checking the dossiers, looking at audit notes, reviewing the KPIs and usage of tools and databases that are used to assist in the risk assessment, as well as review of the processes and procedures in place. This is a time consuming task that involves the collection and collation of information from many sources in order to produce clear and concise reports that accurately reflect the risk and compliance events in the reporting period.

Step 1: Checking Dossiers for Internal Compliance

The Old Way	The New Way
Occasionally a specific dossier will require a full review due to a trigger event, such as a specific transaction or activity change	Set up “smart dossiers” so that risk assessment is continual and always up to date. Consultation dossiers whenever a trigger event occurs.
The Old Result	**The New Result**
The dossier is reviewed in detail. Documents, the assessments and the other considerations are checked to confirm a potential change in risk level	Client risk levels can be quickly reviewed and confirmed whenever a trigger event occurs. Digitization even means that trigger events may even be signaled using automated API calls
Using an integrated digital compliance platform with “smart dossiers” lets you fulfill client requests 10x faster while maintaining proper risk and compliance controls.	

In the old way of checking dossiers for internal compliance, a specific dossier would only be reviewed if there was a trigger event, such as a specific transaction or activity change. This process was time-consuming and required a detailed review of the dossier, including documents, assessments, and other considerations, to confirm any potential change in risk level.

However, the new way of handling dossiers is much more efficient and up to date. "Smart dossiers" have been implemented, allowing for continual risk assessment and ensuring that risk levels are always current. Whenever a trigger event occurs, consultation dossiers are consulted, allowing for quick review and confirmation of client risk levels.

Additionally, digitization has further improved the process by enabling automated API calls to signal trigger events. By utilizing an integrated digital compliance platform with "smart dossiers," client requests can now be fulfilled 10 times faster while still maintaining proper risk and compliance controls. This new approach to checking dossiers for internal compliance is a significant improvement, streamlining the process and increasing efficiency.

Step 2: Reporting to the Board

The Old Way	**The New Way**
The BoD requires risk updates and needs concise information to approve any exceptional cases. Compliance must prepare these reports using data from their various systems and processes.	Keep all data in an integrated system with full audit trails and detailed statistics. Reports are available in real time all the time
The Old Result	**The New Result**
Periodically, the compliance team will review and update their overview statistics and then generate reports and detailed and time consuming reports to be included in the "board pack".	Reports can be generated in minutes rather than hours with standardized formats and consistent data directly from the system. Data is also accessible by API to automatically feed complex business intelligence and decision support systems
Using an integrated digital compliance platform, 360 degree view reports are standardized and available all the time, saving man-days of work per year and providing professional assurance of consistent and unbiased reporting.	

In the old way of reporting to the Board, the compliance team had to gather data from various systems and processes to prepare reports for the Board's risk updates. This process was time-consuming and required a lot of effort to ensure the reports were concise and accurate.

However, with the new way of reporting, all the data is kept in an integrated system with full audit trails and detailed statistics. This allows for real-time access to reports, making the process much more efficient. Instead of periodically reviewing and updating overview statistics, the compliance team can now generate reports in minutes with standardized formats and consistent data directly from the system. This not only saves time but also provides a more professional assurance of consistent and unbiased reporting.

Additionally, the data is accessible through an API, allowing for automatic feeding into complex business intelligence and decision support systems. Overall, the implementation of an integrated digital compliance platform has revolutionized the reporting process, saving man-days of work per year and providing a reliable and efficient way to report to the Board.

Step 3: Conducting the External Audits

The Old Way	**The New Way**
Each year the auditors will want to review the process, procedures and results of the risk management program.	Auditors review the configuration rules and results in place directly on the system along with the audit log showing exactly how the system was used.
The Old Result	**The New Result**
Auditors review the printed documents and procedures and confirm that the risk management program is performing as expected. They note any deficiencies that may exist due to regulatory or best-practice changes since the last audit, which results in changes and updates to the procedures.	Auditors can make quick empirical observations of the entire process and result in a single system. The analysts can address deficiencies on the spot and get auditor sign-off for the configuration changes very quickly.
Using an integrated digital compliance platform means audits and their remediation become much faster, cheaper and 10x more efficient.	

Step 3 of the process involves conducting external audits, and there is a clear distinction between the old way and the new way of conducting these audits. In the past, auditors would review the risk management program by examining printed documents and procedures. They would then confirm whether the program was performing as expected and identify any deficiencies that may have arisen due to regulatory or best-practice changes. This would result in changes and updates to the procedures.

However, with the new approach, auditors can review the configuration rules and results directly on the system. They can also analyze the audit log, which provides a detailed account of how the system was used. This allows auditors to make quick empirical observations of the entire process and address any deficiencies on the spot. As a result, the auditors can provide sign-off for configuration changes much more quickly. The use of an integrated digital compliance platform has revolutionized the audit process, making it faster, cheaper, and 10 times more efficient.

Step 4: Reporting to the Regulator

The Old Way	**The New Way**

Periodically, regulatory authorities will want to review the process, procedures and results of the risk management program	Analysts can produce detailed records, including documents, assessments and audit notes for the regulator in standard formats with the push of a button.
The Old Result	**The New Result**
Regulators review the printed documents and procedures and confirm that the risk management program is performing as expected, as evidenced in the resulting files	Regulators can verify that the risk management program is effective and working without having doubt as to manual process steps and undocumented decisions.
Using an integrated digital platform the compliance process becomes holistic, transparent and simplified so that fines for deficiencies or errors should never happen.	

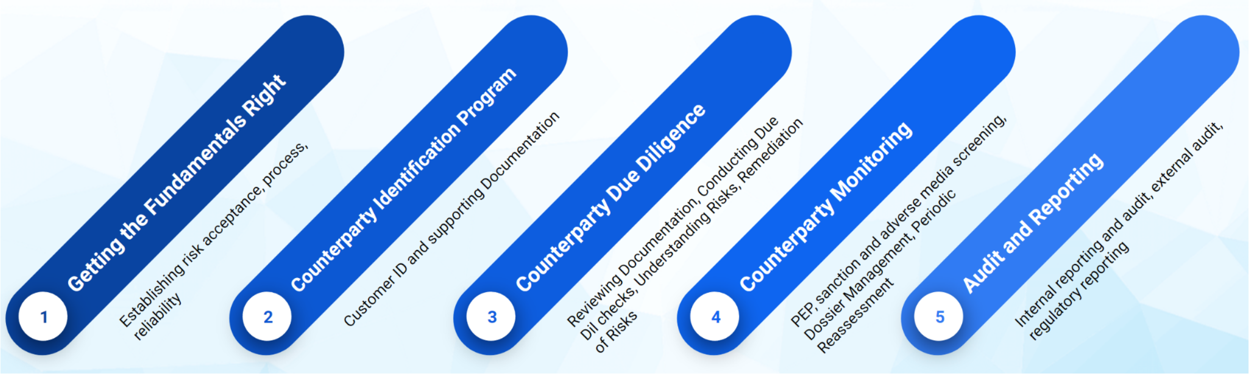
Step 4 of the risk reporting process involves reporting to the regulator, and there is a clear distinction between the old way and the new way of doing this. In the past, regulatory authorities would periodically review the risk management program by examining printed documents and procedures. This process was time-consuming and left room for doubt regarding manual process steps and undocumented decisions.

However, with the new approach, analysts can easily produce detailed records in standard formats with just the push of a button. This integrated digital platform has revolutionized the reporting process, making it holistic, transparent, and simplified. Regulators can now verify the effectiveness of the risk management program without any doubt, as all the necessary information is readily available.

This new way of reporting ensures that fines for deficiencies or errors should never occur, as the risk management program is performing as expected and all decisions are well-documented.

The Big Picture

In summary, you need to get the five pillars of your AML program right in order to succeed. Once these steps are clear, automation becomes the obvious way to manage costs and unlock scale, bringing with it the benefits of a transparent process and a fool-proof audit trail.


1
Getting the Fundamentals Right
Establishing risk acceptance, process, reliability
2
Counterparty Identification Program
Customer ID and supporting Documentation
3
Counterparty Due Diligence
Reviewing Documentation, Conducting Due Dil checks, Understanding Risks, Remediation of Risks
4
Counterparty Monitoring
PEP, sanction and adverse media screening, Dossier Management, Periodic Reassessment
5
Audit and Reporting
Internal reporting and audit, external audit, regulatory reporting

As a reminder, the 5 pillars to focus on are:

1. Fundamentals: What is your Risk Appetite and what are your Risk Management policies?

2. Counterparty Identification: Do you have a robust counterparty identification process?

3. Counterparty Due Diligence: Do you have a reliable and unbiased risk assessment process?

4. Counterparty Monitoring: Do you have a real-time awareness of changes in the risks in your counterparty portfolio?

5. Compliance Risk Reporting: Can you efficiently and reliably report on the robustness of your process and risk assessment conclusions?

Our Approach

Building the right compliance management program just requires the proper organization of your setup, operation and assurance processes. If you get these right, you can make your investors' lives easier, avoid compliance fines and save more than 25% per year on a typical alternative investment compliance operation.

Staff augmentation on manual processes is no longer an option. The growing risks and penalties for non-compliance and the rising cost of salaries make this a very bad strategic choice. Automation, education and investment in new technologies is the winning strategy

So as you can see, all you need to do is to integrate 1) the Fundamentals of Risk Acceptance and Risk Management, Configuration and Tuning, 2) a robust Customer Identification process, 3) a standardized and comprehensive Customer Due Diligence and Risk Assessment process, 4) a Continual Customer Monitoring process and 5) a structured and automated event capturing Regulatory Reporting and Audit Review process, into a digital platform with automated workflows, smart dossier management and a secure and direct customer communication portal and you can make your customers happier, boost your bottom line by €200k and never again face a compliance fine.

There are several ways to achieve this:

- You can set this up all in house with the support of major consulting advisors. You will end up with a compliance framework, process and team that mirrors your competitors. This will take at least 1 year and cost well over €800,000 up front with an annual cost of about the same for a small team. Costs will increase steeply as you scale up the team.
- You can pull together various compliance tools and hire a systems integrator to put them all together for you. This will take at least 2 years and cost well over €1,000,000 with an annual cost of at least €800,000 for a small team. Costs will increase, but not as steeply as the first option, as you scale up.
- Or you can work with KYC3. We can deploy a fully configured and ready to use digital compliance automation solution for you for a fraction of the cost and in weeks to months of project time. You can scale your team and your costs will scale evenly and marginally as you increase your business. And if you need help running it, we can even augment your team to help you get the most out of your technology investment.

Your company and KYC3

KYC3 is for alternative investment, wealth management, private equity and virtual asset service providers who are looking to digitize their entire compliance processes, but are struggling with the complexity and technical challenges of integrating everything together within reasonable time and budget constraints.

Here are some people like you that we have worked with…

We have helped companies such as an Africa focused private equity fund with approximately $1billion under management to digitize their AML risk management across 26 team members in offices in France, Luxembourg, Madagascar and several other countries. They were able to reallocate AML/KYC staff onto higher value risk management functions with immediate annual savings in excess of €125,000 and to focus more on enhanced deep-dive due diligence that is expected to help them produce better investment returns over time.

We have digitized compliance for a retail focused brokerage in the United Kingdom, helping them get up and running in less than 2 weeks, recovering from a failure of their KYC provider and getting their client onboarding process fully digital and integrated in record time.

We have automated the risk screening process for an OTC asset trading firm based in Paris, helping them to screen more than 50,000 counterparties involved in their business over the past years and to fully automate the management and reporting of their AML risk.

We have implemented fully digital dossier risk management for a leading private equity firm in the United Kingdom and Luxembourg. Enabling them to leap from manual checklists and processes to a fully integrated compliance process with immediate remediation and real-time risk screening of all of their counterparties and their components.

We helped a $1 trillion dollar investment manager to manage the complex onboarding process for their institutional investors, gathering and managing all document collection and counterparty identification through an automated portal, massively improving the efficiency of their compliance process, their customer experience and giving them much better risk management capabilities.

We helped an international investment fund focused on developing nations to handle complex compliance efficiently, involving NGOs, international organizations, institutional investors, and putting all of this in a simple and effective system where their small team can scale globally without complexity. Again, saving them hundreds of thousands of Euros, reducing their risk and improving their customer experience.

We helped a large Italian based lender to onboard more clients, identify risks and collect required consent and documentation so that their modest anti-fraud team can more effectively identify and mitigate risks, helpling them eliminate more than 1 million Euros per year in fraudulent loan activity.

Here is what’s going to happen when you work with us.

- You will be able to identify your clients quickly and securely.
- Your clients will be able to securely upload their data directly to you.
- You will be able to see the status of all of your dossiers in real time and have no surprises.
- You will be able to manage complex risk and compliance without worry.
- You will be able to easily evaluate client provided documentation with confidence.
- You will be able to see exactly where the risks are in your portfolio of counterparties.
- You will be able to meet your reporting requirements.
- You will be able to manage complex and dynamic KYB structures.
- You will be able to get instant risk assessment updates when structures change or merge.
- You will be able to always get the latest UBO and control charts of each dossier in your system.

- You will get documented records of all your compliance activities, including customer consent to requirements such as GDPR and FATCA/CRS reporting.
- You will analyze risk with complete and reliable records.
- You will respond to regulators and auditors quickly and accurately.
- You will enjoy the benefits of a fully digital process.
- You will no longer rely on checklists, emails and files scattered across folders.
- You can finally get rid of tedious manual remediation audits and report preparation.
- You can forget about audit surprises and lost documents.
- You will feel confident, empowered and have a clear overview of everything under your responsibilities.
- You will never again face an audit or regulatory review with uncertainty or doubt.
- You will never again be fined for non-compliance due to disorganized information or opaque processes.

We develop long term relationships with our clients and improve our capabilities together in collaborative partnership. Our aim is to deliver the solution that allows your company to minimize complexity and enjoy tangible competitive advantages as quickly as possible.

Working together

Our engagements consist of two phases, the first phase consists of **configuring and delivering your digital compliance platform and processes** and ensuring that your company's analysts are able to make efficient use of them. The Second phase is the **long term operation of the Enterprise Risk Management Systems (ERMS)** with occasional short projects for upgrades and revision, as needed. Both of these phases are aimed at helping you to have the most effective and efficient digital compliance program for your business.

Reviewing and confirming your Risk Acceptance Statement, Policies and Procedures

We will review your Risk Acceptance Statement and accompanying policies and procedures, as well as the definition and planned automation of your processes, we can help. Prior to commencing any technology deployment, we are happy to assist with the detailed technical solution architecture and planning. We are also able to help you to address any deficiencies in your compliance risk management program.

Our founder, Jed Grant, is an experienced systems architect with 30 years of enterprise grade solutions experience gained in international institutions, such as NATO, and CSSF regulated financial institutions in Luxembourg, with nearly a decade of board and executive committee member experience under the IML and then CSSF, as well as regulated institutions in France, the UK and Switzerland. Jed or an equally qualified technical and compliance professional leads our pre-deployment consulting and advisory engagements. At the end of this review, we will present you with an assessment and detailed plan of the transformation to digital compliance for your organization.

Get Digital: **KYC3 Enterprise Risk Management System (ERMS) Core**

The KYC3 ERMS delivers your **KYC/KYB client identification, due diligence, continual monitoring and regulatory reporting** in a simple and integrated platform that automates and facilitates the most laborious tasks of compliance.

- KYC3 ERMS features a fully **configurable and customizable legal compliance setup.** Add any type of entity, define the required documentation for each entity and role, manage the geographical jurisdictions. Set up and document your entire AML process in a few screens of configuration.
- KYC3 ERMS **Smart Dossiers** collect all the information for customer identification, documentation, due diligence, structure, risk assessment and monitoring in a simple to use and comprehensive dossier.
- KYC3 ERMS **Risk screening engine** checks your customers against PEP, Sanctions, adverse media and search engines and provides daily updates of any new risks identified. Results are easily reviewed in a “Tinder for Compliance” style interface.
- KYC3 ERMS **Reporting module** gives quick and easy access to detailed audit information on every event, decision and note that has been made in the system.
- KYC3 ERMS **Entity-relations Manager** provides easy visibility of individual relations (KYC) and corporate structures (KYB) for conflict of interest detection, UBO documentation and management control charting.
- KYC3 **Due Diligence Research** portal offers open and flexible access to the full risk intelligence data set, so you can search as easily as using Google. It also offers a comprehensive **report builder** for generating detailed risk assessment reports in PDF format.
- KYC3 ERMS **Dashboard** gives you **an** immediate overview of your dossiers, potential screening risks identified, counterparty demographics and risk profiles - all with comprehensive and simple sort and drill down capabilities.
- KYC3 ERMS **Entity Tagging** system lets you slice and dice your client data however and how-many ways you require, for example, sorting by fund, by customer type, by business unit. You can always get the exact report you need using the right tags.
- The KYC3 ERMS is a **flexible on-premise, own-cloud or hosted SaaS** solution. An instance can be deployed in your company’s data center, with your chosen hosting provider or hosted by KYC3 on your behalf. We coordinate with the technical teams for proper access and security controls and we coordinate with the hosting team to ensure proper business continuity measures are in place.

Get Automated: **KYC3 ERMS Remote Counterparty Onboarding Module**

The identification of clients is a new challenge in a digital world. In order to have the most efficient and secure interactions possible, you will want to enable your system to identify and collect information directly from your clients.

- Your counterparties, both KYC and KYB, can identify themselves with an eIDAS and GDPR compliant process,
- They can securely upload all the information and documents that you need directly to your ERMS platform
- And they can receive alerts and notifications from you and securely connect to the ERMS to provide remedial information whenever necessary.

Using **advanced computer vision, speech recognition, and live video**, we identify your clients and collect the information you require directly in a **secure encrypted portal, branded and integrated with your website.**

Your company white-labeled **Onboarding Portal** includes

- **Integration** with the look and feel of your company website to provide a seamless experience for your customers.
- **Consent recording** to seamlessly capture your customer's consent to terms and conditions
- **Video identification** that records a live video of your customer, proving that they are actually the person providing the information
- **ID document capture** that takes a live image of your customer's passport or identity card and provides automated assessments of ID quality, extraction of the identity data and verification of document checksums.
- **Configurable Forms capture** so you can collect all of the information that you require as structured form data or uploaded documents.
- **Face recognition** to match the identity document with the video.
- **Voice recognition** to verify the authenticity and liveness of the video.
- **Phone number verification and risk assessment** allowing you to get real-time risk intelligence on the customer's provided mobile phone number.
- **Dynamic onboarding for KYB** to collect complex document packages in a simple onboarding wizard.
- **SMS and Email** messaging capabilities to quickly notify customers of required actions.

Deliverables

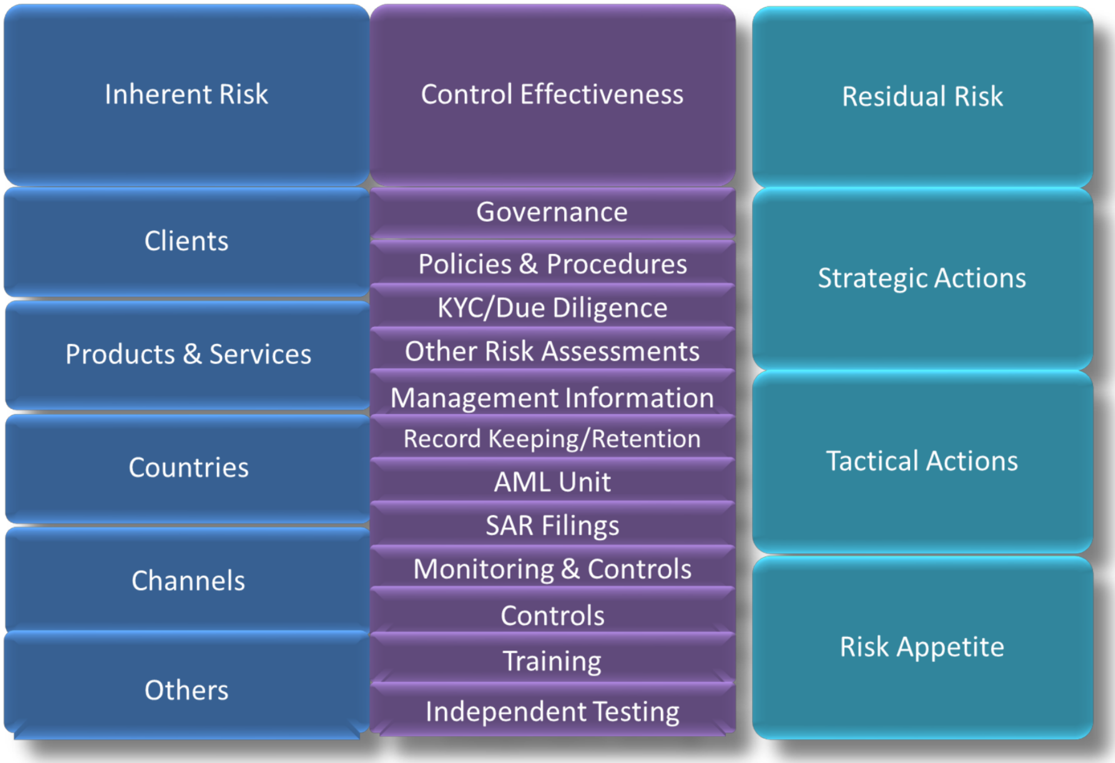
Let's recap all of those features and benefits and put some value on them.

In order to be effective, all the elements need to be integrated and interlocking.

- Your Risk Acceptance Statement needs to map to your Risk Management Procedures.
- Your Customer Identification Process needs to be robust and clear.
- Your Customer Due Diligence Process needs to be standard and well documented.
- Your Customer Monitoring Program must be comprehensive and reactive.
- Your Reporting and Audit trails need to be reliable and clear.

You need all of this to work together, flawlessly and automatically so that you can

1. Manage Inherent Risk from customers and products
2. Achieve Control Effectiveness in your organization and your governance and supervisory structures
3. Make informed decisions regarding your Residual Risks



Inherent Risk

Clients

Products & Services

Countries

Channels

Others

Control Effectiveness

Governance

Policies & Procedures

KYC/Due Diligence

Other Risk Assessments

Management Information

Record Keeping/Retention

AML Unit

SAR Filings

Monitoring & Controls

Controls

Training

Independent Testing

Residual Risk

Strategic Actions

Tactical Actions

Risk Appetite

[1]

There are 3 main phases involved in the establishment and operation of an effective AML risk management program covering all of the activities described above for a small compliance team operating in an alternative investments or fintech niche.

First there is the setup. Develop a system with a compliance expert. Define checklists, documents and periodic reviews. Build risk evaluation methods, print, sign and record

[1] Source: The Wolfsberg Frequently Asked Questions on Risk Assessments for Money Laundering, Sanctions and Bribery & Corruption

everything. Make sure audit records are in place. This effort involves at least €250,000 in resources to achieve. Typically amortized over 5 years, this represents €50,000 per year.

Second there is the operation. Collect documents; review risk, and manage dossiers. Identify risk, conflicts of interest or other potential negative aspects. Build new dossiers, conduct risk assessments and manage corporate changes within counterparties and investments. Ensure proper risk screening, review, remediation and follow up. A typical operation with 3 full time employees has a fully loaded annual cost of at least €450,000.

Third, there are the assurance efforts: board reporting, audits and regulatory reviews. Prepare reports based on regular or periodic demand. Gather and collate documentation. Verify facts and statistics across processes. Confirm the application of policy and procedure. Synthesize summaries and evidence to third parties that reports are accurate and reliable. In a mid-sized investment firm, this effort typically engenders at least ½ full time equivalent (FTE) annually plus external service providers, representing a fully loaded annual cost of at least €250,000.

Our solution delivers on all 3 areas. We focus our efforts on the efficiency and reliability of the processes we enable. This means that your company can handle more growth with less cost, delivering real bottom line gains.

Fully loaded cost of 4-6 FTE compliance professionals		**€800,000.00**
Efficiency Gain	Probability of Realization	Expected Values
0%	2%	€0.00
10%	3%	€2,400.00
15%	15%	€18,000.00
35%	65%	€182,000.00
50%	15%	€60,000.00
Expected gains		**€262,400.00**

Against a base subscription of €4,000 per month, this represents **more than a 500% annual Return on Investment** on the typical annual investment in our core solution and support.

A typical comprehensive IT project of this scale typically has a 3 year breakeven, making annual savings of this order of magnitude worth at least €750,000 .

Summary

By adopting a fully digital compliance process on an integrated platform, you can achieve massive capability gains, deliver savings that flow through to your bottom line, and help you achieve the compliance and customer satisfaction you have always wanted.

Since its inception, KYC3 has developed its own intellectual property and provides SaaS solutions tailored to the needs of AIFM and crypto-asset firms. Our solution eliminates the labor and risk inherent in old school manual dossier processing and tracking systems based on document stores, Excel spreadsheets and email communications by providing an integrated dossier management and risk screening environment with a complete audit trail and a white labeled secure counterparty portal for document collection. Our systems have handled millions of name screening checks and thousands upon thousands of client onboardings.

So let's summarize what you get with KYC3's fully integrated and digital compliance ERMS:

Fundamentals

- Adjusting your Risk Acceptance Statement to match your capacity to manage risk
- Streamlining your compliance process and improving your operational controls
- Automating the risk assessment process for continual and consistent compliance

Customer Identification and Dossier Constitution

- Identifying your clients, even if they are complex entity structures
- Collecting documentation through your own secure digital portal directly into your platform
- Secure authentication through video and identity verification

Customer Due Diligence and Dossier Management

- Quickly reviewing and evaluating provided documentation
- Understanding your clients with automated structure charts and visual risk indicators
- Conducting proper due diligence with built-in PEP, sanction, adverse media and search engine screening
- Automatic "to-do" remediation actions are added based on risk assessments

KYC/KYB AML Monitoring

- See your risk and compliance "big picture" in an easy to understand, always up-to-date dashboard.
- Receive daily alerts of any new PEP, sanction or adverse media elements
- Receive real-time alerts for all expired or outdated documents
- Automatically be notified of mandatory reviews based on risk levels

- Automatically add “to-do” remediation actions to dossiers when customer circumstances change or to meet new regulatory requirements
- Simply merge complex structures together when deals are consummated and have all risk updated accordingly

Regulatory and Audit Reporting

- Produce simple to use risk overviews for regular board meetings, investment committee meetings and more.
- Push button detailed audit reports and full customer dossier reports for auditors and regulators.
- Detailed screening metrics reporting.
- Slice and dice your entity data with tags that you define. Group customers by fund, by business type, by investment, or however you need.

Our solution is designed to deliver on all key areas, focusing on efficiency and reliability to enable your company to handle more growth with less cost. With a fully loaded cost of 4-6 FTE compliance professionals at €800,000, our solution offers significant efficiency gains and expected gains of €262,400. This represents more than a 500% annual Return on Investment on the typical annual investment in our core solution and support, making it a highly valuable and cost-effective option for your company. With a strong focus on delivering real bottom line gains, our solution is a smart investment for any company looking to streamline processes and maximize growth potential.

Take the first step towards transforming your company's compliance landscape and unlocking unprecedented growth. Don't let the opportunity to achieve over 500% annual ROI and significant cost savings pass you by. Contact KYC3 today to explore how our innovative solution can specifically benefit your organization. As a decision-maker, you have the power to steer your company towards greater efficiency and profitability. Let's discuss how we can make this a reality for you. Act now—your company's future success awaits.

Please tell us more about yourself and book a call! https://go.kyc3.com

Annex FAQ

Q: What about GDPR and data protection?

A: Our system is designed with GDPR in mind. **You remain the custodian of your client data at all times and are in complete control from a GDPR perspective.** The exposure of your client data to KYC3 is minimized to a small number of "data processing" cases and data is not retained.

Q: If the solution is on-premise or "own-cloud", how does that work?

A: We deploy the system to your preferred host platform. If your company does not have a preferred hosting provider, KYC3 can work with any trusted provider of your choice: AWS, Azure, Google, anyone. You own the hosting infrastructure contract.

Q: Do we have to decide on all of those options at the start?

A: You can start basic and add features later on. We are happy to start small and grow with you.

Q: Can we have a "free trial"?

A: KYC3 ERMS is an enterprise software platform that is delivered per client. The software is highly customizable and requires preparation before use. Unfortunately we are not able to offer "free trials" due to the set-up and configuration requirements.

Q: What about security?

A: Your client data, your documents and your conclusions all reside in the ERMS platform that we deploy for you in your preferred host platform. Cyber security and BCP are integrated with your infrastructure and to your needs. That said, our compute cluster is hosted in an ISO27001 data center and we employ industry standard security protocols and procedures to limit access to the cluster. None of your data is stored in our cluster.

Q: Can we audit your systems?

A: We are also ready to conduct any feasible test or security audit that you may request on our systems, if you are prepared to cover the third party expenses.

Q: Are you a regulated company?

A: We are an authorized Luxembourg limited liability establishment with a regular business license issued by the Ministry of the Economy.

We have not applied for a PSF license as the current scope of our services doesn't fall under the regulatory regime and would cause significant price increases in our services. That said, KYC3 is capitalized and organized so that it may become a regulated service provider in Luxembourg under the CSSF should our service offering expand or the regulator requests that we do so.

Q: What are your standard terms and conditions?

A: An agreement of 3 annual terms with invoicing at the start of each term**.** Delivery commences upon reception of the signed Service Agreement and effective payment received. The standard terms for KYC3 services apply.

Q: We have a detailed risk assessment process and need to be sure that it will work with your system?

A: If you require detailed risk assessment engine configuration to match your policies and procedures, we can deliver it.

We can tune and configure the ERMS risk assessment engine to match the existing standards used within your company's business and partner businesses. This is a one-off exercise that saves time and avoids the frustration of change.

We review the risk calculations across all dimensions of risk: PEP, sanction, ML/CFT, reputation, structure, jurisdictions and more. Using your company's existing risk management methods and tools as a baseline, we will configure the system and the risk screening engine to produce compatible results.

We will work with your company's compliance team to validate and tune/adjust as necessary to ensure that results are as expected during the first 6 weeks of operation.

Q: We already have our customer data in an existing system. Can we import the data directly to the KYC3 system?

If you have legacy systems containing data that you would like to load into your platform, we can assist you with the extraction, transformation and loading of the data into the ERMS.

Manually loading data into a system can be time consuming and is very laborious and error prone work. For the cost of a few man-days, we can map out and automate this work to load your data efficiently and without errors.

We will conduct a review and assessment of the existing documentation and data and devise a data extraction, transformation and loading (ETL) plan so that the KYC3 ERMS can be loaded with existing client data from the first moment of production. Existing digital assets will be considered and structured data will be incorporated directly into the system meta-data while unstructured data, i.e. scanned documents, will be imported into the document management.

We will organize and load the electronic data into the system in accordance with the defined ETL plan.

Q: We will need to be trained. Can you train us on how to best use the system?

A: Absolutely. Well trained employees will make the best use of the tools they are given. While the least expensive option of the KYC3 deployment options, a 5% gain in efficiency repeated on a daily basis over 180 working days is 45 days for a team of 5, representing ROI of at least 500% on the training investment.

We will deliver detailed training on how to use the KYC3 ERMS. Training is delivered in English via Zoom conference or in person in Luxembourg. Basic training can be completed in a 3 hour session.

Q: Can we interface KYC3 with our core systems?

A: Yes, we provide a full API and can assist with integration. If there are manual processes that would be required to interface between the KYC3 ERMS compliance platform and other core systems, such as an investment management or CRMsystem, investing in automating these integrations saves time and reduces manual manipulation errors and always represents a very good ROI over the long term. We can help evaluate where such expenditures make sense and then help carry them out as cost effectively as possible.

We will develop a common understanding of the detailed requirements of the systems and share how KYC3 technology can best fit into the solution. To do this we will review the desired KYC processes as defined by project management at your company and evaluate where KYC3 can provide maximum benefits.

Q: We have a lot of data and/or demanding BCP requirements, such as redundant systems. Can you scale for our business?

A: Yes. The ERMS system is designed to hold documents for hundreds of thousands or even millions of entities across a distributed and redundant database. We can support data sets up to hundreds of thousands or millions of full digital dossiers.

We can configure multiple ERMS systems to replicate or share data across them. This is useful for business continuity planning and multi-jurisdictional compliance.

We will lead or assist your company's chosen systems integrator to implement the planned integrations. We can engineer deployments that use swarmed, clustered or replicated instances and can support multi-instance BCP installations.

Q: Can you help with the review and elaboration of our existing procedures and provide advisory?

A: Yes, our analysts can work with you to review your compliance program with advisory and assistance on the 5 program elements: Risk Acceptance, Counterparty ID, Counterparty Duedil, Counterparty Monitoring and Compliance Risk Reporting.

We can provide assistance with the formulation and/or adaptation of the Risk Acceptance Statement, the AML Program Policies and/or the AML Program Procedures in light of the capabilities that KYC3 brings to your organization.

Q: What is included in the core KYC3 SaaS ERMS Monthly operating subscription?

A: Access to the KYC3 SaaS ERMS.

Nightly PEP, Sanction and Adverse Media screening.

Access to the KYC3 Compute Cluster for data updates, including full access to our proprietary FACT4 risk database.

System updates, bug fixes and ongoing minor releases.

Simple and remedial technical support by email, video or voice call during CET/CEST working hours on regular business days.

Q: What is included in the Onboarding Portal subscription?

Operation of a white-labeled onboarding portal instance with the KYC3 ERMS.

Updates and minor adjustments of forms, user interfaces and other minor changes to keep abreast with your company's regulatory requirements and commercial web presence as they evolve.

Q: Can we use the World-Check Refinitiv Data for screening?

A: Absolutely. We have a module that allows the system to download the Refinitiv data file on a nightly basis and include Refinitiv data in the risk screening process. To make use of this option, your company must also have a separate data license with Refinitiv.

Q: What are your typical engagement goals and terms?

A: We deliver value in the form of better solutions to the overall process of compliance and risk management. We look at how we can automate and streamline current working processes. We seek feedback from our clients and the industry in order to prioritize and capture as much value for our clients as quickly and efficiently as possible. An agreement of 3 annual terms with invoicing at the start of each term. Delivery commences upon reception of the signed Service Agreement and effective payment received by KYC3.

Q: What is FACT4 and what data is in it?

A: FACT4 is our risk intelligence database. It includes more than 250 million documents gathered since the inception of KYC3 and with history going back more than 30 years in some cases. Every major sanction list is included from around the world with more than 80,000 sanctioned entities, PEP information from many international sources and our own proprietary sources covering over 1 million people and state-owned enterprises, adverse media from more than 110,000 media sources categorized and risk assessed by our FACT4 AI, and company data from several European countries, including the UK, France, Luxembourg and more.

Q: Although FACT4 has some business registries, can you provide more company information?

A: Yes, we can integrate with any company data API that you would like to use. For example, the EBR API allows access to the European Business Registry data on demand. The EBR charges a per-document fee for downloading the documents into your system.

Q: Can you help us with operational compliance support to use the system?

A: Yes, KYC3's analysts can assist your company with the operation of the ERMS. Engagements are led by an ACAMS certified anti-money laundering specialist.

Q: Can you offer bespoke Support and Training for our specific SLA requirements?

A: Yes, we can provide extended technical support to your company's IT team or systems integrator. We can arrange dedicated training sessions for new staff or advanced and bespoke training for existing KYC3 users.

Q: Can you help us with our audit or regulatory review for specific points, if needed?

A: Yes, we can provide executive support directly with your company while engaging in tandem with auditors and supervisory bodies in order to assist with audits or other reviews, covering any points related to our solution, its use and review.