Guide to risk-based AML compliance: What firms need to know about managing risk

How to make sure your AML programme is doing it right

Contents

Introduction

A risk-based approach has become a key element of anti-money laundering (AML) compliance. It's easy to see why: A firm with an AML compliance programme that focuses efforts based on the level of risk indicates a firm that is thinking efficiently and wisely about how to manage its risk and exposure to financial crime.

The approach calls for skill in both risk assessment and the ability to react quickly. Due diligence needs to be conducted and regulatory changes need to be monitored, with the understanding that a regulatory change, such as a new jurisdiction being made high risk, can impact the criteria for high risk in your firm.

It's the best way to run an AML compliance programme but it's important to note that a risk-based approach is not necessarily cheaper or faster because saving money and speed are not the main purposes of a risk-based approach – the reduction in the risk of a compliance failure is.

How do you run an effective AML compliance programme that employs a risk-based approach? What are the strategies and procedures to determine that your risk-based approach is robust, protects your firm and meets the expectations of regulators?

We compiled this guide to help you do just that.

What exactly is a risk-based approach?

A risk-based approach (RBA) means you are identifying the highest compliance risks to your organisation and making them a priority for the organisation's compliance controls, policies and procedures. These are the measures put in place to mitigate that risk. Once your compliance programme reduces those highest risks to acceptable levels, it moves on to medium and then lower risks.

RBA involves not only understanding the risks your organisation faces but also creating controls for these risks based on prioritising the damage they could potentially inflict.

A brief history of the risk-based approach

Prior to the introduction of the risk-based approach to AML, firms would manage their compliance obligations using a 'checkbox' approach – meaning a standardised list of AML requirements was applied to every customer.

That standardised approach prevailed in the 1990s. The UK's Financial Services Authority (FSA), first proposed a risk-based approach in its 2000 publication, A New Regulator for the New Millennium.

The concept of a risk-based approach for AML was first proposed in 2007 by the

Financial Action Task Force (FATF), an inter-governmental body that sets international standards for AML. It was further codified in its 2012 update to the International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation. According to the FATF recommendations, a risk-based approach:

"allows countries, within the framework of the FATF requirements, to adopt a more flexible set of measures in order to target their resources more effectively and apply preventive measures that are commensurate to the nature of risks, in order to focus their efforts in the most effective way."

The FATF's 2012 endorsement of the risk-based approach to AML set the global standard and ensured its ongoing use across all FATF signatories. The FATF stated that:

> "The risk-based approach is central to the effective implementation of the FATF Recommendations."

The virtues of a risk-based approach

The reason regulators believe a risk-based approach is effective is simple: Your firm's highest compliance risks will cause the highest interruption if they happen, resulting in time spent on research, regulatory settlements, unwanted headlines, and endangered business partnerships, among other things.

A risk-based approach also demonstrates to regulators that your firm really worries about its risks and works to mitigate them.

For instance, if you perform the same due diligence procedures on all clients, it could be less efficient. Many of your firm's clients are harmless, while others may present a significant risk. Applying the same standard to all of them indicates that the firm is not thinking about its compliance risks, suggesting instead that the company is only thinking about demonstrating compliance with one more requirement, in this case, due diligence.

Once regulators have that idea in mind – that perhaps the company sees compliance as an item on a checklist to finish as soon as possible – you are in a much worse position. Regulators may begin questioning the sincerity of the company regarding compliance, as well as its ability to comply.

The main elements of a risk-based approach

A risk-based approach focuses efforts based on the level of risk. It involves firms mitigating the risks that they face, with regard to the resources available. Mitigating practices include initial client due diligence (CDD) and ongoing monitoring, as well as a range of internal policies, training, and systems to address the vulnerabilities of the firm.

The key is to implement controls to limit the potential money laundering / terrorist financing (ML/TF) risks your firm identified while conducting risk assessments to stay within your risk tolerance level.

The basic elements of the risk-based approach are:

Risk identification and assessment
This involves identifying money laundering / terrorist financing (ML/TF) risks facing a firm, taking into account its customers, services, countries of operation, and publicly available information regarding those risks

Risk management and mitigation
This involves identifying and applying measures to effectively and efficiently mitigate and manage ML/TF risks

Ongoing monitoring
This involves putting in place policies, procedures, and information systems to monitor changes to ML/TF risks

Documentation
This involves documenting risk assessments, strategies, policies and procedures to monitor, manage and mitigate ML/TF risks

It's important to note: An effective risk-based approach involves a firm's access to accurate, timely and objective information on ML/TF risks. If information is not readily available because authorities have inadequate data to assess risks, are unable to share relevant information on ML/TF risks and threats or access to information is restricted by censorship or data protection provisions, it will be difficult for firms to correctly identify ML/TF risk.

Risk identification and assessment

To identify the risk:

Potential ML/TF risks faced by law firms will vary according to many factors including the activities undertaken by them, the type and identity of the client and the nature and origin of the client relationship.

Certain activities have been found to be more susceptible to ML/TF activities because they involve the movement or management of client assets. These specified activities include:

- Buying and selling of real estate
- Managing of client money, securities, or other assets
- Management of bank, savings, or securities accounts
- Organisation of contributions for the creation, operation, or management of companies
- Buying and selling of business entities

This susceptibility is heightened when these activities are conducted across countries.

To assess the risk:

Firms need to determine how the identified ML/TF threats will affect them. They should analyse the information to understand the likelihood of these risks occurring, and the impact that these would have on the firm.

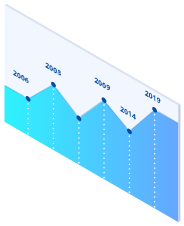
Firms may assess ML/TF risks by applying various categories. ML/TF risks are usually classified as low, medium, or high. The most commonly-used risk categories are:

- Country or geographic risk
- Client risk
- Risk associated with the particular service offered

Firms need to remember that:

Risk assessment information forms the basis for effective ML/TF risk mitigation and should be kept up-to-date

Firms should develop internal policies, procedures, and controls, including appropriate compliance management arrangements and an ongoing employee training programme



Firms may be well-positioned to identify and detect changes in the type of work or the nature of the client's activities in the course of the business relationship

Risk management and mitigation

Identification of the ML/TF risks associated with clients and certain types of work will enable firms to determine and implement reasonable and proportionate measures to manage and mitigate their risks.

Risk mitigating practices include:

- Initial and ongoing CDD
- Internal policies, training, and procedures
  - These should address the specific vulnerabilities the firm faces

In a risk-based approach, the FATF recommends that firms can decide on the most appropriate and effective way to mitigate the ML/TF risk they have identified. These measures should be tailored to the specific risks faced to ensure the risk is adequately addressed and to assist in the appropriate allocation of resources for CDD.

Enhanced CDD measures should be used when the ML/TF risk is higher. In such cases:

- Firms should consider the extent to which they might be involved in unwittingly enabling the substantive offence of ML/TF by providing a legal service
- Firms should consider not providing services or continuing a business relationship with the client

Less stringent measures may be applied in lower-risk situations such as:

- A financial activity is carried out by a natural or legal person on an occasional or very limited basis
- If the firm is representing a client in a single transaction

A key element of a firm's risk management and mitigation is the training that firms are required to provide their staff to identify and detect relevant changes in client activity by reference to risk-based criteria.

These measures and controls may include:

- General training on ML/TF methods and risks relevant to legal professionals
- Targeted training for increased risk awareness for legal professionals
  - Providing specific activities to higher-risk clients
  - Undertaking higher-risk work
- Increased or more appropriately targeted CDD or enhanced CDD for higher-risk clients/situations
  - Providing a better understanding of the potential source of risk
  - Obtaining the necessary information to make informed decisions about how (or whether) to proceed
  - When and how to ascertain evidence and record source of wealth and beneficial ownership information
- Periodic review of the services offered by the firm
- Periodic evaluation of the firm's AML/CFT procedures
  - To determine whether the ML/TF risk has increased
  - To determine whether adequate controls are in place to mitigate those increased risks
- Reviewing client relationships periodically to determine whether the ML/TF risk has increased

Ongoing monitoring

In a risk-based approach, ongoing monitoring is conducted in accordance with the risk level of the client. Your firm's high-risk clients need to be monitored regularly. But it's important to remember that your low-risk clients' status can change easily and quickly so even low-risk clients require some monitoring, relative to the risk they pose.

- During the course of a relationship with a client, a firm needs procedures for ongoing monitoring and review of the client/ transactional risk profile
- The amount and degree of ongoing monitoring and review will depend on the nature and frequency of your firm's relationship with the client and the assessment of the risk involved
- Risk assessments of specific clients may have to be adjusted based on information received from credible sources during reviews

An ongoing monitoring checklist:

- ✓ Re-evaluate your CDD at appropriate intervals
- ✓ Suspend or terminate a business relationship until you have updated information or documents (unless you are fully satisfied you know who your client is)
- ✓ Keep any request you have made for information or documents under review
- ✓ Use technology to aid your ongoing monitoring

When you need enhanced ongoing monitoring

Enhanced ongoing monitoring is automatically required whenever enhanced due diligence (EDD) is applied.

EDD may be required for people or situations that indicate a higher risk. These could involve:

- A business relationship that seems unusual
- A company with a beneficial ownership structure that seems excessively complex
- Non-resident customers or those subject to economic sanctions
- Legal persons or arrangements that are personal asset-holding vehicles
- Companies that have nominee shareholders or shares in bearer form
- Cash-intensive businesses
- Countries subject to sanctions, high risk lists, or embargoes or with significant levels of corruption or criminal activity
- Countries funding or supporting terrorist activities or having designated terrorist organisations operating within their country
- Payments received from unknown or unassociated third parties

One aspect of keeping transactions under review is to ensure they are still in line with the CDD information held on the client, and information contained in the client and matter risk assessments. Whatever controls you have in place to monitor other business relationships, may be intensified in order to apply enhanced monitoring.

This may include:

- Requiring a greater level of information and explanation from the client when activity diverts from that addressed in their client risk assessment
- Greater frequency of checks on transactions
- Undertaking more frequent due diligence checks on your client

Documentation

Once a firm understands its ML/TF risks, its assessments should, in most cases, be documented to be able to demonstrate their basis. (In some cases, such as if the specific risks inherent to the sector are clearly identified and understood, individual documented risk assessments might not be required.)

A documented risk assessment may cover a range of specific risks by breaking them down into three common categories

- Geographic risks
- Client-based risks
- Service-based risks

Each of these risks could be assessed using indicators such as low risk, medium risk, and/or high risk. A short explanation of the reasons for each attribution should be included and an overall assessment of risk determined.

An action plan could accompany the assessment.

The plan could:

- Help identify potential red flags
- Facilitate risk assessment
- Determine CDD measures to be applied

The written risk assessments should be made accessible to all the professionals involved in AML/CFT at the firm.

Risk assessments on longer-term transactions should be done at suitable intervals to ensure no significant risk factors have changed. A final risk assessment should be undertaken before a transaction has been completed.

Risk assessments: What your firm needs to know

As part of your risk-based approach, it's important to focus on the key levels of risk assessment:

Practice Wide Risk Assessments (PWRAs)

Involve a comprehensive way to identify and assess the ML / TF risks your firm faces. This level is fundamental to your AML compliance

Client risk assessments

Involve identifying and assessing the ML/TF risks at the individual client level

Matter risk assessments

Should be undertaken on each new matter for a client, specifically where risks are new or non-repetitive

As new risks are identified at client or matter level, these should inform and allow the updating of higher-level assessments.

Practice-wide risk assessment:

A general overview of the practice, addressing its key features, including:

- Number of partners/staff and other metrics indicating the scale of the practice
- Rate of staff turnover (If relevant) and other aspects of staff culture
- A description of the work areas of the firm
- Types of clients served
- Stability of the client base
- Location of the firm
- Any international exposure the firm might have

A firm needs to maintain a documented PWRA. It must address risk factors relating to:

- Your clients
  - Demographics, PEPs, or close relatives or associates of PEPs
- Countries or geographic areas in which your firm operates
- Countries/geographic areas to which your clients are linked
- Your products or services
  - Such as conveyancing, tax advice, forming of trusts, or client bank accounts
- Your transactions
  - Addressing size, frequency, or complexity
- Your delivery channels
  - Online or via apps or portals, in person or remotely

The PWRA must be comprehensive, tailored to the firm, accurate and kept up to date. The better the quality of the PWRA, the easier it will be for your firm to take a risk-based approach to protecting itself from exposure to financial crime.

Client risk assessments

While your initial risk assessment should always be performed at the beginning of a client relationship, firms should be aware that for some clients, additional information to inform the risk profile may only emerge once further information becomes available or the relationship or matter progresses. The better you know your client and understand your instructions, the better placed you will be to assess risks, spot suspicious activities and protect your practice.

Fundamental to any assessment of client risk is an assessment of whether the client's data align with the background and wider profile of the client. Specifically, the client's:

- Financial circumstances
- Main business activities
- Source of wealth
- Source of funds

Red flags in your client risk assessments:

- The structure or nature of the client entity makes it difficult to identify the true beneficial owner
- The client appears to be attempting to obscure understanding of their business, ownership, or the nature of their matters
- The client is a PEP or is closely related to or associated with a PEP
- The instruction from the client is channelled through a 3rd party and there is a lack of direct interaction with the client
- There are any geographic risks associated with the client
- The client wants to conduct the business relationship or request services in unusual circumstances
- The firm is aware that clients hold residence rights or citizenship in a jurisdiction in exchange for capital transfers, purchase of property, or government bonds
- The client is seeking advice or implementation of an arrangement that has indicators of a tax evasive purpose
- The adverse media about your client is apparent

Your staff should be trained to identify any warning signs as a mitigation to be recorded in your PWRA.

Matter risk assessments:

A focus on the specific risk factors that a matter presents, beyond the client risks already identified.

For each matter you should:

- Identify the client and the beneficiaries of the matter and obtain an understanding of the source of funds and wealth of the client/owners and the purpose of the matter
- Understand the service you are going to provide and whether you have the expertise to deliver it, and whether/how the service could lead to the laundering of money
- Understand why your services are needed, whether a personal or commercial rationale and whether it appears reasonable or genuine
- Be vigilant to red flags
- Make a determination as to what action you need to take, including what evidence you need to collect and ongoing monitoring requirements
- Document and record all steps taken

Matter risk assessments will help you to consider whether you are comfortable acting and if so, to adjust your internal controls to the appropriate level according to the risk presented.

A matter risk assessment sample question list:

- ✓ Are there any features in the matter which may represent a higher risk?
- ✓ Is the matter generally complex in nature?
- ✓ Is the matter undertaken at short notice, within a short timescale, or involving high volumes?
- ✓ Does the matter involve new sources of finance – anything unregulated such as crowdfunding platforms or some aspects of bitcoin/cryptocurrencies?
- ✓ Does the matter involve trust or other legal entity company formation, management, or service provision?
- ✓ Is the matter routine for the practice, and if not, does lack of experience or expertise add to the risk?
- ✓ Do the source of funds or the parties to the matter frequently change?
- ✓ Is the matter longer term in nature, or does it involve funds being locked in for substantial periods of time?
- ✓ Is the matter publicly funded by the UK or a similarly reputable government?
- ✓ Is the matter publicly funded from jurisdictions where corruption is prevalent?

A matter risk assessment is less likely to be needed where:

- Matters undertaken for a given client are highly repetitive, with risk remaining consistent between one matter and another, and the risk is addressed comprehensively by the client risk assessment
- The firm is providing an ongoing Registered Office facility for the client, though ongoing monitoring of this relationship should still be required

Red flags in your matter risk assessments are:

- The size, nature, purpose, commercial rationale or complexity of the matter are unusual or unclear
- The source of wealth or funds involved in the matter is unclear or obscured
- There is involvement of or payment to or from 3rd parties, especially where the relationship between the parties does not seem clear or the payments do not make sense in the overall transaction
- There is difficulty in identifying structures/ beneficiaries/interests involved in a matter
- The matter involves structuring of a transaction which obscures understanding of the nature of the transaction or ownership of the entities involved
- The level and type of matter do not fit the client's profile or involve a sector in which the client would not ordinarily operate

The red flags your firm needs to look out for in managing risk

1. Transactional risks

- A request by the client for financial transactions to occur outside of the legal professional's trust account
- Services that are capable of concealing beneficial ownership from authorities
- Services that rely heavily on new technologies that have inherent vulnerabilities to exploitation by criminals
- Transfer of real estate or other high-value goods or assets between parties in a period that is unusually short with no apparent legitimate reason
- Payments received from un-associated or unknown third parties and payments in cash where this would not be a typical method of payment
- Transactions where it is readily apparent to the legal professional that there is inadequate consideration
- The use of shell companies, companies with ownership through nominee shares or bearer shares and control through nominee and corporate directors without an apparent legitimate reason
- Services that have deliberately provided, or depend upon, more anonymity in relation to the client's identity or regarding other participants, than is normal under the circumstances

2. Product risks

- Large volume/high-value conveyancing
- Corporate acquisitions
- Tax mitigation strategies
- Work involving high-risk jurisdictions
- The creation and/or management of specialist entities

3. Delivery Channel risks

- Matters that rely on indirect contact with your client (e.g., via a representative or agent) rather than holding a direct relationship with the client
- Activity that is delivered online or via any other channel that may facilitate anonymity
- Questionable methods used to undertake identification and verification and general due diligence requirements

4. Delivery Channel risks

- Countries identified as providing funding or support for terrorist activities or that have designated terrorist organisations operating within them
- Countries identified as having significant levels of organised crime, corruption, or other criminal activity, including source or transit countries for illegal drugs, human trafficking and smuggling and illegal gambling
- Countries subject to sanctions, embargoes, or similar measures issued by international organisations
- Countries identified as having weak governance, law enforcement, and regulatory regimes, including countries identified by FATF statements as having weak AML/CFT regimes
- Countries identified to be uncooperative in providing beneficial ownership information to authorities

5. Client risks

- PEPs and persons closely associated with or related to PEPs
- Clients conducting their business relationship or requesting services in unusual or unconventional circumstances
- Clients where the structure or nature of the entity or relationship makes it difficult to identify in a timely manner the true beneficial owner or controlling interests
- Clients attempting to obscure understanding of their business, ownership or the nature of their transactions, such as
- Unexplained use of shell and/or shelf companies, front companies, legal entities with ownership through nominee shares or bearer shares
- Control through nominee and corporate directors, legal persons or legal arrangements
- Splitting company formation and asset administration over different countries, all without any apparent legitimate reason
- Unexplained use of informal arrangements such as family or close associates acting as nominee shareholders or directors
- Unusual complexity in control or ownership structures without a clear explanation, where certain circumstances, structures, geographical locations, international activities, or other factors are not consistent with the legal professionals' understanding of the client's business and economic purpose
- Client companies that operate a considerable part of their business in or have major subsidiaries in countries that may pose a higher geographic risk
- Clients that are cash (and/or cash equivalent) intensive businesses

The challenges for firms in a risk-based approach

Each firm has distinctive elements and in implementing a risk-based approach, legal professionals will need to make reasonable judgements for their particular services and activities. Their risk-based approach should be based on their firm's unique characteristics and practice profile. This may mean that legal professionals and firms adopt different detailed practices.

Appropriate mitigation measures will also depend on the nature of the legal professional's role and involvement. Circumstances may vary considerably between professionals who represent clients directly and those who are engaged for distinct purposes. Where these services involve tax laws and regulations, legal professionals also have additional considerations related to a country's or jurisdiction's permissible means to structure transactions and entities or operations to legally avoid and/or minimise taxes.

Legal professionals can be involved in the formation, management, or administration of legal entities and arrangements. In this role, they may encounter challenges in keeping current and accurate beneficial ownership information depending upon the nature and activities of their client. Other challenges may arise when onboarding new clients with minimal economic activity associated with the legal entity and/or its owners. Additionally,

whether the source is a public registry, another third-party source, or the client, there is always a potential risk in the correctness of the information, in particular where the underlying information has been provided by the client.

Although the implementation of a risk-based approach should not impair a client's right of access to justice, legal professionals and their firms must be alert to ML/TF risks posed by the services they provide to avoid the possibility that they may unwittingly commit or become an accessory to the commission of an ML/TF offence.

This may include restricting the method and source of payments for the services being provided, dictating greater focus on monitoring and reporting clients and their funds for unusual or suspicious activity.

There is a complicated interplay between the requirement to comply with AML/CFT obligations and the principle of legal professional privilege. Many countries provide exceptions in the law that allow legal professionals to make disclosures of suspicion of ML/TF without incurring penalties or liability or breaching ethical obligations and in others to provide an exception to disclosure if the information is directly encompassed by a legitimate claim of privilege.

Legal professionals may be cautious in making disclosures that would otherwise breach privilege or confidentiality rules due to uncertainties in the application of these exceptions, lack of adequate information or training in relation to these rules, the complexities of their clients' situations, or a combination of these factors. Criminals may misperceive that legal professional privilege and professional secrecy will delay, obstruct or prevent investigation or prosecution by authorities if they utilise the services of a legal professional. With a risk-based approach to AML compliance, this does not have to be the case.

A risk-based approach for law firms

Here is a practical step-by-step guide for law firms – especially smaller ones – to implement the risk-based approach.

Client acceptance and know your client policies: identify the client and its beneficial owners and the true "beneficiaries" of the transaction. Obtain an understanding of the source of funds and source of wealth of the client where required, its owners and the purpose of the transaction.

Engagement acceptance policies: understand the nature of the work. Legal professionals should know the exact nature of the service that they are providing and have an understanding of how that work could facilitate the movement or obscuring of the proceeds of crime.

Understand the commercial or personal rationale for the work: legal professionals need to be reasonably satisfied that there is a commercial or personal rationale for the work undertaken. Legal professionals are not obliged to objectively assess the commercial or personal rationale if it appears reasonable and genuine.

Be attentive to red flag indicators: exercise vigilance in identifying and then carefully reviewing aspects of the transaction if there are reasonable grounds to suspect that funds are the proceeds of criminal activity, or related to terrorist financing. Subject to qualifications, these cases could trigger reporting obligations.

Consider what action needs to be taken and have a plan: the outcomes of a risk assessment of a particular client or transaction will dictate the level and nature of the evidence/documentation collated under a firm's CDD/EDD procedures.

Documentation: legal professionals should adequately document and record all steps taken.

Principles of the risk-based approach to AML

In conclusion, the risk-based approach to AML shifts the focus of AML compliance from post-analysis of data, to proactive judgement. Firms must work on an ongoing basis to understand the money laundering threats they face and deploy commensurate measures to manage their risk exposure.

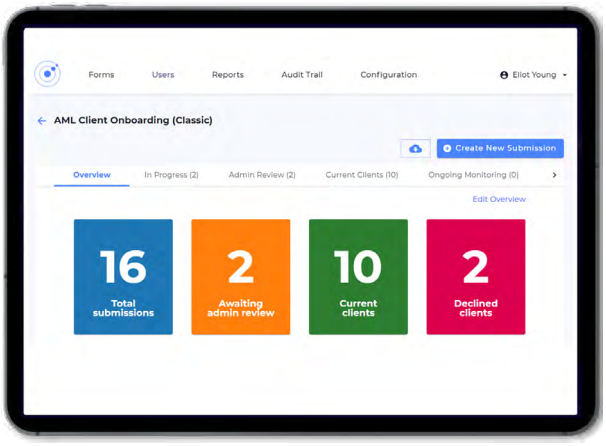
In practice, this means that customers may be classified individually by their risk exposure – and that 'higher risk' customers are under greater levels of AML scrutiny. Broadly, the risk-based approach to AML allows firms to:

- Recognize the existence of risk
- Perform assessments of risk
- Develop and deploy strategies to address risks

Implemented effectively, the risk-based approach allows for a balanced integration of human judgement and smart technology in the AML compliance process.

VinciWorks' AML client onboarding solution

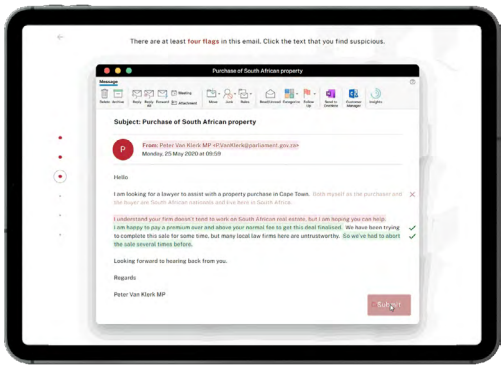
Omnitrack, VinciWorks' AML client onboarding solution enhances both the risk assessment and document collection aspects of client onboarding. Our template workflows adapt to the specific risks posed by each client, based on factors such as jurisdiction, type of entity and industry. This allows you to make informed choices about each client using the risk-based approach. Our comprehensive workflows incorporate industry-specific guidance such as LSAG for law firms.



The flexibility of Omnitrack lets you choose the default workflow most appropriate to your business. The workflow can be customised to suit your own areas of practice and risk scoring system. Our team will guide you through every step of the process.

- All the stages of client onboarding, including client identification, client verification, integration with PEPs / sanctions checkers, source of wealth and funds checks, risk assessments and ongoing monitoring, are in a centralised location
- You can set a client or matter file to 're-open' after a period of time, depending on the risk level assigned to the client or matter, ensuring that no client or matter is left without periodic review. The time-based automations allow admins in Omnitrack to fully automate the ongoing monitoring process.
- You can complete a risk assessment on a client based on the scores generated from a series of risk-related questions
- When carrying out a client or matter risk assessment you have the ability to review the specific red flags in a dedicated tab (or within the workflow) thereby focusing on those clients and matters that require immediate attention

AML training suite – Relevant training for all staff



VinciWorks strives to make its AML training more than simply a tick-box exercise. VinciWorks' AML training provides users with a thorough overview of money laundering laws and offences and relevant procedures to follow. Users will learn how to spot and what to do about potential red flags, how to report suspicions and penalties for violations. Every user who takes the training will receive tailor-made content specifically designed for their jurisdiction, job role and risk level.

AML audit

Our partners at Compliance Office have the expertise needed to help you conduct an independent, tech-enhanced AML audit, in accordance with the latest Legal Sector Affinity Group (LSAG) guidance. Their team keeps their pulse on the latest AML requirements and your audit will be completed by former practising solicitors with many years of experience in law firm regulation, often former SRA staff.

Contact us

VinciWorks

www.vinciworks.com
enquiries@vinciworks.com
+44 (0) 208 815 9308