

CILEx Regulation

Sectoral Risk Assessment

September 2026

Executive Summary	2
Headline Findings	3
Introduction	5
Purpose	5
Intended Audience.....	6
CRL Staff	6
CRL Supervised Community.....	6
CRL Regulated Community (Outside Scope).....	6
Methodology.....	6
Identifying Risks Currently Faced by Firms	8
Identifying Emerging and Potential Risks	8
Critical Risk Considerations	9
Services Offered.....	9
Client Profiles	10
Geographical Location.....	10
Nature of Financial Transactions	11
Training and Governance Frameworks.....	11
Emerging & Potential Risk Areas.....	12
Service Provision Changes.....	12
Technology, AI & Cyber-Enabled Crime	13
Financial Sanctions & International Risk.....	13
Personnel Changes	13
Overall Risk Evaluation	14
Guidance for Firms	15
AML Policy Documentation.....	15
Practice-Wide Risk Assessment (PWRA).....	16
Client / Matter Risk Assessment (CMRA).....	18
Customer Due Diligence (CDD).....	20
Source of Funds (SoF) Checks	21
PEP and Sanction Checks.....	23
Suspicious Activity Reporting (SAR).....	24
Training.....	25
UK Regulatory Requirements	25
CRL Regulatory Requirements.....	26
Conclusion	28
Glossary of Terms	30

Executive Summary

This Sectoral Risk Assessment (SRA) provides an overview of the money laundering, terrorist financing and proliferation financing risks affecting firms regulated and supervised by CILEx Regulation (CRL). It supports CRL's risk-based approach to supervision and is intended to help firms understand, assess and mitigate financial crime risks within their own practices.

Whilst the UK legal sector continues to be assessed nationally as presenting a Medium level of money laundering, terrorist financing and proliferation financing risk, CRL has assessed the overall risk within its supervised population as Low. This reflects both the characteristics of the supervised sector and the continued improvement in AML compliance standards observed through supervisory activity.

The firms supervised by CRL are predominantly engaged in probate, estate administration, wills, family law, litigation and advocacy services, with limited exposure to higher-risk activities such as conveyancing, Trust and Company Service Provider (TCSP) services, complex corporate structures and high-risk jurisdictions. Most firms also act primarily for UK-based individual clients.

Supervisory reviews identified significant improvements in AML governance arrangements, customer due diligence processes, sanctions compliance frameworks and the quality of Practice-Wide Risk Assessments (PWRAs). However, a number of residual risks remain. In particular, firms should continue to strengthen the quality and evidencing of Source of Funds and, where appropriate, Source of Wealth enquiries, maintain comprehensive AML training records, improve the quality of Client and Matter Risk Assessments (CMRAs), and ensure that sanctions screening, PEP assessments and ongoing monitoring activities are supported by clear audit trails. Supervisory findings generally relate to the quality and consistency of existing controls rather than the absence of controls.

The threat landscape continues to evolve, and firms must remain alert to emerging risks including artificial intelligence-enabled fraud, deepfake technology, cyber-enabled financial crime, sanctions evasion and cryptoasset-related activity. Although these risks are not currently driving the sector's overall risk rating, firms should ensure they are appropriately considered within risk assessments, policies, procedures and training programmes.

This assessment should be used to inform firms' Practice-Wide Risk Assessments (PWRAs), Client and Matter Risk Assessments (CMRAs), AML policies, customer due diligence procedures, sanctions controls, training programmes and wider financial crime frameworks. This assessment also reflects the evolving AML supervisory landscape and should assist firms in preparing for future regulatory developments, including the proposed transition of AML supervisory responsibilities to the FCA. It also serves as a reference point for CRL staff and other stakeholders involved in AML supervision and compliance.

Headline Findings

- **Overall Sector Risk Rating: Low**
 - The overall sector risk rating has reduced from Medium to Low, reflecting significant improvements in AML governance, customer due diligence, sanctions compliance, Practice-Wide Risk Assessments (PWRAs) and wider compliance maturity across the supervised population.
 - Although residual risks remain, supervisory reviews indicate that most findings now relate to the quality and evidence of existing controls rather than the absence of AML controls.
- **Low-Risk Areas Identified**
 - Services offered remain predominantly probate, estate administration, wills, family law, litigation and advocacy services, with limited exposure to higher-risk legal services such as conveyancing and Trust and Company Service Provider (TCSP) work.
 - Client profiles remain predominantly UK-based individuals, with limited exposure to complex corporate structures, Politically Exposed Persons (PEPs) or sanctioned individuals.
 - Geographic exposure remains low, with very limited overseas activity and no reported exposure to FATF high-risk jurisdictions.
- **Residual Risk Areas Identified**
 - **Source of Funds and Source of Wealth:** Supervisory activity identified inconsistency in the scope, evidencing and recording of Source of Funds enquiries, particularly where firms rely primarily on legal fee checks or do not adequately evidence enquiries undertaken.
 - **Training and Competency Records:** Whilst AML training is generally being undertaken, firms do not always maintain sufficient records evidencing training completion, content, competency assessment and compliance with Regulation 24 requirements.
 - **Risk Assessment Quality:** Variability remains in the quality of PWRAs and Client and Matter Risk Assessments (CMRAs), particularly regarding residual risk analysis, narrative justification and ongoing monitoring records.
 - **PEP and Sanctions Audit Trails:** Firms should continue strengthening evidential records relating to screening activity, escalation decisions and ongoing monitoring arrangements.
- **Emerging Risks**
 - Artificial Intelligence (AI), deep-fake technology and increasingly sophisticated fraud techniques present emerging risks for client onboarding, identity verification and source of funds verification processes.
 - Cyber-enabled fraud and sanctions evasion activity continue to develop as emerging threats relevant to all regulated sectors.
 - Personnel changes within firms continue to create governance risks where AML responsibilities, training and succession arrangements are not adequately maintained.
 - Regulatory reform and the planned transition of AML supervision to the FCA may create uncertainty for firms and should be considered within

governance, training and compliance planning.

- **Areas of Good Practice**

- Widespread adoption of electronic identity verification and sanctions screening solutions.
- Stronger AML governance arrangements, with appropriately designated MLRO and MLCO functions across most firms.
- Improved sanctions compliance frameworks and integration of screening processes into operational systems.
- Improved quality and maintenance of AML policies and Practice-Wide Risk Assessments.

- **Regulatory Expectations**

- All firms, regardless of whether they fall within the scope of [MLR 2017](#), should adopt a risk-based approach to money laundering, terrorist financing and proliferation financing risks.
- Firms should maintain documented risk assessments, effective customer due diligence procedures, proportionate AML controls and adequate training records.
- CRL will continue to review AML documentation, undertake desk-based supervisory reviews and conduct risk-based onsite inspections where appropriate.

Introduction

CRL serves as one of the designated Professional Body Supervisors responsible for overseeing compliance with anti-money laundering (AML), counter-terrorist financing (CTF) and proliferation financing obligations. To support a proportionate and risk-based approach to supervision, CRL maintains an ongoing assessment of current, emerging and evolving risks affecting the regulated and supervised communities under its oversight.

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 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.

This assessment has also been informed by findings from CRL's supervisory activities, including AML Statement reviews, onsite inspections, thematic analysis and intelligence obtained through engagement with other supervisory bodies, law enforcement agencies and government publications, including the UK National Risk Assessment.

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

- Direct supervisory resources proportionately and effectively towards areas presenting the greatest money laundering, terrorist financing and proliferation financing risk.
- Inform risk-based supervision, thematic reviews and onsite inspection activity.
- Provide guidance to the regulated and supervised populations on identifying, mitigating and managing financial crime risks.
- Support firms when developing, reviewing and maintaining their AML frameworks, including Practice-Wide Risk Assessments, Client and Matter Risk Assessments and AML policies.

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

In Autumn 2025, HM Government announced its intention to transfer anti-money laundering supervision of the legal and accountancy sectors from Professional Body Supervisors (PBSs) to the Financial Conduct Authority (FCA). As the proposed transition develops, CRL will continue to exercise its supervisory responsibilities and maintain its risk-based approach to AML supervision. CRL will also work collaboratively with HM Treasury, the FCA, OPBAS, professional bodies and the supervised community to support an orderly and effective transition. Firms should remain aware that periods of regulatory change can create uncertainty and operational challenges and should therefore continue to maintain effective AML controls and compliance arrangements throughout the transition period.

This document represents CRL's most recent assessment of the money laundering, terrorist financing and proliferation financing risks affecting its regulated and supervised communities and should be read alongside the latest National Risk Assessment, AML Supervision Report and other relevant CRL guidance.

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 money laundering, terrorist financing and proliferation financing risks, together with CRL's supervisory expectations.

CRL Regulated Community (Outside Scope)

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](#)
- Consider emerging risks identified within the National Risk Assessment, including cyber-enabled fraud, sanctions evasion, artificial intelligence and cryptoasset-related activity.

CRL recommends that all members of the regulated and supervised communities incorporate the findings of this assessment into their annual AML, counter-terrorist financing, proliferation financing and financial sanctions training programmes.

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.
- Consider emerging risks relevant to the firm's business model, including cyber-enabled crime, sanctions evasion, artificial intelligence, remote onboarding and cryptoasset-related activity.

Methodology

CRL has a responsibility to identify, assess, understand and mitigate the risks of money laundering, terrorist financing and proliferation financing affecting its regulated and supervised communities. This includes both firms currently subject to AML supervision and

those whose activities may bring them within the scope of the [MLR 2017](#). CRL's approach is informed by supervisory intelligence, AML Statement reviews, onsite inspections, thematic analysis and external intelligence sources.

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](#).
- Trust or Company Service Providers (TCSPs), as defined in [Regulation 12\(2\) of the MLR 2017](#).

CRL's risk assessment methodology supports a proportionate, intelligence-led and risk-based approach to supervision. It is designed to:

- Identify current risks and vulnerabilities present within supervised firms.
- Assess the effectiveness of controls and mitigations implemented by firms.
- Identify emerging and evolving threats which may increase sectoral risk exposure.
- Inform supervisory priorities, inspections, guidance and regulatory engagement.
- Support the allocation of supervisory resources to higher-risk firms, services and activities.
- Support sectoral risk assessment reviews and the identification of emerging financial crime trends.

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.
- Thematic reviews and supervisory trend analysis.
- Information shared through the AML Supervisors Forum (AMLSF), Legal Sector Affinity Group (LSAG), OPBAS and relevant law enforcement agencies.
- National Risk Assessment findings and wider economic crime intelligence.
- 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, including updates to the [UK's National Risk Assessment](#), intelligence from law enforcement and supervisory authorities, sanctions developments, legislative reform, emerging technologies and wider economic crime trends. This ensures that supervisory activity remains responsive to evolving threats and vulnerabilities.

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.
- **Onsite Inspections:** Risk-based inspections used to assess the effectiveness of AML controls in practice and validate information provided through AML Statements and supervisory reviews.

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.
- **Source of Funds and Source of Wealth controls:** Including how firms obtain, verify and evidence information regarding the origin of funds and assets.
- **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.
- **Sanctions and Screening Arrangements:** Including sanctions compliance, PEP screening, audit trails and ongoing monitoring processes.

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 identify new and evolving risks, CRL maintains an ongoing programme of intelligence gathering, supervisory engagement and environmental scanning. This ensures that emerging money laundering, terrorist financing, proliferation financing and wider economic crime threats are identified and incorporated into supervisory planning and future updates to this Sectoral Risk Assessment.

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.

- **AML Supervisors Forum (AMLSF)** and other professional body supervisory networks.
- **Office for Professional Body Anti-Money Laundering Supervision (OPBAS).**
- **Office of Financial Sanctions Implementation (OFSI)** publications and engagement activity.
- **National Crime Agency (NCA)** threat assessments and strategic intelligence reports.
- **The UK National Risk Assessment (NRA)**, which outlines national-level threats and vulnerabilities relevant to the legal and professional services sectors.
- **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.

Particular consideration is given to emerging threats identified within the National Risk Assessment, including sanctions evasion, professional enablers, cyber-enabled crime, artificial intelligence, deepfake technology, and increasingly sophisticated fraud methodologies. CRL assesses the relevance of these threats to its supervised population and updates its supervisory approach accordingly.

Critical Risk Considerations

The [2025 NRA](#) continues to identify conveyancing, Trust and Company Service Provider (TCSP) activity and the misuse of client accounts as the legal services most vulnerable to money laundering. The NRA also identifies emerging threats relating to sanctions evasion, professional enablers, cyber-enabled crime, cryptoassets and Artificial Intelligence (AI), all of which should be considered by firms when assessing risk.

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.

The supervised population continues to be concentrated within generally lower-risk legal service areas, including probate, estate administration, wills, family law, litigation and advocacy. Limited exposure to conveyancing, corporate work and TCSP activity significantly reduces the sector's overall risk profile.

Two firms within the supervised population reported providing limited TCSP-related services as part of a broader service offering. No firms were identified as operating primarily as Trust and Company Service Providers and no significant TCSP activity was identified during the reporting period.

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. The supervised population remains predominantly focused on individual UK-based clients. Whilst some firms undertake work for private companies, trusts and other legal persons, exposure to complex corporate structures remains limited and generally involves straightforward ownership arrangements.

AML Statement submissions confirmed that firms reported minimal exposure to Politically Exposed Persons (PEPs) and no firms reported acting for sanctioned clients or identifying sanctioned individuals during the reporting period. The increased use of electronic verification, sanctions screening and client onboarding technologies provides additional mitigation against client-related financial crime risks.

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 or small companies 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 \(FATF\)](#).

The majority of supervised firms reported operating exclusively within the United Kingdom, with only limited overseas exposure and no reported exposure to jurisdictions currently identified by FATF as high-risk jurisdictions subject to a Call for Action.

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.

Whilst geographical exposure remains low, firms should remain alert to growing risks

associated with overseas fraud networks, sanctions evasion, cross-border financial crime and international ownership structures identified within the National Risk Assessment.

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.

Among the 22 CRL firms, 32% do not accept cash payments at all. A further 59% restrict cash payments to £500 or under, while the remaining 9% cap cash acceptance at £600 to £800.

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](#).

Supervisory activity identified significant improvements in Source of Funds procedures when compared with previous reporting periods. However, inconsistencies remain regarding the scope of enquiries undertaken, the extent to which Source of Wealth is considered, and how evidence is recorded within Client and Matter Risk Assessments and matter files. Source of Funds verification therefore remains one of the principal residual AML risks across the supervised population.

This risk is particularly relevant for firms undertaking probate and estate administration work, where significant client account balances may be administered as part of legitimate legal services. Firms should ensure that the source and legitimacy of funds are appropriately understood and evidenced.

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.

Supervisory reviews identified significant improvements in AML governance arrangements, with most firms maintaining designated compliance officers, current AML policies and documented reporting structures. However, weaknesses remain in the evidence of training activity and compliance with Regulation 24 record-keeping requirements.

Firms should ensure that formal AML training records:

- 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.
- **PEP and Sanctions Audit Trails:** Firms should maintain clear evidential records of sanctions screening, PEP assessments, escalation decisions and ongoing monitoring activities. Supervisory activity identified variability in the quality of these records.
- **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.

The increasing use of technology within legal services also requires firms to ensure that training programmes remain current and address evolving risks such as cyber-enabled fraud, sanctions evasion, Artificial Intelligence (AI), deep-fake technology and cryptoasset-related threats.

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

Emerging & Potential Risk Areas

In addition to the risks currently identified within all 22 CRL firms, firms must remain alert to emerging threats and changing risk exposures. Economic crime techniques continue to evolve rapidly, driven by technological developments, increasingly sophisticated fraud methodologies, sanctions evasion techniques and the growing international nature of financial crime.

Firms should regularly review their Practice-Wide Risk Assessments (PWRAs), Client and Matter Risk Assessments (CMRAs), AML policies and training programmes to ensure that emerging risks are appropriately identified, assessed and mitigated. Changes to business activities, client types, service offerings, delivery channels or operational structures should trigger a review of the firm's risk assessment framework.

Firms should also remain aware of proposed reforms to the UK's AML supervisory framework, including the planned transfer of supervisory responsibilities from Professional Body Supervisors to the FCA. Whilst delivery arrangements continue to develop, firms should monitor regulatory communications and ensure that governance, training and compliance arrangements remain effective throughout any transition period.

Service Provision Changes

The legal and professional services sector continues to evolve in response to regulatory reform, technological developments and changing client expectations. Firms should carefully assess the AML implications for introducing new services, operating models or client types.

Changes arising from the [Economic Crime and Corporate Transparency Act \(ECCTA\) 2023](#), including enhanced Companies House verification requirements, are expected to strengthen corporate transparency and reduce opportunities for abuse of company structures. However, firms providing corporate, company formation or related advisory services should continue to assess the risk of being used to facilitate money laundering, sanctions evasion or other forms of economic crime.

Firms expanding into higher-risk service areas, including conveyancing, Trust and Company Service Provider (TCSP) activities or complex corporate work, should ensure that their AML controls, risk assessments and staff training are updated accordingly.

Technology, AI & Cyber-Enabled Crime

The increasing use of technology presents both opportunities and risks for regulated firms. Artificial Intelligence (AI) tools are becoming increasingly sophisticated and may be used to generate fraudulent documents, impersonate clients, create convincing deepfake audio or video content, and facilitate social engineering attacks.

Firms should ensure that identity verification processes remain robust and proportionate, particularly where clients are onboarded remotely. Reliance on a single source of identification may not be sufficient where heightened risks are identified.

Cyber-enabled financial crime also represents an increasing threat. Criminals continue to target legal service providers through business email compromise, payment diversion fraud, ransomware attacks and the interception of client communications. Firms should maintain appropriate cyber security controls and ensure staff receive training on emerging cyber-related risks.

Whilst the supervised population currently reports limited exposure to cryptoasset-related activity, firms considering the acceptance of cryptocurrency or involvement in matters linked to digital assets should undertake enhanced due diligence and ensure that the source of funds, source of wealth and ownership of assets can be appropriately evidenced.

Financial Sanctions & International Risk

Financial sanctions compliance continues to be an area of growing importance. Firms should ensure that appropriate sanctions screening, politically exposed person (PEP) screening and ongoing monitoring arrangements remain in place throughout the lifecycle of a matter.

The risk of sanctions evasion continues to evolve, particularly where complex ownership structures, overseas entities, intermediaries or cross-border financial arrangements are involved. Firms should remain alert to attempts to obscure beneficial ownership or conceal links to sanctioned individuals, entities or jurisdictions.

Even where exposure to higher-risk jurisdictions remains limited, international elements within a matter should always be considered as part of the firm's risk assessment process.

Personnel Changes

While staff turnover within the supervised population remains relatively low, changes in personnel can create operational and compliance risks if responsibilities are not effectively transferred.

Firms should provide AML induction training to new employees as soon as practicable following appointment and ensure that training records are retained in accordance with regulatory requirements.

Particular attention should be given to maintaining continuity in key compliance functions. The responsibilities of the Money Laundering Reporting Officer (MLRO), Deputy MLRO (where appointed) and Money Laundering Compliance Officer (MLCO) should remain clearly defined and adequately resourced at all times.

Firms should also consider succession planning for key AML roles to ensure that absences, departures or organisational changes do not adversely affect AML oversight, reporting or compliance monitoring activities.

Overall Risk Evaluation

CRL has assessed the overall risk of money laundering, terrorist financing and proliferation financing within its supervised community as Low.

This assessment reflects the generally low-risk nature of the services provided by the supervised population, which remains predominantly focused on probate, estate administration, wills, family law, litigation and advocacy services. Exposure to higher-risk activities such as conveyancing, Trust and Company Service Provider (TCSP) services, complex corporate structures and high-risk jurisdictions remains limited.

The assessment is further supported by the predominance of UK-based individual clients, low levels of overseas exposure, widespread adoption of electronic identity verification and sanctions screening solutions, and improvements observed in AML governance, Practice-Wide Risk Assessments (PWRAs), customer due diligence procedures and financial sanctions compliance.

Notwithstanding the overall low-risk assessment, a number of residual risks remain within the sector. In particular:

- **Financial Transactions** continue to present a medium risk due to the ongoing need to strengthen Source of Funds and Source of Wealth enquiries, improve evidential records and ensure that verification measures are applied consistently and proportionately.
- **Training and Governance Frameworks** continue to present a medium risk due to variability in AML training records, the quality of risk assessment documentation, evidence of ongoing monitoring activities and the maintenance of comprehensive audit trails for sanctions and PEP screening.

Whilst these issues do not indicate widespread non-compliance, they represent areas where firms should continue to strengthen existing controls and improve the quality of documentation supporting those controls.

The risk environment also continues to evolve. Emerging risks associated with artificial intelligence, deep-fake technology, cyber-enabled fraud, sanctions evasion and crypto-asset-related activity require ongoing monitoring and consideration within firm-level risk assessments and AML frameworks.

CRL will continue to adopt a risk-based approach to supervision, using AML Statements, supervisory reviews, onsite inspections, intelligence sources and sector-wide analysis to monitor trends and identify emerging vulnerabilities. Future supervisory activity will focus on ensuring that firms maintain effective and proportionate controls, whilst continuing to build on the significant improvements observed across the supervised population during the reporting period.

Guidance for Firms

CRL has identified a number of money laundering, terrorist financing and proliferation financing risks that firms should consider when developing and maintaining their AML frameworks.

One of the primary objectives of this assessment is to assist firms in understanding these risks, evaluating their exposure and implementing proportionate controls to mitigate them.

This section provides practical guidance and examples of good practice to help firms maintain effective AML controls and meet their regulatory obligations in the following key 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](#) require regulated firms to establish, maintain and regularly review appropriate policies, controls and procedures to mitigate and manage money laundering, terrorist financing and proliferation financing risks.

AML policies form a fundamental part of a firm's compliance framework and should reflect the nature, size and complexity of the business. Policies should be informed by the firm's Practice-Wide Risk Assessment (PWRA), aligned to the services offered and supported by practical procedures that staff can apply consistently.

CRL's review of AML documentation during the 2025-26 supervisory cycle identified significant improvements in the overall quality of AML policies across the supervised population. Most firms maintained documented policies that were current, proportionate and broadly aligned to their business activities. However, a number of recurring areas for improvement were identified.

- **Document Control and Governance Weaknesses:** Several policies lacked clear version control, review dates or approval records. In some instances, policies had been updated but it was not apparent when changes had been made or who had authorised them.
- **Insufficient Proliferation Financing Coverage:** Whilst awareness of proliferation financing obligations has improved, a number of policies contained only limited reference to proliferation financing risks or did not adequately explain how such risks should be assessed and mitigated.
- **Limited Source of Funds and Source of Wealth Guidance:** Some firms maintained broad references to Source of Funds checks but provided limited operational guidance regarding when checks should be undertaken, what evidence should be obtained and how the results should be recorded.
- **Sanctions Procedures Requiring Greater Detail:** While sanctions screening was generally addressed, policies did not always contain sufficient information regarding escalation procedures, ongoing monitoring requirements, OFSI reporting obligations, licensing considerations or the management of potential matches.

- **Policies Not Fully Aligned to Business Activities:** In a small number of cases, policies contained references to services, risks or controls that did not reflect the firm's actual business model, suggesting that documentation had not been fully tailored to the firm's practice areas and risk profile.

To support firms in strengthening their AML documentation, CRL recommends that firms:

- **Maintain Tailored Policies:** Ensure AML policies accurately reflect the firm's services, client base, delivery channels and risk exposure and are not reliant on generic wording or template content.
- **Strengthen Document Governance:** Implement effective version control, approval processes and review dates to demonstrate that policies are actively managed and regularly reviewed.
- **Expand Proliferation Financing Controls:** Ensure AML documentation adequately addresses proliferation financing obligations and supports compliance with current legislative requirements.
- **Enhance Source of Funds Procedures:** Clearly document the firm's approach to Source of Funds and, where appropriate, Source of Wealth enquiries, including evidential expectations and escalation requirements.
- **Develop Comprehensive Sanctions Procedures:** Include clear guidance covering sanctions screening, ongoing monitoring, escalation procedures, asset freeze obligations, OFSI reporting requirements and the firm's approach to sanctions-related decision making.
- **Review Policies Following Significant Change:** Policies should be reviewed at least annually and whenever there are material changes to the firm's services, client profile, regulatory obligations or risk exposure.

Practice-Wide Risk Assessment (PWRA)

Under [Regulation 18](#) of the [MLR 2017](#), firms within scope of the regulations must identify and assess the risks of money laundering, terrorist financing and proliferation financing to which their business is exposed. These assessments must be documented, kept under regular review and used to inform the firm's AML policies, procedures and controls.

A well-developed PWRA is a fundamental component of an effective AML framework. It enables firms to understand their inherent risks, assess the effectiveness of existing controls and determine whether additional mitigations are required. The assessment should be proportionate to the size, nature and complexity of the firm and should consider factors such as:

- Client risk.
- Service and matter risk.
- Geographic risk.
- Delivery channel risk.
- Transaction risk.
- Sanctions risk.
- Proliferation financing risk.
- Emerging economic crime threats relevant to the firm's services.

The PWRA should also take account of external sources of information, including the National Risk Assessment (NRA), Legal Sector Affinity Group (LSAG) guidance, sector-specific risk assessments and guidance issued by CRL.

CRL routinely reviews firms' PWRAs through desk-based reviews, supervisory engagement and inspection activity. Firms should therefore ensure that their assessments remain current, are subject to regular review and accurately reflect the firm's risk profile and business activities.

CRL identified that all 22 of its firms maintained a documented PWRA. However, a number of recurring weaknesses were identified.

- **Insufficient Risk Analysis:** Many assessments identified relevant risks but contained limited analysis of how those risks affected the firm in practice or how existing controls mitigated those risks.
- **Limited Service-Specific Assessment:** Some firms did not adequately differentiate between the risks associated with different services, client types or delivery channels, resulting in risk assessments that were overly broad.
- **Weak Residual Risk Evaluation:** Whilst inherent risks were often identified, firms did not always demonstrate how the effectiveness of mitigating controls had been considered when determining overall risk exposure.
- **Incomplete Consideration of Emerging Risks:** Some PWRAs contained limited consideration of sanctions evasion, proliferation financing, misuse of corporate structures, professional enabling risks, technology-enabled crime and other emerging threats identified through national risk assessments and supervisory intelligence.
- **Reactive Rather Than Proactive Review:** In several cases, review dates suggested that documents had been updated immediately prior to submission to CRL, with limited evidence of regular review throughout the reporting period.
- **Inconsistent Risk Scoring Methodologies:** Some firms applied risk ratings without clearly explaining the methodology used or the rationale supporting the final risk assessment.

To support firms in strengthening their PWRAs, CRL recommends that firms:

- **Maintain a Comprehensive and Documented PWRA:** Ensure the assessment is fully documented, proportionate to the firm's activities and capable of demonstrating compliance with Regulation 18.
- **Undertake Detailed Risk Analysis:** Move beyond generic descriptions of risk by clearly explaining how identified risks arise within the firm's practice and how those risks are managed.
- **Assess Inherent and Residual Risk Separately:** Consider both the level of risk before controls are applied and the firm's residual risk exposure after mitigating measures have been implemented.
- **Address Emerging Risks:** Regularly review emerging threats identified through CRL publications, the NRA, LSAG guidance and wider economic crime intelligence, ensuring these risks are reflected where relevant.
- **Implement a Clear Review Process:** Review and update the PWRA at least annually and whenever there is a significant change to the firm's services, client base, ownership structure or risk profile.
- **Ensure Senior Management Oversight:** The PWRA should be approved by senior

management and form part of the firm's wider governance and compliance framework.

- **Use the PWRA to Drive AML Controls:** The findings of the PWRA should directly inform AML policies, Client and Matter Risk Assessments (CMRAs), training programmes and ongoing monitoring arrangements.

A common theme identified during the 2025-26 review cycle was that firms generally understood the requirement to maintain a PWRA, but the quality of supporting analysis varied significantly. Firms should ensure that their PWRA demonstrates not only what risks exist, but also how those risks have been assessed, mitigated and reviewed over time. This provides a clear evidential basis for the firm's risk-based approach and supports the effectiveness of its wider AML compliance framework.

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 where a client or matter is assessed as low risk, firms should ensure that the rationale for the risk rating is clearly documented and supported by appropriate evidence. The level of detail recorded should be proportionate to the risks identified and sufficient to demonstrate that appropriate due diligence and risk assessment measures have been undertaken.

CRL's supervisory reviews identified a number of recurring themes in CMRA documentation

where firms could strengthen record keeping, evidencing and overall assessment quality:

- **Lack of Detail and Supporting Rationale:** Some CMRAs relied heavily on Yes/No responses with limited narrative explanation. Whilst key risk factors such as PEP status, sanctions exposure and source of funds were generally considered, firms did not always record the rationale behind risk decisions or provide sufficient evidence of verification steps undertaken.
- **Variability in Assessment Quality:** Whilst most firms maintained documented CMRAs, the quality, structure and level of detail varied. In some cases, assessments relied heavily on template wording or file notes that did not clearly demonstrate how specific risks had been assessed and mitigated.
- **Source of Funds Recording:** Source of Funds considerations were generally reflected within AML policies; however, firms did not always adequately record within the CMRA what enquiries had been undertaken, what evidence had been reviewed or how concerns had been resolved. In some cases, assessments relied primarily on information provided by the client without recording additional verification steps.
- **PEP and Sanctions Screening Audit Trails:** Although firms generally conducted PEP and sanctions screening, supervisory reviews identified inconsistencies in how screening results, escalation decisions and ongoing monitoring activities were documented within client files and risk assessments.

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

- **Enhance Assessment Quality:** Firms should ensure that CMRAs contain sufficient narrative explanation to demonstrate how risks have been assessed, what checks have been undertaken, what evidence has been reviewed and how any identified risks have been mitigated. Risk ratings should be supported by a clear rationale and documented decision-making process.
- **Ensure Alignment with Firm-Wide Controls:** Firms should ensure that CMRAs are consistent with their PWRA, AML policies and procedures, and reflect the specific risks associated with the client, matter and service provided.
- **Maintain Ongoing Reviews:** Firms should review and update CMRAs whenever there is a material change in risk, at key stages of a matter, and where new information becomes available that may affect the risk assessment.
- **Train Staff on CMRA Completion:** Firms should provide targeted training on identifying and assessing risk factors, documenting due diligence measures and recording risk-based decisions consistently and effectively.
- **Quality Assurance and Monitoring:** Firms should implement proportionate quality assurance procedures to review CMRAs periodically and ensure assessments remain accurate, complete and consistent across the firm.
- **Document Ongoing Monitoring:** Firms should ensure that ongoing monitoring activities are recorded appropriately throughout the life of a matter, including changes in client circumstances, source of funds information, sanctions screening results and any revised risk assessments.

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 undertake appropriate client identification and verification measures, regardless of whether they fall within the scope of the MLR 2017. Such measures support the management of financial crime risks, assist with conflict checks and help identify PEPs, sanctioned individuals and other higher-risk clients. Firms should retain sufficient records to demonstrate the checks undertaken and the decisions reached.

CRL's supervisory reviews identified several recurring themes where firms could strengthen the quality, consistency and evidencing of their CDD procedures:

- **Identity Verification Records:** Most firms had established identity verification procedures; however, documentation did not always clearly demonstrate what identification had been obtained, how it had been verified, or where supporting evidence was retained.
- **Recording of Electronic Verification Results:** The use of electronic verification and screening tools has become increasingly common across the supervised

population. However, firms did not always record within the CMRA or matter file which checks had been undertaken, the results obtained or any follow-up actions required.

- **Links Between CDD and Source of Funds Enquiries:** Firms did not always demonstrate how CDD findings informed Source of Funds enquiries or how additional verification measures were applied where higher-risk indicators were identified.
- **Ongoing Monitoring:** Firms did not always clearly evidence ongoing monitoring activities, including updates to client information, reassessments of risk, sanctions rescreening and reviews triggered by changes in circumstances.
- **Policy and Procedure Alignment:** Supervisory reviews identified instances where AML policies described controls that were not consistently evidenced within client files, CMRAs or associated records.

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

- **Maintain Clear Identity Verification Records:** Firms should ensure that client files and risk assessments clearly record the identification documents reviewed, verification methods used and the outcome of checks undertaken.
- **Utilise Appropriate Verification Technology:** Firms should consider the use of reliable electronic verification and screening tools where appropriate and ensure the results of such checks are retained within the client file or case management system.
- **Ensure Consistency Between CDD and Source of Funds Controls:** Firms should ensure that CDD findings, risk assessments and Source of Funds enquiries are considered together and that any higher-risk indicators trigger additional enquiries or enhanced due diligence where appropriate.
- **Implement Effective Ongoing Monitoring:** Firms should ensure client information, risk assessments and screening outcomes are reviewed and updated where there is a material change in risk or circumstances.
- **Ensure Alignment Between Policies and Practice:** Firms should periodically review AML procedures, client files and risk assessments to ensure operational practices remain consistent with documented AML policies.
- **Provide Regular CDD Training:** Firms should provide staff with regular training on client identification, verification requirements, ongoing monitoring, escalation procedures, high-risk indicators and the effective use of any verification technologies.

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, possess, or transfer criminal property (Sections [327](#) and [329](#)), 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](#).

Firms should apply a risk-based approach to SoF enquiries, ensuring that checks are proportionate to the level of risk presented by the client and matter. The enquiries undertaken, evidence reviewed and conclusions reached should be clearly documented and supported by reliable information, such as bank statements, property sale completion statements, inheritance documentation or other appropriate evidence.

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

Source of Funds enquiries remain a key area of supervisory focus. Whilst supervisory reviews identified improvements in the approach taken by many firms, variability remains in the quality of enquiries undertaken and the extent to which those enquiries are evidenced within client files, risk assessments and supporting documentation.

CRL's supervisory reviews identified several recurring themes where firms could strengthen the quality, consistency and evidencing of Source of Funds enquiries:

- **Variability in Source of Funds Procedures:** Most firms addressed Source of Funds requirements within their AML policies and procedures; however, the level of detail provided varied considerably. In some cases, procedures did not clearly explain what evidence should be obtained, when additional enquiries were required or how findings should be documented.
- **Recording of Source of Funds Enquiries:** Firms did not clearly record within the CMRA or client file what Source of Funds enquiries had been undertaken, what evidence had been reviewed or how the legitimacy of funds had been assessed. The rationale supporting risk-based decisions was not always evident.
- **Consistency Between Policies and Client Files:** Supervisory reviews identified instances where AML policies described Source of Funds controls that were not fully reflected within client files, risk assessments or supporting records. Firms should ensure that documented procedures are consistently applied in practice.
- **Risk-Based Application of Source of Funds Controls:** Source of Funds enquiries were not always applied consistently across different matter types. Firms should ensure that the level of enquiry is proportionate to the risks identified and that decisions to limit or expand enquiries are appropriately justified and documented.

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

- **Maintain Clear Source of Funds Procedures:** Firms should establish documented procedures that explain when Source of Funds enquiries are required, what types of evidence may be appropriate and how enquiries should be recorded and evidenced.
- **Record Source of Funds Enquiries Clearly:** Firms should ensure that CMRAs and client files clearly record the enquiries undertaken, evidence reviewed, any concerns identified and the rationale supporting the firm's conclusions.
- **Apply a Risk-Based Approach:** Firms should ensure that Source of Funds enquiries are proportionate to the risks presented by the client and matter. Where minimal enquiries are considered appropriate, the rationale should be recorded.
- **Ensure Consistency Between Policy and Practice:** Firms should periodically review client files and risk assessments to ensure Source of Funds procedures are being applied consistently and in accordance with documented AML policies.

- **Provide Regular Training on Source of Funds Enquiries:** Firms should ensure relevant staff understand how to identify red flags, assess Source of Funds information, document enquiries appropriately and escalate concerns where necessary.
- **Review and Update Procedures Regularly:** Firms should periodically review Source of Funds procedures to reflect changes in legislation, regulatory guidance, emerging risks and lessons learned from supervisory activity.
- **Consider Source of Wealth Where Appropriate:** Where higher-risk clients, higher-value matters, unusual transactions or other risk indicators are present, firms should consider whether Source of Wealth enquiries are required in addition to Source of Funds checks and record the reasoning for their approach.

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 adopt a risk-based approach to identifying, assessing and managing risks associated with Politically Exposed Persons (PEPs), their family members and known close associates, as well as individuals, entities and jurisdictions subject to financial sanctions. Effective screening and ongoing monitoring are important controls in preventing economic crime and ensuring compliance with UK financial sanctions legislation.

PEP and Sanctions screening remains an important component of a firm's AML and financial crime framework. Supervisory reviews identified widespread use of screening processes and electronic screening solutions; however, variability remains in how checks, outcomes, escalation decisions and ongoing monitoring activities are evidenced within client files and risk assessments.

CRL's supervisory reviews identified several recurring themes where firms could strengthen the quality, consistency and evidencing of PEP and sanctions screening controls:

- **Variation in Documented Procedures:** Most firms included PEP and Sanctions controls within their AML policies and procedures; however, the level of detail varied. In some cases, policies did not clearly describe screening methodologies, escalation processes, ongoing monitoring requirements or record-keeping expectations.
- **Recording of Screening Activity:** Whilst many firms utilise electronic screening tools, supervisory reviews identified inconsistencies in how screening activity was recorded. Client files and risk assessments did not always demonstrate what screening had been undertaken, when checks had been completed or the outcome of those checks.
- **Consistency Between Policies and Operational Records:** Supervisory reviews identified instances where documented procedures were not fully evidenced within client files, CMRAs or other AML records. Firms should ensure screening controls are consistently documented and applied in practice.

- **Escalation and Ongoing Monitoring Records:** Firms did not always maintain clear audit trails demonstrating how potential matches were reviewed, what decisions were taken, who authorised those decisions or how ongoing monitoring requirements were managed following onboarding.

To support firms in meeting their obligations relating to PEP and sanctions screening, CRL recommends the following:

- **Maintain Clear Screening Procedures:** Firms should establish documented procedures covering the screening process, timing of checks, escalation requirements, ongoing monitoring arrangements and record-keeping expectations.
- **Document Screening Results:** Firms should ensure that screening activity, outcomes, risk assessments and any resulting actions are appropriately recorded within the CMRA, client file or case management system.
- **Utilise Appropriate Screening Solutions:** Firms should consider the use of reliable and up-to-date screening tools where appropriate and ensure that the results of any screening undertaken are retained for audit purposes.
- **Ensure Consistency Between Policy and Practice:** Firms should periodically review client files, screening records and AML documentation to ensure that operational practices remain aligned with documented procedures.
- **Provide Regular Training:** Firms should ensure that relevant staff receive training on identifying PEPs and sanctions risks, interpreting screening results, applying risk-based decision making and escalating concerns appropriately.
- **Maintain Escalation and Reporting Procedures:** Firms should ensure staff understand internal reporting arrangements, MLRO escalation processes, sanctions reporting requirements and the circumstances in which a Suspicious Activity Report (SAR) may be required.
- **Maintain Ongoing Screening:** Firms should consider when sanctions and PEP rescreening is appropriate, particularly for long-running matters, changes in risk profile or where new information becomes available during the course of a matter.

Suspicious Activity Reporting (SAR)

Suspicious Activity Reporting (SAR) forms a critical part of the UK's anti-money laundering framework. Under [Part 7](#) of the [Proceeds of Crime Act 2002 \(POCA\)](#), individuals working within the regulated sector may be required to make disclosures where they know, suspect, or have reasonable grounds to suspect that money laundering is taking place. Firms must also maintain effective systems and controls to identify, assess and escalate suspicious activity as part of their wider AML framework.

Effective SAR processes support firms in identifying potential criminal property, protecting the firm from exposure to money laundering offences and contributing to the wider national response to economic crime. Firms should ensure that all staff understand how concerns are identified, escalated internally and, where appropriate, reported to the National Crime Agency (NCA).

CRL's review of AML Statements, supervisory returns and supporting documentation identified several recurring themes relating to SAR awareness and reporting arrangements.

- **No SARs Submitted During the Reporting Period:** No SARs were reported as having been submitted by firms within the supervised population during the reporting period. Whilst this may reflect the relatively small size and risk profile of much of the population, firms should regularly evaluate whether staff are capable of identifying suspicious activity and escalating concerns appropriately.

- **SAR Portal Registration Not Universally Maintained:** Most regulated firms had access to the National Crime Agency SAR Portal. However, a small number of firms had not established, activated or maintained SAR Portal access despite previous supervisory engagement.
- **Limited Internal Reporting Procedures:** Some firms maintained only high-level references to SAR obligations within AML documentation. Procedures did not always clearly explain how concerns should be raised internally, how decisions should be documented or who was responsible for making external disclosures.
- **Insufficient Record Keeping and Audit Trails:** Firms were not always able to demonstrate how internal suspicions had been assessed, documented and resolved where a decision had been taken not to submit a SAR.
- **Training and Awareness Gaps:** In a small number of cases, AML training records did not demonstrate adequate coverage of SAR reporting obligations, internal escalation processes or common money laundering indicators relevant to the firm's services.

To strengthen SAR compliance arrangements, CRL recommends that firms:

- **Maintain Active SAR Portal Registration:** Ensure that the firm's MLRO, nominated officer or other relevant individual has active access to the NCA SAR Portal and understands how reports are submitted.
- **Implement Clear Internal Reporting Procedures:** Establish documented procedures that explain how suspicions are identified, escalated, assessed and recorded, including roles and responsibilities at every stage of the process.
- **Provide Regular SAR Training:** Ensure staff receive training on recognising money laundering indicators, identifying suspicious activity, internal reporting requirements, confidentiality obligations and the risks associated with tipping off.
- **Maintain Appropriate Records:** Keep records of internal disclosures, investigations, decisions and rationale, including cases where a decision is made not to submit a SAR. This helps demonstrate compliance with legal and regulatory obligations.
- **Periodically Review Reporting Effectiveness:** Firms should periodically assess whether SAR policies and procedures remain effective by reviewing internal reports, compliance monitoring outcomes and emerging risk indicators.
- **Align SAR Procedures with Wider AML Controls:** SAR processes should be integrated with the firm's PWRA, AML Policy, Client and Matter Risk Assessments (CMRAs), ongoing monitoring arrangements and staff training programme.

The absence of SAR submissions does not necessarily indicate an absence of risk. Firms should ensure that their reporting framework encourages appropriate challenge, escalation and documentation of concerns, and that staff remain alert to emerging threats such as fraud, sanctions evasion, criminal use of companies and trusts, organised immigration crime and other forms of economic crime relevant to the legal sector.

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 and regulatory framework, risk indicators, suspicious activity reporting procedures and the firm's internal AML controls and should be tailored to the employee's role and responsibilities.

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 training records during supervisory reviews and onsite inspections and may request them as part of ongoing supervisory activity. Firms should therefore ensure that training records are accurate, complete and capable of demonstrating compliance with [Regulation 24](#) of the [MLR 2017](#).

Training and staff competency remain a key area of supervisory focus. Supervisory reviews identified that AML training is generally being undertaken across the supervised population; however, improvements are required in the recording, evidencing and monitoring of training activity to demonstrate compliance with [Regulation 24](#) of the [MLR 2017](#).

CRL's supervisory reviews identified several recurring themes where firms could strengthen their training and competency frameworks:

- **Training Record Quality:** Whilst most firms were able to demonstrate that AML training had been undertaken, training records were not always sufficiently detailed to demonstrate compliance with Regulation 24. In some cases, records did not clearly identify who had completed training, when training occurred or what topics had been covered.
- **Maintenance of Training Records:** Firms did not always maintain training records consistently or update them following the completion of training activities. Supporting information, such as course content, training providers or evidence of completion, was not always retained.
- **Training for Key Compliance Personnel:** Supervisory reviews identified variability in the level of documented AML training retained for MLROs, MLCOs and other

senior personnel. Firms should ensure that individuals with specific AML responsibilities receive appropriate training relevant to their functions.

- **Coverage of Emerging and Specialist Risk Areas:** Training programmes did not always clearly demonstrate coverage of topics such as proliferation financing, financial sanctions, suspicious activity reporting procedures, cyber-enabled crime and emerging financial crime threats.

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

- **Maintain Comprehensive Training Records:** Firms should retain up-to-date training records detailing the individuals trained, dates of training, topics covered, training provider, delivery method and any supporting evidence of attendance or completion.
- **Ensure Annual and Role-Specific Training:** Training should be conducted annually and tailored to staff responsibilities. MLROs, MLCOs and other individuals with AML responsibilities should receive training appropriate to the nature and scope of their responsibilities.
- **Cover All Relevant AML Topics:** Firms should ensure training covers money laundering and terrorist financing risks, proliferation financing, SAR reporting procedures, PEP & Sanction screening, data protection, artificial intelligence-enabled fraud, cyber-enabled financial crime and emerging economic crime risks where relevant to the firm.
- **Embed Training Within the Compliance Framework:** Firms should incorporate training into their wider compliance programme and use lessons learned from supervisory activity, internal reviews and emerging risks to inform future training needs.
- **Monitor Training Effectiveness:** Firms should periodically assess whether training remains relevant, effective and proportionate to the firm's risk profile, and use feedback, quality assurance reviews and supervisory findings to support continuous improvement.
- **Maintain Evidence of Competency:** Firms should consider how they assess and evidence staff understanding of AML obligations, particularly for individuals undertaking key compliance functions or higher-risk work.

Conclusion

The UK legal sector continues to present a Medium risk of money laundering, terrorist financing and proliferation financing. As identified within the National Risk Assessment, certain legal services remain attractive to criminals seeking to conceal, transfer or legitimise the proceeds of crime, particularly where client accounts, conveyancing services, complex corporate structures or Trust and Company Service Provider (TCSP) activities are involved.

However, based on AML Statement submissions, supervisory reviews, onsite inspections and wider monitoring activity, CRL has assessed the overall residual risk within its supervised population as Low.

This assessment reflects the characteristics of the firms subject to CRL AML supervision, which are predominantly focused on probate, estate administration, wills, family law, litigation and advocacy services. The supervised population has limited exposure to higher-risk activities such as conveyancing and TCSP services, predominantly acts for UK-based individual clients and has minimal exposure to high-risk jurisdictions or complex ownership structures.

Supervisory activity has also identified positive improvements in AML compliance arrangements across the supervised population, including stronger governance frameworks, improved Practice-Wide Risk Assessments, increased use of electronic identity verification and sanctions screening solutions, and greater awareness of money laundering, terrorist financing and proliferation financing risks.

Notwithstanding the overall low-risk assessment, CRL has identified Financial Transactions and Training and Governance Frameworks as the principal residual risk areas requiring continued attention.

Financial Transactions remain assessed as Medium Risk due to ongoing variability in the quality and evidencing of Source of Funds and, where appropriate, Source of Wealth enquiries. Whilst firms are generally undertaking these checks, supervisory reviews identified opportunities to improve the consistency of enquiries, supporting documentation and audit trails.

Training and Governance Frameworks also remain assessed as Medium Risk due to variability in AML training records, risk assessment quality, ongoing monitoring records and evidential audit trails relating to sanctions and PEP screening activities. These findings primarily relate to the recording and evidencing of controls rather than an absence of controls.

Firms should continue to review and strengthen their AML frameworks, ensuring that Practice-Wide Risk Assessments, Client and Matter Risk Assessments, customer due diligence measures and staff training programmes remain proportionate to the risks presented by their business activities.

The risk environment continues to evolve, and firms should ensure that emerging threats including artificial intelligence-enabled fraud, cyber-enabled crime, sanctions evasion, deepfake technology and cryptoasset-related activity are appropriately considered within their risk assessments, policies and procedures.

The proposed transition of AML supervisory responsibilities to the FCA represents a significant regulatory development for the supervised sector. Whilst details of implementation continue to evolve, CRL will continue supervising firms and maintaining its existing risk-based approach throughout the transition period. CRL will work with government, the FCA and the profession to support a smooth transition and minimise disruption to firms.

CRL will continue to apply a risk-based and intelligence-led approach to supervision

through AML Statement reviews, onsite inspections and engagement with key stakeholders. Future supervisory activity will focus on supporting firms in maintaining effective and proportionate controls, whilst building upon the positive improvements observed across the supervised population during the reporting period.

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.
SRA (Sectoral Risk Assessment)	CILEx Regulation's evaluation of the money laundering and terrorist financing risks faced by the legal services sector, designed to help regulated firms understand, assess, and mitigate the specific risks relevant to their activities.
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.