CILEx Regulation
Sectoral Risk Assessment
September 2025

Table of Contents

Executive Summary

This Sectoral Risk Assessment (SRA) provides a comprehensive overview of the money laundering, terrorist financing, and proliferation financing risks facing firms regulated and supervised by CILEx Regulation (CRL). It is designed to support CRL's risk-based approach to supervision and guide firms in understanding and mitigating economic crime risks.

Key findings include:

- **Overall Risk Rating:** The supervised sector is assessed as medium risk, driven primarily by weaknesses in financial transaction controls and training/governance frameworks.
- **Low-Risk Areas:** Services offered, client profiles and geographic exposure are generally low risk due to limited conveyancing activity, predominantly individual clients, and UK-based operations.
- **Medium-Risk Areas:** Financial transactions and training practices require improvement, particularly around source of funds checks, AML training logs and ongoing monitoring.
- **Emerging Risks:** Changes in service provision, remote working practices and the potential acceptance of cryptocurrency introduce new vulnerabilities that firms must proactively manage.
- **Regulatory Expectations:** CRL expects all firms, regardless of whether they are in or out of the scope of the Money Laundering Regulations 2017 (MLR 2017), to conduct due diligence, maintain documented risk assessments and implement proportionate AML controls.

This assessment should be used by firms to inform their Practice-Wide Risk Assessment (PWRA), Client/Matter Risk Assessments (CMRA), AML policies, and training programmes. It also serves as a reference for CRL staff and other stakeholders involved in AML supervision and compliance.

Headline Findings

- **Overall Sector Risk Rating: Medium**
    - While several risk categories are assessed as low, weaknesses in financial transaction controls and training/governance elevate the overall risk profile.
- **Low-Risk Areas Identified**
    - Services offered are largely probate and estate administration, with limited conveyancing and Trust & Company Service Provider (TCSP) activity.
    - Client profiles are predominantly individual and UK-based, with minimal exposure to Politically Exposed Persons (PEPs) or Sanctioned individuals.
    - Geographic exposure is low, with rare engagement with high-risk jurisdictions.
- **Medium-Risk Areas Identified**
    - **Financial Transactions:** Inadequate source of funds checks and inconsistent documentation in CMRAs.
    - **Training & Governance:** Gaps in AML training records, insufficient coverage of key topics and lack of ongoing monitoring.
- **Emerging Risks**
    - Remote working and potential use of cryptocurrency introduce new identity and transaction verification challenges.
    - Personnel changes require robust onboarding and continuity in AML oversight roles.
- **Compliance Gaps**
    - Absence or poor quality of documented PWRAs and CMRAs.
    - Misalignment between AML policies and actual practices.
    - Limited use of electronic verification tools and inconsistent SAR procedures.
- **Regulatory Expectations**
    - All firms, including those outside the scope of MLR 2017, are expected to conduct due diligence and maintain documented risk assessments.
    - CRL will continue to review AML documentation and reserves the right to request it at any time.

Introduction

CRL serves as one of the designated Professional Body Supervisors for ensuring compliance with anti-money laundering (AML) legislation. To enhance the effectiveness of its oversight and mitigate the risk of economic crime, CRL must maintain a clear understanding of both current and emerging risks within the regulated community under its supervision.

Purpose

Under Regulation 17 of the MLR 2017, CRL is required, in its capacity as a supervisory authority, to identify and assess both domestic and international risks of money laundering (ML) and terrorist financing (TF) that affect its supervised population.

Money laundering involves concealing the origins of funds obtained through criminal activity, while terrorist financing refers to the collection or provision of funds, whether from lawful or unlawful sources, with the intention or knowledge that they will be used to support terrorist acts.

In addition, CRL monitors the risk of proliferation financing[1] within its supervised population, which is the provision of funds or financial services used to support the development, acquisition, or transfer of weapons of mass destruction and related materials.

The purpose of this SRA is to ensure that these risks are clearly identified and understood, enabling CRL to:

- Direct its supervisory efforts proportionately and effectively to areas of highest risk.
- Provide guidance to the supervised population on how to mitigate and manage these risks.

CRL also monitors the activities of the broader regulated community to determine whether their operations bring them within the scope of the MLR 2017.

This document represents the most recent SRA conducted by CRL.

Intended Audience

The CRL SRA is designed to support a range of stakeholders, each playing a critical role in preventing money laundering and broader economic crime. Its purpose is to inform and guide the following audiences.

CRL Staff

Those involved in regulatory functions, particularly where responsibilities intersect with anti-money laundering (AML) supervision. The assessment supports CRL's risk-based approach to regulation.

CRL Supervised Community

Firms and individuals whose legal service activities bring them within the scope of the MLR 2017. The assessment helps these entities understand sector-specific risks and regulatory expectations.

[1] *The act of providing funds or financial services for use, in whole or in part, in the manufacture, acquisition, development, export, trans-shipment, brokering, transport, transfer, stockpiling of, or otherwise in connection with the possession or use of, chemical, biological, radiological or nuclear weapons(CBRN), including the provision of funds or financial services in connection with the means of delivery of such weapons and other CBRN-related goods and technology, in contravention of the relevant financial sanctions obligation.*

CRL Regulated Community (Outside the Scope of the MLR)

While not directly subject to the MLR 2017, these entities are encouraged to:

- Comply with broader economic crime legislation, including the Proceeds of Crime Act (POCA) 2002, the Terrorism Act (TACT) 2000, and obligations related to proliferation financing
- Avoid inadvertently facilitating economic crime through poor risk management or lack of awareness
- Take time to review the latest UK National Risk Assessment

We recommend that all members of the regulated and supervised communities incorporate this assessment into their annual AML training.

Additionally, supervised firms should refer to this assessment when drafting or updating their Regulation 18 PWRA. Even firms not strictly within the scope of the MLR 2017 are encouraged to conduct a PWRA to:

- Provide context for assessing risk in individual client matters.
- Inform the development of effective AML policies and procedures.

Methodology

CRL has a responsibility to identify and assess the risks, and potential risks, faced by its supervised community. This includes not only those currently under supervision but also those who may fall within scope and require supervision under the MLR 2017.

The supervised community comprises individuals and firms providing services as:

- Tax Advisers, as defined in Regulation 11(d) of the MLR 2017.
- Independent Legal Professionals, as defined in Regulation 12(1) of the MLR 2017.
- TCSPs, as defined in Regulation 12(2) of the MLR 2017.

CRL's risk assessment methodology is designed to:

- Identify current risks faced by supervised firms, based on firm-specific data and sector-wide trends.
- Detect emerging risks that may impact the supervised community in the future.
- Support a proportionate, risk-based approach to supervision and regulatory engagement.

This process draws on a wide range of information sources, including:

- Annual Returns submitted by supervised firms.
- AML Statements submitted by supervised firms.
- Outcomes from inspections and reviews.
- Complaints and intelligence reports.
- The nature of services provided and client profiles.
- Geographic risk factors, including links to high-risk jurisdictions.

- Financial transactions and how client money is handled.
- Governance structures, staffing levels, and AML training records.
- The firm's own PWRA and internal controls.

CRL also monitors external developments, such as updates to the UK's National Risk Assessment, intelligence from law enforcement, and changes in legislation or economic crime trends.

Identifying Risks Currently Faced by Firms

To effectively understand the risks of money laundering, terrorist financing, and proliferation financing within its supervised sector, CRL begins by assessing the specific risks faced by each individual firm.

This assessment is informed by a range of data sources, including:

- **The AML Statement:** completed annually by firms, focusing on money laundering and broader economic crime.
- **The Annual Return:** required from all regulated firms, providing operational and structural insights.
- **Inspections and Reviews:** conducted by CRL to evaluate compliance and identify emerging risks.

When assessing risk, CRL considers a broad set of factors, including but not limited to:

- **Firm history and complaints:** including trading background and any regulatory concerns.
- **Nature of services provided:** recognising that some services carry inherently higher risk.
- **Client profile and interaction:** including client type, geographic location, and how services are delivered.
- **Financial indicators:** such as annual turnover and the volume of client money held.
- **Staffing and training:** including adequacy of resources and AML training programmes.
- **Internal controls:** such as the firm's AML policies, procedures, and its own PWRA.

This multi-source, multi-factor approach enables CRL to apply a proportionate, risk-based supervisory model tailored to the specific vulnerabilities of each firm.

Identifying Emerging and Potential Risks

To stay ahead of new and evolving threats, CRL actively monitors a wide range of intelligence sources to identify risks that could impact its supervised community. This proactive approach ensures that CRL can adapt its supervisory strategy in response to emerging trends in money laundering, terrorist financing, and proliferation financing.

Key sources of information include:

- **The Legal Sector Affinity Group (LSAG)** and its sub-groups, which provide sector-specific insights and collaborative intelligence.
- **The Joint Money Laundering Intelligence Taskforce (JMLIT)** and the **National Economic Crime Centre (NECC)**, which offer cross-sector intelligence and

strategic threat assessments.

- **The UK National Risk Assessment (NRA)**, which outlines national-level threats and vulnerabilities relevant to the legal and professional services sectors.
- **Reports submitted by firms**, including suspicious activity reports (SARs) and other disclosures.
- **Complaints and intelligence received about firms**, which may indicate systemic or emerging risks.

By triangulating these sources, CRL is able to identify patterns, anticipate threats, and refine its risk-based approach to supervision.

Critical Risk Considerations

The 2025 NRA has identified the legal sector as presenting a low risk for terrorist financing but a high risk for money laundering. The services most vulnerable to exploitation by criminals and corrupt elites for money laundering purposes continue to be conveyancing, trust and company service providers (TCSPs), and the misuse of client accounts.

When assessing individual firms, we consider the following key risk factors:

- Services offered
- Client profile
- Geographic location
- Nature of financial transactions
- Training and governance frameworks

These factors are explored in the following sections, which present insights drawn from our risk assessments of supervised firms, as well as broader observations across the wider regulated population.

Services Offered

Firms within our supervised sector typically offer specialist services rather than a broad range of legal activities. Most provide a combination of probate, trust, and estate administration services. While estate administration is considered higher risk due to the potential for managing high-value transactions, this risk can be significantly mitigated through robust checks on the source of funds and thorough due diligence on clients and beneficiaries. Additionally, the requirement that these services relate to the estate of a deceased individual inherently limits opportunities for money laundering.

Only one firm in our supervised population is currently authorised to undertake conveyancing, and this is restricted to transactions directly linked to probate estates. As such, the risk associated with this activity is assessed as lower than for mainstream conveyancing.

Four firms now offer TCSP services. However, none have formed new companies on behalf of clients in recent years, which contributes to a low risk assessment for this activity.

Based on these observations, we have assessed this risk factor for our supervised sector as low.

Client Profiles

Most firms in our supervised sector work exclusively with individual clients, typically through face-to-face interactions. Only one firm engages with corporate clients, primarily assisting local SMEs with business-to-business debt recovery. These clients have straightforward ownership structures, further reducing risk.

Over the past year, no firms in the supervised sector have reported dealings with PEPs or individuals subject to Sanctions. The predominance of in-person client onboarding supports effective identity verification and due diligence.

Across the wider population of CRL-regulated firms, services also tend to focus on individual clients, though there is a notable increase in those working with corporate entities. Where corporate clients are involved, they are generally micro[2] or small companies[3] with established service agreements.

As with the supervised sector, no firms in this broader group reported interactions with PEPs or Sanctioned individuals in the past year.

Based on this information, we have assessed this risk factor for our supervised sector as low.

Geographical Location

This risk factor is closely linked to client risk but focuses on other individuals involved in the matter, such as beneficiaries, and their connections, particularly where there are links to high-risk jurisdictions. This includes payments received from, made to, or otherwise associated with jurisdictions identified as high-risk by the Financial Action Task Force (FATF).

Firms in our supervised sector typically engage with clients either in person or through secure digital face-to-face channels. As a result, the client base is predominantly UK-based.

While there have been a small number of overseas clients, these cases are rare, relating to UK legal matters and have been subject to appropriate identification and due diligence checks.

During the reporting period, no firms reported dealings with individuals from or connected to jurisdictions identified as high-risk by FATF.

Based on this information, we have assessed this risk factor for our supervised sector as low.

Nature of Financial Transactions

As highlighted in the 2025 NRA, the holding of client money continues to present a heightened risk of firms being targeted for money laundering, terrorist financing or proliferation financing. These risks are mitigated in law firms by the requirement under the CILEx Accounts Rules to submit an annual Accountant's Report.

Additionally, before CRL authorises or supervises a firm, it must be satisfied that appropriate controls are in place for managing client money. This includes safeguards around the receipt of payments and the provision of client account details, specifically to whom and when such details are shared.

---

[2] *If it has any 2 of the following: a turnover of £632,000 or less, £316,000 or less on its balance sheet, or 10 employees or less (Companies House)*

[3] *If it has any 2 of the following: a turnover of £10.2 million or less, £5.1 million or less on its balance sheet, or 50 employees or less (Companies House)*

Among supervised firms, 49% do not accept cash payments at all. A further 49% restrict cash payments to amounts under £500, while the remaining 2% cap cash acceptance at £2,000.

These limitations reduce the attractiveness of these firms to criminals seeking to exploit cash-based vulnerabilities, and fall under the newly defined £3,000 Defense Against Money Laundering (DAML) reporting threshold limit which came into effect on 31 July 2025 under The Proceeds of Crime (Money Laundering) (Threshold Amount) (Amendment) Order 2025.

Despite these controls, source of funds checks have been widely identified as insufficient. In many cases, documentation within CMRAs is weak, and firm policies often lack clear definitions of acceptable evidence or verification procedures or omit them entirely. Some firms have incorrectly treated estate-based funds as inherently low risk and have not conducted adequate source of funds verification.

Based on these findings, we have assessed this risk factor for our supervised sector as medium risk.

Training and Governance Frameworks

Regular and consistent training on the key aspects of AML is essential for all staff. This training should include guidance on identifying 'red flags' that trigger Enhanced Due Diligence (EDD) and clearly explain the nature and scope of those higher-level checks.

While some firms maintain AML training records that include all relevant staff, our assessments have identified a widespread need for improvement. Specifically, firms must ensure that formal training logs:

- Are maintained and updated regularly
- Include sufficient detail for auditability
- Clearly outline the content covered, including topics such as proliferation financing
- Reflect periodic AML and broader compliance training, as required under Regulation 24 of the MLR 2017

In addition to training, our analysis has identified three related risks:

- **Ongoing AML Monitoring:** Firms must demonstrate that AML risks are monitored throughout the lifecycle of a matter, not merely at the beginning and/or end. This should be clearly demonstrated in the CMRA.
- **PWRA Coverage:** Firms must ensure their Regulation 18 PWRA includes consideration of proliferation financing. Additionally, firms should assess whether the size and nature of their business necessitate an independent audit function.
- **Verification in Non-Face-to-Face Engagements:** Where clients are not met in person, verification checks must be more robust. CMRA documentation should specify the electronic verification methods used, how they link to the individual, and, where possible, include copies of supporting documents.

Based on these findings, we have assessed this risk factor for our supervised sector as medium risk.

Emerging & Potential Risks Areas

In addition to the risks already identified within our supervised community, firms must remain vigilant to other risks that may emerge as their operations evolve. This includes changes to service offerings, geographic areas of operation, internal procedures, or staffing. Such changes can introduce new vulnerabilities or alter existing risk profiles.

It is essential that any such developments are promptly reassessed and appropriately mitigated. These changes should be clearly documented and reflected in the firm's PWRA, as well as in its formal policies and procedures, ensuring compliance with regulatory expectations and maintaining a robust risk management framework.

Service Provision Changes

Under the Economic Crime and Corporate Transparency Act (ECCTA) 2023, Companies House began offering voluntary identity verification from 8 April 2025. This applies to anyone submitting information to the public register, including those acting on behalf of a company. The initiative aims to enhance transparency and reduce fraud, with mandatory identity verification to be introduced from 18 November 2025.

While this development may reduce the number of firms offering TCSP services, it is possible that CRL may need to supervise firms owned by CILEx members providing TCSP services that are not currently regulated as CRL firms.

These developments highlight the importance of ongoing monitoring and reassessment of sector-wide risks, especially in relation to onboarding controls and client due diligence.

Evolving Operational Practices

The growing prevalence of remote working highlights the importance of firms ensuring that verified identities genuinely correspond to the individuals they are engaging with. The ease with which high-quality fake identity and banking documents can now be produced, particularly with the increasing sophistication of artificial intelligence (AI), represents an emerging risk.

However, this risk is currently considered low within the legal sector, as firms often rely on certified professionals within a prospective client's geographic location to conduct in-person identity verification.

Should CRL-authorised firms begin accepting cryptocurrency payments, they must implement robust procedures to verify the true source of any cryptocurrency assets received. This includes ensuring that appropriate due diligence is carried out to assess the legitimacy and origin of such funds, in line with AML obligations.

Personnel Changes

Although staff turnover remains relatively low, it is essential that firms provide prompt AML induction training to all new employees as part of their onboarding process. This training should not be delayed until the firm's next scheduled training cycle, as doing so could compromise the timely and effective preparation of new staff in meeting AML obligations.

Staff changes must also not disrupt the firm's compliance arrangements. In particular, the responsibilities of the Money Laundering Reporting Officer (MLRO), Deputy MLRO (DMLRO) (where applicable) and the Money Laundering Compliance Officer (MLCO) must be maintained at all times to ensure continuity in oversight and reporting.

Overall Risk Evaluation

CRL has assessed the overall risk of money laundering, terrorist financing and proliferation financing within its supervised community as medium. While several individual risk categories, such as services, clients and location, are rated as low-risk, the presence of medium-risk ratings in Financial Transactions (which highlighted inadequate Source of Funds checks and inconsistent documentation within CMRAs) and Training & Governance (which highlighted gaps in AML Training records, insufficient coverage of key topics and a lack of ongoing monitoring) elevates the overall risk profile.

These areas are critical to maintaining AML compliance and operational integrity, and any weaknesses here can significantly increase exposure to financial crime.

This medium risk rating is not static. By addressing the identified vulnerabilities and continuing to monitor emerging risks, CRL aims to reduce the overall risk level over time. Improvements in internal controls, staff training, and transaction oversight will be key to achieving a future reassessment that reflects a low-risk status.

Guidance for the Supervised / Regulated Community

CRL has identified a range of key risks within the supervised / regulated sector. One of the primary objectives of this risk assessment is to support the supervised community in understanding these risks and taking appropriate steps to mitigate them. This section outlines practical guidance to help ensure compliance and strengthen AML controls across the following critical areas:

- AML Policy Documentation
- Practice-Wide Risk Assessment (PWRA)
- Client / Matter Risk Assessment (CMRA)
- Customer Due Diligence (CDD)
- Source of Funds (SoF) Checks
- PEP & Sanction Checks
- Suspicious Activity Reporting (SAR)
- Training

AML Policy Documentation

The MLR 2017, as amended by the Money Laundering and Terrorist Financing (Amendment) Regulations 2019, form the foundation of the UK's legal framework for preventing money laundering and terrorist financing. These regulations place mandatory requirements on businesses across a range of sectors, including legal practices, to establish and maintain effective anti-money laundering (AML) policies and procedures.

CRL's review of AML Policy documentation submitted by regulated firms revealed several areas of concern:

- **Superficial and Template-Based Policies**: Many policies were found to be overly generic, based on standard templates with minimal customization. In some instances, template prompts were still present, indicating a lack of attention to detail and limited engagement with the content. This approach undermines the effectiveness of AML frameworks and suggests insufficient operational integration.
- **Omission of Proliferation Financing Risk:** A significant number of policies failed to address the risk of proliferation financing, despite its inclusion as a regulatory requirement under the Money Laundering and Terrorist Financing (Amendment) (No. 2) Regulations 2022, effective from 1 September 2022. This amendment introduced a clear obligation for regulated entities to identify, assess, and mitigate the risk of proliferation financing. While firms within the CRL population may be considered lower risk in this area, the requirement to assess, document, and mitigate this risk remains mandatory.
- **Inadequate Source of Funds Procedures:** SoF procedures were frequently missing, vague, or superficial. Many policies did not clearly outline the steps taken to verify the legitimacy of funds or describe how these checks were conducted and documented.
- **Limited Detail on PEP & Sanction Checks:** Although PEP and Sanction checks were referenced in most policies, the level of procedural detail varied significantly. Few firms provided clear guidance on how these checks are conducted, stored, and recorded. Additionally, escalation procedures in the event of a true match were often missing or undefined, posing a risk to compliance and operational integrity.

To support firms in improving the quality of their AML Policy documentation, CRL recommends the following:

1. **Comprehensive and Clearly Articulated:** Policies should be tailored to the nature

and scale of the firm's operations and reflect the specific risks faced.

2. **Aligned with Current Regulatory Expectations:** Documentation must incorporate all relevant regulatory requirements, including those introduced by recent amendments.
3. **Subject to Regular Review and Updates:** Firms should establish a review cadence to ensure policies remain current and responsive to changes in the regulatory landscape and business operations.

Practice-Wide Risk Assessment (PWRA)

Under Regulation 18 of the MLR 2017, all relevant businesses, including law firms, are required to carry out and maintain a written PWRA. This assessment must identify and evaluate the firm's exposure to money laundering, terrorist financing, and, where applicable, proliferation financing risks.

This assessment is not merely a compliance exercise; it is a foundational tool for developing effective AML policies, controls, and procedures. It enables firms to adopt a risk-based approach, ensuring that resources are directed toward areas of greatest vulnerability. The PWRA must be documented, regularly reviewed, and approved by senior management, with updates made to reflect changes in the firm's risk profile or regulatory environment.

While the MLR 2017 formally apply only to firms within the scope of Regulations 11 or 12, CRL encourages all firms under its regulatory oversight to conduct a PWRA. By undertaking this assessment, firms can gain a clearer understanding of their exposure to money laundering, terrorist financing, and proliferation financing risks.

The PWRA should be proportionate to the size and nature of the business and must consider a range of risk factors, including:

- The types of clients the firm serves
- The geographic areas in which it operates
- The nature of services offered
- The characteristics of transactions handled
- The delivery channels used (e.g., face-to-face, online)

The PWRA must also consider information provided by CRL, including the latest NRA, CRL's own SRA, and other CRL-published materials related to economic crime. Upon completion of the PWRA, firms should be able to produce an overall risk rating that identifies areas of elevated risk or potential deficiencies, along with the corresponding mitigation measures implemented.

CRL routinely reviews a firm's PWRA and reserves the right to request it at any time. Firms must therefore ensure that their PWRA is accurate, comprehensive, and regularly updated, with a clearly defined review cycle of no less than once per year.

CRL's review of PWRA documentation submitted by regulated firms revealed several areas of concern:

- **Absence of Documented PWRA**: Several firms failed to provide a documented PWRA, constituting a breach of Regulation 18 of the MLR 2017. In some cases, firms questioned the necessity of the PWRA, reflecting an outdated understanding of current compliance obligations.
- **Insufficient Depth and Coverage:** Where PWRAs were submitted, many lacked

the necessary depth and failed to address key risk areas, such as Sanctions exposure and delivery channels. These omissions suggest a limited grasp of the full scope of risk factors that must be considered under Regulation 18.

- **Lack of Regular Review and Proactive Maintenance:** Several documents appeared to have been updated only in response to CRL's request for submission, with revision dates aligning precisely with the request timeline. This reactive approach indicates that regular review cycles are not being maintained, and that updates are driven by external prompts rather than internal governance.

To support firms in meeting their obligations under Regulation 18 and improving the quality of their PWRAs, CRL recommends the following:

1. **Ensure a Documented PWRA Is in Place**: All firms must maintain a written, PWRA. This is a legal requirement and forms the foundation of a firm's AML framework.
2. **Adopt a Risk-Based Approach**: The PWRA should be tailored to the firm's specific services, client base, geographic exposure and transaction types. It must consider all relevant risk factors, including Sanctions, delivery channels and proliferation financing.
3. **Demonstrate Operational Depth:** The assessment should go beyond generic statements and include detailed analysis of how risks are identified, assessed, and mitigated in practice.
4. **Establish a Review Cadence**: Firms should implement a formal schedule for reviewing and updating the PWRA; at least annually or in response to significant changes in business operations or the regulatory landscape.
5. **Engage Senior Management:** The PWRA must be approved by senior management and integrated into the firm's broader compliance strategy, ensuring accountability and oversight.
6. **Use PWRA to Inform AML Controls:** The findings of the PWRA should directly inform the firm's AML policies, procedures, and training programmes, ensuring alignment between risk assessment and operational controls.

Client / Matter Risk Assessment (CMRA)

Under Regulation 28 of the MLR 2017, firms subject to AML supervision, including legal practices, are required to undertake CDD measures. A key component of this process is the completion of CMRAs, which help firms identify and evaluate the specific risks associated with individual clients and the matters they instruct on.

These assessments must be conducted at the outset of a client relationship and at the earliest opportunity for each new matter. They are essential for determining the appropriate level of due diligence to apply and must consider factors such as:

- The purpose and intended nature of the business relationship or transaction
- The size and frequency of transactions to be deposited by a client
- The client's geographic location and risk profile
- The regularity and duration of the business relationship with a client
- The presence of high-risk indicators (e.g., PEP status, high-risk jurisdictions, complex or unusually large transactions).

Regulation 28 also requires firms to identify and verify the identity of customers and

beneficial owners, and to understand the ownership and control structure of legal entities where applicable.

Regulation 33 requires that EDD checks should be conducted where a client / matter has been assessed as being at a higher risk of money laundering, terrorist financing or proliferation financing, and these additional checks undertaken must be captured in the CMRA.

The outcome of the CMRA should directly inform whether CDD or EDD is required.

Firms must ensure that CMRAs are clearly documented, tailored to the specific risks identified, and aligned with the firm's PWRA. CMRAs should demonstrate how risks are mitigated and must be updated throughout the lifecycle of the matter to reflect any changes in circumstances, services, or client behaviour. CRL recognises that some legal matters may take longer to conclude, making ongoing review and documentation essential for maintaining compliance.

Even in cases where a matter is assessed as low risk, the documentation should reflect a level of detail consistent with medium or high-risk classifications. This ensures that the rationale for the risk rating is clearly recorded and demonstrates that appropriate checks have been carried out.

CRL's review of CMRA documentation submitted by regulated firms revealed several areas of concern:

- **Lack of Detail and Depth:** Many CMRAs relied on Yes/No responses without supporting commentary or rationale. Risk factors such as PEP status, Sanctions exposure and source of funds were often mentioned, but not substantiated with evidence or verification steps.
- **Inconsistent Formatting and Documentation:** CMRAs varied significantly in structure and completeness. Some firms submitted file notes instead of formal risk assessments, while others had blank or templated responses.
- **Missing or Superficial Source of Funds Checks:** SoF was frequently mentioned in policy but not reflected in CMRA documentation. Verification methods were unclear or absent, with some firms relying solely on client explanations.
- **Limited Evidence of PEP and Sanction Screening:** Although policies referenced PEP and Sanctions checks, CMRAs rarely documented outcomes or escalation procedures. Use of third-party screening tools was inconsistent and often not evidenced.

To support firms in meeting their obligations under Regulation 28 and improving the quality of their CMRAs, CRL recommends the following:

1. **Enhance Operational Detail:** Firms must move beyond tick-box assessments by including details on actions taken, by whom and when, commentary on risk decisions, demonstrate that the necessary risk factors have been considered, sufficient documentation of all checks performed, including an overall risk score, and evidence of escalation or mitigation actions.
2. **Integrate CMRAs with AML Policy and PWRA:** Firms must ensure CMRA content aligns with PWRA and AML policies.
3. **Implement Review Cadence:** Firms must establish a formal schedule for CMRA reviews covering the inception of the matter, at key milestones (e.g. receipt of funds or change in client profile) and at the conclusion of the matter.
4. **Train Staff on CMRA Completion:** Firms must provide targeted training on identifying and assessing risk factors, documenting verification steps and using any

established screening tools effectively.

5. **Audit and Quality Control:** Firms must introduce or strengthen internal audit controls to ensure CMRA quality and consistency, as well as using feedback loops to improve staff understanding.

Customer Due Diligence (CDD)

Regulation 27 of the MLR 2017 states that relevant persons are legally required to apply Customer Due Diligence (CDD) measures in specific circumstances. These include:

- **Establishing a business relationship:** CDD must be conducted at the outset of any ongoing relationship with a client, including verifying identity and understanding the nature and purpose of the relationship.
- **Conducting occasional transactions:** CDD is required for one-off transactions involving the transfer of funds exceeding €1,000 (or equivalent), and for other occasional transactions exceeding €15,000, depending on the business type.
- **Suspicion of money laundering or terrorist financing:** If there is any suspicion of criminal activity, CDD must be applied regardless of transaction value or client history.
- **Doubts about previously obtained information**: If the adequacy or accuracy of previously collected identification or verification data is in question, firms must reapply CDD measures.

Regulation 28 of the MLR 2017 sets out the requirements for CDD at the outset of a business relationship and on an ongoing basis, requiring firms to:

- Verify the identity of the client using reliable, independent sources (e.g. passport, utility bills)
- Identify and verify any beneficial owners
- Understand the ownership and control structure of legal entities
- Assess the purpose and intended nature of the business relationship or transaction

The MLR 2017 applies a risk-based approach to the application of CDD:

- Regulation 33 requires EDD in certain circumstances where there is a higher risk of money laundering, terrorist financing or proliferation financing
- Regulation 31 requires that, where there has been a failure to complete adequate CDD, to not proceed with the business relationship or transaction, and must terminate any existing client business relationships.

CRL recognises that some regulated firms fall outside the scope of the MLR 2017, as they do not provide transactional services, tax advice, or trust and company services.

However, CRL expects all firms to carry out CDD, as services such as litigation and immigration can still facilitate economic crime. These checks also support conflict of interest assessments and help identify PEPs or Sanctioned individuals. Firms must retain records of CDD for all matters, documented either in a standalone CMRA or within the client file in their case management system.

CRL's review of CDD practices outlined within firms submitted documentation revealed several areas of concern:

- **Inconsistent Identity Verification (IDV) Practices:** While most firms referenced ID checks in their AML policies, CMRAs often lacked evidence of how identity was

verified. Some firms relied solely on face-to-face checks without documenting accepted forms of ID or verification steps.

- **Limited Use of Electronic Verification Tools:** A few firms mentioned tools like Amiqus or Lexis Nexis, but usage was inconsistent and not always reflected in CMRAs. Many firms still rely on manual ID checks, which may be less robust and harder to audit.
- **Superficial SoF Checks:** SoF was frequently mentioned in policy documents but not evidenced in practice. CMRAs often lacked documentation of how SoF was verified, with some firms relying on verbal explanations or listing "Bank" without detail.
- **Lack of Ongoing Monitoring:** Few firms demonstrated procedures for ongoing CDD, such as monitoring client relationships or updating risk assessments during the matter lifecycle.
- **Contradictions Between Policy and Practice:** Several firms showed discrepancies between their AML policies and actual CDD practices, particularly around cash handling, IDV and SoF verification.

To support firms in meeting their obligations under Regulation 27 and improving the quality of their CDD practices, CRL recommends the following:

1. **Strengthen Identity Verification Procedures:** Clearly define accepted ID documents and verification steps, whilst also ensuring CMRAs record the type of ID used, how it was verified and where it is stored.
2. **Adopt and Integrate Electronic Verification Tools:** Use reliable electronic IDV platforms[4] to enhance accuracy and auditability, whilst also ensuring tools are referenced in both policy and CMRA documentation. Such tools carry the added benefit of automating checks for PEP & Sanctioned individuals.
3. **Formalise SoF Checks:** Develop a standard process for SoF checks, including documentary evidence (e.g. bank statements, inheritance documents), implement risk-based thresholds for enhanced checks and clearly record verification outcomes in CMRAs.
4. **Implement Ongoing CDD Procedures:** Introduce procedures for periodic review of client relationships and transactions, ensuring that the CMRA is updated at key stages to evidence this (e.g. receipt of funds or change in client profile).
5. **Ensure Alignment Between Policy and Practice:** Regularly audit CDD practices to ensure they reflect the firms AML Policy and address any contradictions such as cash handling limits or IDV methods whilst updating documentation accordingly.
6. **Train Staff on CDD Execution:** Provide targeted training on conducting and documenting IDV, including SoF verification, the use of any established electronic tools and recognizing red flags and escalation procedures.

Source of Funds (SoF) Checks

Under the UK's anti-money laundering (AML) framework, verifying the SoF is a critical component of CDD, designed to prevent the handling of criminal property.

The Proceeds of Crime Act 2002 (POCA) makes it a criminal offence to acquire, use,

[4] *Examples of IDV platforms are Amquis (https://amquis.co), LexisNexis IDU (https://risk.lexisnexis.co.uk/products/idu), Compliance Assist (https://complianceassist.co.uk), and Veriff (https://www.veriff.com)*

possess, or transfer criminal property (Sections 327[5] and 329[6]), placing a legal obligation on firms to ensure that client funds are legitimate. Under POCA, criminal property is broadly defined to include money, all types of property, whether real, personal, heritable, or moveable, as well as intangible assets such as things in action and other incorporeal property.

The MLR 2017, particularly Regulations 28, 31, and 33, reinforce this by requiring firms to scrutinise the origin of funds during CDD, especially when establishing a business relationship, conducting high-value or complex transactions, or dealing with high-risk clients such as PEPs or individuals from jurisdictions identified as high-risk by FATF.

All firms must apply a risk-based approach, ensuring SoF checks are proportionate, documented and supported by reliable evidence such as bank statements property sale completion statements, or inheritance documents such as a Grant of Probate.

Failure to verify SoF not only undermines AML compliance but may also expose firms to criminal liability under POCA.

CRL's review of SoF practices as set out in documentation submitted by firms revealed several areas of concern:

- **Limited or Incomplete SoF Procedures:** Many firms mention SoF in their AML policies but fail to provide clear procedures or evidence of checks in practice. In several cases, SoF was marked as "N/A" or described vaguely (e.g. "Bank"), without supporting documentation or rationale.
- **Inconsistent Documentation in CMRAs:** CMRAs often lack detail on how SoF is verified, what documents are reviewed and whether the checks are risk-based. Some firms rely on client explanations without requiring documentary evidence, which is insufficient under current regulatory expectations.
- **Policy-Practice Misalignment:** Firms frequently reference SoF checks in policy documents, but these are not reflected in actual client files or risk assessments. In some cases, AML policies allow for verbal confirmation or account checks, but CMRAs show no evidence of these being performed.
- **Reactive Updates and Gaps in Review:** Several firms updated their AML policies or SoF procedures only in response to CRL requests, rather than as part of a proactive compliance strategy. SoF checks were often omitted for lower-risk services (e.g. simple wills), despite regulatory requirements to assess all matters.

To support firms in meeting their obligations under current regulations to conduct sufficient SoF checks, CRL recommends the following:

1. **Establish Clear and Documented SoF Protocols:** Define what constitutes acceptable evidence (e.g. bank statements, inheritance documents, sale agreements) and include step-by-step guidance on how SoF should be verified and recorded.
2. **Integrate SoF Checks into CMRAs:** Ensure every CMRA includes a section for SoF verification, including type of evidence reviewed, the method of verification, risk-based rationale and the outcome (and escalation, if applicable).
3. **Apply SoF Checks to All Matters:** Avoid blanket exclusions (e.g. "N/A for simple wills") unless justified and documented, and even in low-risk matters, ensure a basic SoF assessment is executed to ensure compliance.
4. **Align Policy with Practice:** Review AML policies to ensure they reflect actual procedures and conduct internal audits to verify that SoF checks are being

[5] *It is an offence for a person to, conceal, disguise, convert, transfer criminal property or to remove criminal property from the UK.*
[6] *It is an offence for a person to acquire, use or possess criminal property.*

performed consistently across client files.

5. **Train Staff on SoF Verification:** Provide targeted training on the identification of red flags, conducting and documenting SoF checks and escalating any concerns appropriately.
6. **Implement Review Cadence:** Regularly review and update SoF procedures to reflect changes in regulation, risk exposure, and service offerings.

PEP and Sanction Checks

Under the MLR 2017, requirements for PEPs and Sanctions checks are primarily addressed through Regulation 33, which mandates the application of EDD in high-risk scenarios, including when a client is identified as a PEP or is connected to a high-risk third country.

Additionally, Regulation 35 provides a detailed definition of PEPs and outlines the specific obligations firms must meet when entering or continuing a business relationship with a PEP, their family members, or known close associates. These obligations include obtaining senior management approval, establishing the source of wealth and funds and conducting enhanced ongoing monitoring.

Together, these regulations ensure that firms apply a risk-sensitive approach to identifying and mitigating exposure to money laundering and terrorist financing risks associated with politically exposed or Sanctioned individuals.

CRL's review of PEP and Sanction checking practices outlined within firms submitted documentation revealed several areas of concern:

- **Lack of Documented Procedures**: Many firms referenced PEP and Sanctions checks in their AML policies but did not provide clear procedures on how these checks are conducted, recorded or escalated. Several firms' policies lacked detail on screening tools used, frequency of checks or handling of true matches.
- **Reliance on Manual or Unverified Screening:** Some firms relied on manual checks or basic tools (e.g. OFSI lists) without integration into case management systems. Where third-party tools were used (e.g. Lexis Nexis, InfoTrack), their application was not consistently documented.
- **Policy-Practice Misalignment:** Discrepancies were noted between AML policies and actual practices. For example, policies stated that Sanctions checks were mandatory, but firms admitted they were not performed.
- **Limited Escalation and Reporting Protocols:** Few firms had defined escalation paths for handling true matches or suspicious results. It was also observed that registration with the NCA SAR Portal was inconsistent, and no firms reported SARs related to PEP or Sanctions issues.

To support firms in meeting their obligations under current regulations to conduct sufficient SoF checks, CRL recommends the following:

1. **Develop Clear, Written Procedures:** Define how PEP and Sanctions checks are conducted, including screening tools used, timing (e.g. at onboarding, periodically), documentation and storage and escalation protocols for true matches.
2. **Integrate Checks into CMRAs:** Ensure every CMRA includes confirmation of PEP/Sanction screening as well as the outcomes, and risk-based commentary including any actions taken.
3. **Use Reliable Screening Tools:** Employ reputable third-party tools with up-to-date data sources, as well as integrating screening into case management systems for

consistency and auditability.

4. **Align Policy with Practice:** Review AML policies to ensure they reflect actual procedures, and address contradictions, ensuring staff understand and follow documented protocols.
5. **Train Staff on Screening and Escalation:** Provide training on the identification of PEPs and Sanctioned individuals, the effective use of screening tools and the escalation and appropriate reporting of matches.
6. **Ensure SAR Portal Registration:** All firms must be registered with the NCA SAR Portal and understand their obligations to report suspicious activity, including PEP/Sanctions-related concerns.

Suspicious Activity Reporting (SAR)

In the UK, the obligation to submit Suspicious Activity Reports (SARs) is primarily governed by Part 7 of the Proceeds of Crime Act 2002 (POCA), which criminalises the failure to report knowledge or suspicion of money laundering under Sections 327 to 330.

Complementing this, the MLR 2017, specifically Regulation 17, require regulated firms to establish systems and controls to identify and report suspicious activity.

While POCA defines the offences and reporting duties, the MLR 2017 sets out the operational framework for firms to implement preventative measures. Failure to submit a SAR when suspicion arises is a criminal offence under POCA, making robust internal reporting procedures and staff training essential for compliance.

CRL's review of SAR practices outlined within firms submitted documentation revealed several areas of concern:

- **Lack of Registration with the NCA SAR Portal:** A significant number of firms, both regulated and unregulated, were not registered with the National Crime Agency's SAR Online Portal, despite being strongly recommended to do so. This includes firms that handle client money and are within scope of MLR 2017.
- **Zero SAR Submissions:** Across all firms, no SARs were submitted during the reporting period. While this may reflect low-risk activity and the small size of the supervised population, it also raises concerns about the awareness of reporting obligations and the ability to identify suspicious activity within these firms.
- **Absence of Documented SAR Procedures:** Many AML policies referenced SARs but lacked detail on how suspicious activity is identified, who is responsible for reporting, any defined internal escalation procedures, and record keeping and audit trails.
- **Training Gaps:** Several firms did not provide evidence of Regulation 24-compliant AML training, including SAR awareness topics. As such, staff within these firms may not be adequately trained to recognise or respond to suspicious activity indicators.

To support firms in meeting their obligations under current regulations to conduct sufficient SoF checks, CRL recommends the following:

1. **Register with the NCA SAR Portal:** All firms within scope must ensure their Nominated Officer is registered and able to submit SARs. Registration should be verified and clearly documented in terms of roles and responsibilities for reporting.
2. **Develop Clear SAR Procedures:** AML Policies should include criteria for identifying suspicious activity, roles, and responsibilities (e.g. MLRO), escalation and reporting steps, and confidentiality and protection protocols.

3. **Train Staff on SAR Awareness:** Provide regular training on recognizing red flags, internal reporting channels, legal obligations and protections, and the use of the NCA SAR Portal.
4. **Maintain SAR Logs and Audit Trails:** Even if no SARs are submitted externally, firms should maintain a log of internal assessments, including decisions and rationale to explain why a SAR has not been submitted. This supports transparency and regulatory oversight.
5. **Integrate SARs into Risk Assessments:** SAR-related risk should be reflected in the PWRA and CMRA documents held by the firm.

Training

UK Regulatory Requirements

Regulation 24 of the MLR 2017 requires all employees who may contribute to the identification or mitigation of money laundering, terrorist financing or proliferation financing risks receive regular and documented training.

This training must cover the legal framework, risk indicators and procedures for handling suspicious activity, and should be tailored to the employee's role. Training must also respond to key changes within the firm, including updates to the PWRA, changes in services offered and associated risk indicators, legislative or regulatory developments and shifts in staffing or roles. Firms are required to maintain written records of all training delivered, including the dates, content and participants to demonstrate ongoing compliance with Regulation 24 of the MLR 2017.

The requirement applies broadly to relevant staff, not just those directly involved in financial transactions, and extends to sole practitioners, who must ensure they remain up to date with AML obligations despite not employing others.

All regulated firms must ensure their training programs comprehensively address legal and regulatory obligations, including those under the Proceeds of Crime Act (POCA) 2002 and the Terrorism Act (TACT) 2000. Effective training not only supports compliance but also helps prevent firms and their staff from inadvertently facilitating wider economic crime.

CRL Regulatory Requirements

CILEX members and CILEX-authorised Practitioners must also comply with the CILEx Regulation CPD Regulations 2021, which require them to maintain, improve, and extend the skills necessary for the proper performance of their professional and legal duties.

CPD activities must cover areas such as compliance, legal knowledge and professional standards, and should be tailored to the individual's membership grade. These obligations support broader regulatory requirements, including AML and data protection training under the MLR 2017.

Additionally, the CILEx Code of Conduct mandates that practitioners maintain up-to-date legal knowledge (Principle 5.1) and address any training deficiencies (Principle 5.2). Failure to meet CPD requirements may constitute misconduct under the Code.

CRL routinely reviews a firm's training log during inspection visits and reserves the right to request it at any time as part of a desk-based review. Firms must therefore ensure their training records are accurate, complete and kept up to date at all times.

CRL's review of Training practices outlined within firms submitted documentation revealed several areas of concern:

- **Lack of Formal Training Logs:** Several firms did not maintain a Regulation 24-

compliant training log, making it difficult to verify who was trained, when and on what content. In some cases, training was confirmed informally but not evidenced through documentation.

- **Outdated or Incomplete Training Records:** Some firms provided training logs with entries dating back to 2022 or 2023, with no recent updates despite policy requirements for annual training. Training records often lacked detail on course content, providers or relevance to AML obligations.
- **Training Gaps Among Key Staff:** MLROs, MLCOs and other senior staff were found to have incomplete or missing training histories, raising concerns about leadership-level compliance awareness.
- **Limited Coverage of Key Risk Areas:** Training content often lacked depth on Proliferation Financing, SAR procedures and sanctions screening, despite these being critical areas under MLR 2017.

To support firms in meeting their obligations under current regulations to conduct adequate training, CRL recommends the following:

1. **Maintain a Formal Training Log:** Ensure a structured and up-to-date log is kept, detailing staff names and roles, dates of training undertaken, topics covered, course materials evidencing the scope of training, training provider, method of delivery and, where applicable, copies of certificates confirming successful completion. This log should be readily available for inspection or submission during desk-based review requests.
2. **Ensure Annual and Role-Specific Training:** Training should be conducted annually and tailored to staff responsibilities. MLROs and MLCOs should receive **enhanced training** on reporting obligations and risk management.
3. **Cover All Relevant AML Topics**: Training must include money laundering and terrorist financing risks, proliferation financing, SAR reporting procedures, PEP & Sanction screening and data protection, as it relates to AML.
4. **Embed Training into Compliance Culture:** Move beyond reactive updates by integrating training into the firm's compliance calendar. Use training outcomes to inform updates to AML policies and procedures.
5. **Monitor and Review Training Effectiveness:** Conduct periodic reviews to assess whether training is improving staff awareness and operational compliance. Use feedback and audit findings to refine future training.

Conclusion

This SRA highlights the evolving landscape of economic crime risks within CRL's supervised and regulated community. The overall risk rating remains medium, reflecting a combination of strong performance in certain areas and persistent vulnerabilities in others.

Firms have demonstrated low exposure in terms of client profiles, geographic reach and service types. Weaknesses in financial transaction oversight, training practices and documentation standards, particularly around source of funds checks and risk assessments, require urgent attention.

CRL expects all firms, whether or not they are subject to AML supervision, to adopt a proactive and proportionate approach to risk management. This includes maintaining accurate and up-to-date AML policies, conducting thorough Practice-Wide and Client/Matter Risk Assessments, and ensuring staff are adequately trained and equipped to identify and respond to red flags.

As the sector continues to evolve, through changes in service offerings, technology adoption and regulatory developments, firms must remain agile and vigilant. CRL will continue to monitor these changes and provide guidance to support compliance and reduce exposure to economic crime.

By addressing the findings in this assessment and embedding a culture of continuous improvement, firms can strengthen their resilience and contribute to the integrity of the legal sector.

Glossary of Terms

Term	Definition
AML (Anti-Money Laundering)	Measures and regulations designed to prevent the processing of criminal proceeds through legitimate financial systems.
CDD (Customer Due Diligence)	The process of verifying the identity of clients and assessing the risks associated with a business relationship or transaction.
CMRA (Client/Matter Risk Assessment)	A documented assessment of the risks associated with a specific client and legal matter, used to determine the level of due diligence required.
CRL (CILEx Regulation Limited)	The regulatory body responsible for overseeing legal professionals and firms, including AML supervision.
DAML (Defense Against Money Laundering)	A report submitted to the UK's National Crime Agency (NCA) seeking consent to proceed with a transaction suspected of involving criminal property.
EDD (Enhanced Due Diligence)	Additional checks required when a client or transaction is considered high risk, such as when dealing with PEPs or high-risk jurisdictions.
FATF (Financial Action Task Force)	An international body that sets standards and promotes effective implementation of measures to combat money laundering and terrorist financing.
IDV (Identity Verification)	The process of confirming a client's identity using reliable and independent documentation or electronic tools.
ML (Money Laundering)	The process of concealing the origins of money obtained through criminal activity.
MLCO (Money Laundering Compliance Officer)	The individual responsible for ensuring a firm's compliance with AML regulations.
MLRO (Money Laundering Reporting Officer)	The designated person within a firm responsible for receiving internal reports of suspicious activity and submitting SARs to the NCA.
MLR 2017 (Money Laundering Regulations 2017)	The UK's primary legislation governing AML obligations for regulated sectors.
NRA (National Risk Assessment)	A government-issued report assessing the risks of money laundering and terrorist financing across sectors in the UK.
PEP (Politically Exposed Person)	An individual who holds or has held a prominent public position, as well as their family members and close associates, requiring enhanced scrutiny.
POCA (Proceeds of Crime Act 2002)	UK legislation that criminalises the handling of criminal property and sets out obligations for reporting suspicious activity.
PWRA (Practice-Wide Risk Assessment)	A firm-level assessment of AML risks across its operations, required under Regulation 18 of MLR 2017.
SAR (Suspicious Activity Report)	A report submitted to the NCA when a firm suspects that a transaction may involve criminal property or terrorist financing.
SoF / SoW (Source of Funds / Source of Wealth)	The origin of the money used in a transaction, which must be verified to ensure it is not derived from criminal activity. On occasion, this will also extend to wider SoW checks.
TCSP (Trust or Company Service Provider)	A firm or individual offering services such as forming companies, acting as directors, or managing trusts, often considered high risk for AML.