RICS PROFESSIONAL STANDARD

Countering bribery, corruption, money laundering and terrorist financing

Global

1st edition, February 2019

Effective from September 2019

RICS®

Countering bribery, corruption, money laundering and terrorist financing

RICS professional standard

1st edition, February 2019

Effective from 1 September 2019

Published by the Royal Institution of Chartered Surveyors (RICS)

Parliament Square

London

SW1P 3AD

www.rics.org

Produced by the RICS Commercial Property Professional Group.

This document was originally published in February 2019 as an RICS professional statement and was reissued in October 2022 as an RICS professional standard.

ISBN 978 1 78321 330 6

Contents

Acknowledgements

RICS would like to thank the following for their contributions to this professional standard.

Technical author:

Alex Ktorides (Inces Gordon Dadds)

With special thanks to Benjamin Atkins and James Fraser

Working group:

Andrea Amadesi FRICS (APREA)

Alexander Aronsohn FRICS (RICS)

Nigel Astbury MRICS (Christie and Co)

Peter Bolton-King FRICS (RICS)

Caitriona de Burca (Sherry Fitzgerald)

Gillian Dixon, Gerald Eve

Frances Forsyth (Arcadis)

Raquel Loll (RICS)

Vicky Moss (BNP Paribas Real Estate)

Ilana Rosenzweig (RICS)

Thijs Stoffer (ICREA)

Cyril Troyanov (Altenburger Ltd)

Jo Upton MRICS (Pegasi)

Richard Watson MRICS

RICS Professional Group lead:

Nigel Sellars FRICS (RICS)

Special thanks:

Jon Bowey MRICS

RICS Publishing:

Standards Publishing Manager: Antonella Adamus

Project Manager: Ellie Scott

Editor: Sean Agass

RICS standards framework

RICS' standards setting is governed and overseen by the Standards and Regulation Board (SRB). The SRB's aims are to operate in the public interest, and to develop the technical and ethical competence of the profession and its ability to deliver ethical practice to high standards globally.

The RICS Rules of Conduct set high-level professional requirements for the global chartered surveying profession. These are supported by more detailed standards and information relating to professional conduct and technical competency.

The SRB focuses on the conduct and competence of RICS members, to set standards that are proportionate, in the public interest and based on risk. Its approach is to foster a supportive atmosphere that encourages a strong, diverse, inclusive, effective and sustainable surveying profession.

As well as developing its own standards, RICS works collaboratively with other bodies at a national and international level to develop documents relevant to professional practice, such as cross-sector guidance, codes and standards. The application of these collaborative documents by RICS members will be defined either within the document itself or in associated RICS-published documents.

Document definitions

Document type	Definition
RICS professional standards	**Set requirements or expectations for RICS members and regulated firms about how they provide services or the outcomes of their actions.** RICS professional standards are principles-based and focused on outcomes and good practice. Any requirements included set a baseline expectation for competent delivery or ethical behaviour. They include practices and behaviours intended to protect clients and other stakeholders, as well as ensuring their reasonable expectations of ethics, integrity, technical competence and diligence are met. Members must comply with an RICS professional standard. They may include: • mandatory requirements, which use the word 'must' and must be complied with, and/or • recommended best practice, which uses the word 'should'. It is recognised that there may be acceptable alternatives to best practice that achieve the same or a better outcome. In regulatory or disciplinary proceedings, RICS will take into account relevant professional standards when deciding whether an RICS member or regulated firm acted appropriately and with reasonable competence. It is also likely that during any legal proceedings a judge, adjudicator or equivalent will take RICS professional standards into account.
RICS practice information	**Information to support the practice, knowledge and performance of RICS members and regulated firms, and the demand for professional services.** Practice information includes definitions, processes, toolkits, checklists, insights, research and technical information or advice. It also includes documents that aim to provide common benchmarks or approaches across a sector to help build efficient and consistent practice. This information is not mandatory and does not set requirements for RICS members or make explicit recommendations.

Glossary

The following definitions relate to this professional standard and do not include legal or other matters as defined in relation to local legislative or regulatory requirements.

Term	Definition
Adequate knowledge	An appropriate understanding of the issues and responses connected to bribery, corruption, money laundering and terrorist financing so that the individual can apply the requirements of this professional standard to their role. This level of knowledge will vary depending on the sector, organisation and role that the individual works in. The knowledge may be gained through attending training, private study or work-based experience.
Applicable laws	The local and global laws and regulations that apply to firms and individuals. These may depend on the main place of business, where the alleged corrupt act or bribe was paid or received, or the country in which a parent company is registered.
Beneficial ownership/owner	Anyone who benefits from ownership of a security or property, who may or may not be on record as the owner. This also incorporates those who exercise ultimate effective control over a legal person or arrangement. In many jurisdictions the beneficial owner is defined as an individual who owns or controls 25% or more of the shares or profits of a legal entity.
Bribery	The offer, promise, giving, demanding or acceptance of an advantage as an inducement for an action that is illegal, unethical or a breach of trust.
Corruption	The misuse of public office or power for private gain, or misuse of private power in relation to business practice and performance.

Term	Definition
Customer due diligence (CDD)/know your customer (KYC)	Taking the appropriate steps to ascertain who the customer or client is and, if relevant, their ultimate beneficial owner is and counterparty. These can be relatively simple checks to verify the identity of the customer/client or may entail deeper investigations. This is a legal and regulatory requirement in many countries.
'Facilitation payment'	A payment made to a government official with the purpose of speeding up a routine administrative action. Such payments are customary and legal in some countries, but in many jurisdictions they are criminalised.
Money laundering	Concealing the source of the proceeds of criminal activity to disguise their illegal origin. This may take place through hiding, transferring and/or recycling illicit money or other currency through one or more transactions, or converting criminal proceeds into seemingly legitimate property.
Person of Significant Control (PSC)	Individuals or legal entities who have significant control or influence over a company. This control and influence can be exercised in a variety of ways, for instance the individual has absolute veto rights over decisions related to the running of the company.
Politically exposed person (PEP)	Individuals and the family members of such individuals, entrusted with prominent public functions by any country or international organisation. This includes heads of state or government, senior politicians, senior governmental, judicial or military officials, senior executives of state-owned corporations and directors, deputy directors and members of the board or equivalent functions within international organisations. PEPs who relinquish office or their relatives who cease being family members (e.g. through divorce) are no longer treated as PEPs 12 months after this occurs.

Term	Definition
Price-fixing monopoly-cartel	A group of formally independent producers of goods or services whose goal is to increase their collective profits by pushing the price of a product as high as possible (or perhaps fix, peg, discount or stabilise prices), generally leading to profits for all sellers.
Professional money launderers	Those that specialise in enabling criminals to evade anti-money laundering and counter-terrorist financing safeguards and sanctions. They perform this function for a fee or commission. For instance, tax advisers, lawyers or accountants who act as professional facilitators for criminals.
Red flags	Common characteristics that either individually or in combination might indicate potential misuse of the real estate sector for money laundering or terrorist financing purposes.
Reliance	The extent to which the required checks on individuals or companies have been undertaken satisfactorily by a third party, meaning that these checks do not need to be duplicated.
Reporting	Taking the appropriate action to draw attention to known or suspected activity involving money laundering, bribery or corruption issues and/or terrorist financing. The action of reporting may take the form of internal or external processes, and should as a minimum comply with the applicable laws as defined.
Scheme	A specific operation or case of money laundering or terrorist financing that combines various techniques, mechanisms and instruments into a single structure.

Term	Definition
Terrorism	The use or threat of violence to pursue ideological objectives committed by governments, non-state actors, or undercover personnel serving on behalf of governments. Terrorism reaches beyond its immediate target victims and is also directed at targets that represent a larger spectrum of society. Various national legislations contain their own definitions of terrorism and lists of groups designated terrorist organisations.
Terrorist financing	The solicitation, collection or provision of funds with the intention that they may be used to support terrorist acts or organisations. Funds appropriated directly or indirectly for this purpose constitute terrorist funding.
Triggering event	An event that necessitates a firm re-evaluating the risk level of a customer, client, partner, third party provider or employee, and possibly conducting enhanced due diligence.

For further information on these definitions please refer to the Financial Action Task Force (FATF) – see www.fatf-gafi.org.

Foreword

As an anti-corruption NGO, Transparency International (TI) seeks to raise awareness of the social, economic and political costs of corruption, and advocates concrete measures to tackle them. In the 25 years since TI was founded, large-scale corruption has become increasingly understood as a cross-border phenomenon. Corruption involves not only public officials and private bribe payers, but often also requires access to the financial system, the use of anonymous shell companies and professional facilitators to help launder the proceeds.

Far from being a victimless crime, corruption also deprives state institutions of sorely needed resources. Resources that could be used for investment in health, education and infrastructure among many other areas.

In recent years, the evidence base showing that money laundering through real estate is not just a risk but a reality has multiplied. Research published in 2016 by TI-UK identified 986 London land titles with links to Politically Exposed Persons (PEPs), owned through corporate structures registered in secrecy jurisdictions. In Canada, meanwhile, 46 of the 100 most expensive homes in Vancouver were found to have unclear ownership using offshore shell companies, trusts and nominees.

As well as weaknesses in anti-money laundering legal frameworks that allow for these and other types of opaque ownership, in many countries public authorities have insufficient resources for oversight and supervision. Country assessments carried out by the global standard-setter FATF (Financial Action Task Force), in over 50 countries since 2014, have identified repeated institutional and legal gaps.

In this context, proactive steps taken by the real estate profession to strengthen standards, such as this professional standard from RICS, are very welcome. In particular, the expectation in this standard that RICS members and regulated firms should go beyond legislative and regulatory requirements is critical, precisely due to the structural weaknesses that exist. Where consistently implemented, measures that serve to increase transparency, reduce risk and promote trust also lead to improved business outcomes at the sector level.

During 2017 and 2018, TI benefited directly from RICS input on a project that seeks to increase dialogue between authorities, the sector and civil society regarding the effective implementation of anti-money laundering measures. TI looks forward to continued engagement with RICS, and to sharing the lessons that emerge from the roll-out of this professional standard to RICS membership.

– Transparency International, December 2018

25 YEARS TRANSPARENCY INTERNATIONAL the global coalition against corruption

Part 1: Requirements

1.1 Overview

This professional standard deals with *bribery*, *corruption*, *money laundering* and *terrorist financing* and is divided into three parts:

1 Mandatory requirements for *anti-bribery* and *corruption* and for *anti-money laundering* and *terrorist financing*.

2 Guidance setting out supporting good practice for *anti-bribery* and *corruption* and for *anti-money laundering* and *terrorist financing*.

3 Supplementary guidance on some of the concepts described in parts 1 and 2.

Bribery and *corruption* mitigation controls will typically involve monitoring the activities of your own organisation. Meanwhile effective management of *money laundering* and *terrorist financing* risks involves being vigilant of the actions of outside parties that RICS-regulated firms and members may do business with, such as clients and third-party introducers.

Bribery, *corruption*, *money laundering* and *terrorist financing* are illegal and unethical. It is possible, however, that more than one of these activities can take place in a single transaction. You should be vigilant for this kind of activity both inside and outside your own organisation, with clients and third parties, and have procedures in place to identify, monitor, report and prevent it.

This professional standard defines terms used throughout in the *Glossary*. Defined terms are shown in italics when used elsewhere in the document.

1.2 Application

This professional standard applies to all RICS members and RICS-regulated firms involved with work where there is potential for *bribery*, *corruption*, *money laundering* and/or *terrorist financing*. If the standard contradicts local legislation then the legislation takes precedence.

1.3 Bribery and corruption

1.3.1 In relation to bribery and corruption **RICS-regulated firms must**:

- not offer or accept, directly or indirectly, anything that could constitute a *bribe*
- have plans in place to comply with applicable laws governing *bribery* and *corruption*, and ensure that these are followed

- *report* any activity they are aware of that breaches *anti-bribery* and *corruption* laws to the relevant authorities (as specified in local legislation); where there is no local legislation the activity should be recorded and, if possible, reported to a senior manager
- act with due diligence to perform periodic written evaluations of the risks that face the firm and that may lead to the facilitation of *bribery* or *corruption*; in determining the appropriate level of due diligence, the firm may consider the type of business activities they engage in and the environment in which they operate
- retain information detailing how the firm has met the requirements of this professional standard.

1.3.2 In relation to bribery and corruption **RICS members must**:

- not offer or accept, directly or indirectly, anything that could constitute a *bribe*
- ensure that they have *adequate knowledge* of *bribery and corruption* to be able to comply with the requirements of this professional standard
- report any activity they are aware of that breaches applicable *anti-bribery* and *corruption* laws to the relevant authorities (as specified in local legislation); where there is no local legislation the activity should be recorded and, if possible, reported to a senior manager.

1.4 Money laundering and terrorist financing

1.4.1 In relation to money laundering and terrorist financing **RICS-regulated firms must**:

- not facilitate or be complicit in *money laundering* or *terrorist financing* activities
- have systems and training in place to comply with these laws, and ensure these are followed
- *report* any suspicions of *money laundering* or *terrorist financing* activities to the relevant authorities (as specified in local legislation); where there is no local legislation the activity should be recorded and, if possible, reported to a senior manager
- evaluate and review periodically the risks that prospective and existing business relationships present in terms of *money laundering* or *terrorist financing* offences taking place
- ensure that their responses to the risks identified are appropriate, including conducting appropriate checks on clients and customers
- use *reliance* only where there is an appropriate level of confidence in the quality of the information provided by the third party – *reliance* should only be taken from third parties with standards conforming to the legal requirements, that provide the obliged market participant with a complete exchange of all legally required AML information regarding the identified party and only by confirming the identity and verification of identity of the client or counterparty in question; ultimate responsibility for the assessment of risk and actions taken based on this remain with the member or regulated firm
- take appropriate measures to understand the client and the purpose of the transaction
- verify the identity of their client by undertaking basic identity checks

- record and retain information detailing how the firm has met the requirements of this professional standard.

1.4.2 In relation to *money laundering* and *terrorist financing* **RICS members must**:

- not facilitate or be complicit in *money laundering* or *terrorist financing* activities
- *report* any suspicions of *money laundering* or *terrorist financing* activities to the relevant authorities (as specified in local legislation); where there is no local legislation the activity should be recorded and, if possible, reported to a senior manager.

Part 2: Guidance

2.1 Bribery and corruption

2.1.1 In relation to *bribery* and *corruption* **RICS-regulated firms** should:

- prepare a written policy covering *anti-bribery* and *corruption* including a risk assessment detailing the nature and impact of risk affecting the business – this policy should be reviewed and updated periodically as appropriate
- have appropriate governance and systems controls in place, proportionate to the type of work the firm does
- encourage transparency within the organisation by implementing a register including but not limited to:
  - gifts
  - hospitality, entertainment and expenses
  - customer travel and hospitality
  - political contributions
  - charitable donations and sponsorships
  - potential conflicts of interest
- provide clear guidance for staff so that they understand their role in preventing bribery and corruption and are aware that the following will not be tolerated:
  - so-called '*facilitation payments*'; although such payments may not be illegal in the local country where the payment is made, no such payments should be made without explicit authorisation from the head office
  - bribes
  - price-fixing to create a monopoly or cartel arrangement
  - failure to declare a conflict of interest
- appoint a contactable person within the company or local office to discuss compliance and ethics matters; the largest regulated firms may decide to formally appoint a local compliance and ethics champion, which is best practice for the largest regulated firms; smaller firms may still elect to make such an appointment, depending on resource implications
- publish a code of behaviour and provide this to staff
- carry out appropriate due diligence on third-party suppliers to ensure they are acting appropriately; if present in local bribery and corruption legislation then in line with their requirements.

2.1.2 In relation to *bribery* and *corruption* **RICS members** should:

- declare certain items to their employer, including but not limited to:
  - gifts
  - hospitality, entertainment and expenses
  - customer travel and hospitality
  - charitable donations and sponsorships
- attend relevant training provided by their employer or a regulator addressing *bribery* and *corruption*
- be familiar and act in compliance with their employer's policy, process and code of behaviour relating to *bribery* and *corruption*
- if in a senior management position, take a leadership role in attempting to ensure that their employer has an appropriate regime in place for addressing *bribery* and *corruption* risks.

2.2 Money laundering and terrorist financing

2.2.1 In relation to *money laundering* and *terrorist financing* **RICS-regulated firms** should:

- have a written policy addressing *money laundering* and *terrorist financing* risks that covers the following issues:
  - in high-risk situations where enhanced due diligence is required, understanding the source of funds in a transaction
  - identifying PEPs, PSCs and any potential breaches of sanctions
  - the process to be followed for *customer due diligence*
  - the situations in which simplified due diligence, standard/ordinary due diligence, or enhanced due diligence will be appropriate (see 3.6)
- have appropriate governance and systems controls in place, proportionate to the type of work the firm does
- provide appropriate, recurring training for staff, to ensure they are familiar with the risks associated with *money laundering* and *terrorist financing* and the firm's systems to counter these risks
- keep reports of suspicion of *money laundering* and *terrorist financing* activity confidential (for guidance surrounding whistleblowing see 3.11)
- identify the *beneficial owner* of a company/client involved within a transaction
- appoint a senior person to be responsible for ensuring *anti-money laundering* and *counter-terrorist financing* policies are in place and complied with.

2.2.2 In relation to *money laundering* and *terrorist financing* **RICS members** should:

- keep abreast of current training/regulation offered to them either by their employer or by a regulator addressing *money laundering* or *terrorist financing*

- comply with their employer's policy and process relating to *money laundering* and *terrorist financing*
- keep reports of suspicion of *money laundering* and *terrorist financing* activity confidential
- if in a senior management position, take a leadership role in attempting to ensure that their employer has an appropriate regime in place for addressing *money laundering* and *terrorist financing* risks.

Part 3: Supplementary guidance

3.1 Bribery and corruption risks

It is important that firms and individuals are aware of the *bribery* and *corruption* risks facing them during their normal business. Assessment of risk may start with a review of the types of risks most pertinent to the firm. Typically, such risks are broken down in a risk register and categorise the kind of industry standards that apply to the major business activities of the firm (especially accepted ways of winning and doing work).

The level of risk will often depend on the country in which business is done and the extent to which national controls are available and/or applied. Some countries and sectors give rise to a much higher risk than others (see, for example, Transparency International's *Corruption Perceptions Index* and lists of high-risk countries published by FATF). Where business is being done in countries or sectors with a higher risk, have a plan to deal with the issues this creates. It is useful to consider how information can be shared between branches and offices on a common transaction or client in order to ensure risks are properly identified.

Firms that have determined their activities give rise to very low risks of *bribery* and *corruption* require fewer controls in place than those firms with greater risks, possibly because of the range of activities they undertake, the countries they work in and the sectors in which they operate.

It is good practice for firms that consider they have higher risks to appoint a person or team to be responsible for assessing these risks, before designing and testing controls that can be put in place to mitigate against them. Those with lower risks still will need to assess their risks and monitor these for change. Periodic review is necessary to make sure the risks and the controls are still in line with the assessment.

Regardless of risk exposure, all firms are expected to have some clear rules about what is acceptable, and appropriately set limits that all their staff know and can easily access.

For firms with lower risk, very extensive policies and procedures are not necessarily needed. Reminders to staff (and agents) of what is expected in business process and a clear threshold set by those at the top of each firm will be sufficient for many firms, except those with higher risks.

3.2 Money laundering and terrorist financing risks

Money laundered funds are often 'layered' via single or a series of payments or transfers/ transactions, so that the proceeds can be hidden and used later by the perpetrator.

Typical examples include using the proceeds of crime to purchase a legal asset such as real estate, held in the name of an individual or a more complex structure, such as a legal trust

or a group of companies. The asset is held onto and eventually either used for lifestyle purposes or sold and converted into cash. This is how criminals recycle their proceeds and why firms and individuals are exposed to high risk in the property and real estate sectors.

Knowing who you are doing business with is a significant first step in countering *money laundering* and *terrorist financing*. *Know your client* (KYC) or *customer due diligence* (CDD) requirements are now common, and in many countries a legal and regulatory requirement. These establish that before taking on a new client or transaction appropriate steps are taken to ascertain who the client is and, if relevant, who the ultimate *beneficial owner* of the client is and where appropriate the counterparty. These can be relatively simple identity checks or can involve deeper investigations where circumstances require (e.g. where there is a concern over the background associations of an introducer, or where the KYC documents are not provided when asked for and without reasonable excuse). KYC or CDD procedures are a good foundation for an anti-money laundering programme for all firms.

Sometimes a transaction will include other professionals. In some limited cases, the fact that a buyer or seller has already been 'on boarded' by a lawyer or accountant may indicate that a lighter touch may be applied when carrying out steps as CDD. This is acceptable, but firms are encouraged to take a risk-based approach to each case (see 3.5). Firms and individuals should, as a minimum when assessing this risk, consider:

- the reliability of the professional
- whether the other professional is in an equivalent jurisdiction
- the nature of the transaction
- the sector the client is operating in, and
- whether there is a need to carry out enhanced due diligence (EDD) (see 3.6), such as where there is a PEP involved in the ownership or funding chain.

Other professionals in the purchase/sale cycle may also be targets for money launderers. Just because a lawyer, financier, estate agent or other surveyor are involved in the chain, this does not mean the customer, client or the transaction are legitimate. Firms and individuals should keep in mind that:

- Ultimate responsibility for risk assessment of the client and the resultant actions taken by the firm in respect to them can never be outsourced to another party.
- *Red flags* for *money laundering* ought not to be ignored.

Firms with overseas offices need to consider how they will apply a common approach to *money laundering* across their offices. There is, however, less likely to be a need for a very extensive *money laundering* programme in smaller or medium-sized firms that have local, known clients and operate in low-risk countries. This as compared to multi-service firms with overseas offices operating in countries ranked as higher risks.

Every firm will benefit from using effective training suitable for their staff and agents. Training has to be practical and accessible. Circulating anonymised *money laundering*

decisions is also a good way to familiarise staff with the issues the firm is facing in its day-to-day business.

Firms are expected to document their approach to *money laundering* and *terrorist financing*. In all but the smallest firms, presentations on at least an annual basis are expected to be made to the board/senior managers on how the firm's approach to managing these risks appears to be holding up.

It is important not to report concerns widely that can lead to 'tipping off' offences or otherwise compromise those involved. Tipping off broadly means telling or letting a client or some third party know that a report has been made to a local crime agency and/or that there is an investigation ongoing. Reports will need to be made very discreetly and to a small audience. *Money laundering* suspicions must be made to the nominated officer or person appointed internally as responsible, who can advise individuals on next steps.

3.3 Reliance

Reliance has to be considered using a risk-based approach. In instances where the client has instructed or has already passed the checks required by a regulated entity in an appropriate country, such as a law firm or large lending institution, it may be acceptable to rely on their checks of the client. This means identification of the individual reliant on the verification having been carried out by the regulated firm or institution.

This approach would not be acceptable, however, in cases where the source of funds is considered suspicious. For example, if a young, non-working individual has no cash assets but is buying a high-end apartment for the sum of millions, it would be appropriate to undertake further checks on the origin of this money. In such situations, ultimate responsibility for risk assessment of the client and the actions taken remain with the firm even if it relies on checks undertaken by a third party.

There may also be specific data protection requirements that need to be considered depending on the territory/region, such as the period of time for which a third party is required, or entitled, to hold the data being relied on.

3.4 Departures

A 'departure' is a circumstance where specific legislative, regulatory or court order needs to be followed that

differ from some of the requirements of this professional standard. RICS members and firms are expected to record such conflict(s) in writing between applicable laws and this professional standard, the deviation(s) taken from this professional standard because of the conflict(s), and any additional reporting or controls implemented based on applicable laws.

The requirement to depart from this professional standard pursuant to legislative, regulatory or court order takes precedence over all other requirements of this professional standard.

3.5 Risk-based approach

For a risk-based approach a useful starting point may be to consider 'the three Ws' – who you act for, what you are doing and why you are being asked to do something – when assessing risks to your business.

Within a risk-based approach a greater level of resource is devoted to higher risk areas, which will have been identified using a risk assessment.

A risk-based approach will involve planning to use resources in a proportionate way to target the risks in a firm. This involves assessing *bribery*, *corruption*, *money laundering* and *terrorist financing* risks before forming the plan accordingly.

3.6 Enhanced and simplified due diligence

Customer due diligence (CDD) involves collecting standard evidence to verify the identity of different types of clients. Examples include companies, trusts, special purpose vehicles, partnerships and charities.

Requirements to carry out CDD vary from country to country, but always comprise the following elements:

- identify the transacting party/parties
- verify the identification is valid and
- carry out additional checks where necessary, according to certain risk factors.

Simplified Due Diligence (SDD) means that full CDD is not needed. In a situation assessed as having a low risk of *money laundering*, applying basic verification may be appropriate. Internal policies and procedures need to set out (subject to local laws) when SDD can be applied. Evidence of the client's status may suffice, such as a check on the local company register, the status of a company, or evidence of listing on the stock exchange.

Enhanced due diligence (EDD) will need to be applied in situations (see 3.9 for the example of PEPs) where under your policies and assessments, or the applicable laws, more checking and monitoring is required to complete the client profile, requiring continued review of the client or the transaction.

It is for each firm to set up and consistently apply its approach to CDD. Some applicable laws provide when either SDD or EDD need to be utilised and this is expected to be followed. In the UK, for instance, applying SDD is now no longer an automatic option in any situation and firms need to always be alert to *red flags* that may indicate *money laundering* risks are elevated and deeper due diligence needed.

Source of funds and source of wealth checks are also closely aligned to the *money laundering* risks inherent in a transaction or from client activity. Firms need to understand how a transaction is being funded and consider whether the size and commercial sense of a particular deal matches the funding information obtained.

Some situations will warrant a check on the source of funds, such as where the source of wealth is clearly not matching the commercial factors. Information such as bank statements, trust deeds or evidence of a bonus payment may be needed and in turn may bring about further questioning.

Being familiar with when to check the source of funds and understand wealth background intimately is a function of experience and has to generally be described in a firm's procedures and in training.

Professionals need to also be mindful of the need to refresh CDD on their existing clients or customers from time to time and are expected to have a policy on this. Revisiting the information every three years may be appropriate in many situations. Risks can arise when low risk clients are taken on for a particular matter and remain 'in the system' for a much riskier transaction that follows later. The risk is then that the firm does not elevate its due diligence because the client has already passed internal, lower-threshold checks. It would be best practice to gather up-to-date identification documentation at the commencement of each new transaction, or at regular, frequent intervals if engaged in an enduring business relationship with the client (as can be common in commercial transactions).

3.7 Compliance and ethics champion

Appointing a compliance and ethics champion is potentially a very effective way to help embed systems that help detect and counter *money laundering* and *terrorist financing*, *bribery* and *corruption*. Typically, this role will be allocated to a senior manager with experience of how the business works and with visibility of a department or office. Firms constrained because of their size and/or resources, however, may not be able to elevate this function to a senior manager, but should put appropriate measures in place.

These champions can take an overview of those individual(s) responsible for CDD and ethics in a firm. They can help to promote good practice and are closer to the day-to-day risks that arise so are better able to inform senior managers of new risks and make practical

recommendations regarding suitable controls. Internal investigations too, where needed, can be managed by champions who will be an invaluable resource to internal and external lawyers or compliance professionals.

For firms with a larger resource base, there is probably a champion already responsible for CDD, so look to formalise this role as a part of an approach to *money laundering* governance. Firms constrained by resource may find champions a cost-effective way to cope with increased demand.

3.8 Code of behaviour

A code of behaviour is a formal and typically short document that enshrines a firm's commitment to good ethics and what is expected by those acting for the firm. Such

documents can set out the correct behaviour in certain situations, or who to contact in the event of an issue.

As with a number of the suggested measures, whether to have a written code of behaviour will depend on the size, complexity and locations of each firm. A one or two office firm of less than 25 people in total may not require such a document. Larger firms are expected to decide for themselves if a code of behaviour is worthwhile.

3.9 Politically exposed persons (PEPs)

PEPs are high risk from a *money laundering* and *corruption* perspective because they hold positions of influence – indeed many jurisdictions specifically legislate for this. It needs to be noted that just because an individual has been identified as a PEP does not mean that firms are expected to automatically reject their business or treat their transaction as suspicious.

A correct approach to dealing with a PEP is to have a policy that enables a PEP to be detected on a risk basis. Many firms have automated searches for all new clients (and suppliers and agents in high risk countries) which will pick up if someone is a PEP. Smaller firms may search according to pre-set risk criteria and ask the clients directly if they are PEPs.

If it is determined that a customer or client, or potential customer or client, is a PEP, this should be a *trigger* for EDD to be applied on the customer or client. As part of this process, there will then need to be a deeper assessment of the transaction type and potentially the source of funds being utilised. Decisions made around a PEP need to be documented. Senior managers are expected to be involved in deciding whether to proceed with a transaction involving a PEP as a party or if they are providing third-party funding (such as a parent funding a purchase for his or her children).

When dealing with companies or other legal entities, the same processes apply if a *beneficial owner* is a PEP.

3.10 Beneficial ownership

In the case of most entities (partnership, companies and trusts), the *beneficial owner* will be the person who ultimately owns or controls a legally defined minimum percentage of the shares or voting rights in that entity. Some laws place this at 25 per cent or more, others at 10 per cent or more. In the case of a trust, this refers to an interest of a defined minimum percentage of the capital of the trust property or – where there is no specified beneficiary – the person who controls the trust or in whose main interest this trust was set up.

The *beneficial owner* of a client organisation can be identified by requiring helpful document types to be provided, such as a recent Certificate of Incorporation or Annual Return for a company, or written confirmation from a lawyer stating who the *beneficial owner(s)* are for a trust.

3.11 Whistleblowing

Depending on their size, it may be appropriate for RICS-regulated firms to have a formal whistleblowing policy covering when and how employees should report concerns, and how such reports will be treated. In the case of SMEs, having a formal whistleblowing policy may represent a disproportionate expense and so is not a requirement. Larger firms, however, will find it difficult to justify why they do not have such a policy in place. If relevant this policy should provide guidance for whistle-blowers who face compelling local reasons (such as war, political instability and natural disasters) not to make a report through the usual channels, indicating alternative safe channels for reporting.

References

Financial Action Task Force (FATF). *Money laundering FAQ*. Available: www.fatf-gafi.org/faq/moneylaundering/ (accessed 24.10.18).

RICS (2017). *Conflicts of interest*, 1st edition.

RICS (2007). *RICS Rules of Conduct for Firms*, version 6, effective 25 April 2017. London: RICS.

RICS (2007). *RICS Rules of Conduct for Members*, version 6, effective 1 January 2013. London: RICS.

Transparency International (2017). *Corruption Perceptions Index*. Available: https://www.transparency.org/research/cpi/overview (accessed 24.10.18).

Further reading

This material does not cover important local guidance issued by national governments, supervisory authorities and regulators due to this professional standard*'s global status.*

Deloitte (2015). *Building world class ethics and compliance programs*. Available: https://www2.deloitte.com/content/dam/Deloitte/no/Documents/risk/Building-world-class-ethics-and-compliance-programs.pdf (accessed 24.10.18).

FATF (2018). *Concealment of beneficial ownership*. Available: http://www.fatf-gafi.org/publications/methodsandtrends/documents/concealment-beneficial-ownership.html (accessed 24.10.18).

FATF (2018). *Consolidated assessment ratings*. Available: http://www.fatf-gafi.org/publications/mutualevaluations/documents/assessment-ratings.html (accessed 24.10.18).

FATF (2018). *Professional money laundering*. Available: http://www.fatf-gafi.org/publications/methodsandtrends/documents/professional-money-laundering.html (accessed 24.10.18).

ISO 37001: 2016. *Anti-bribery management systems – Requirements with guidance for use*. Geneva: ISO.

OECD (2018). *OECD due diligence guidance for responsible business conduct*. Available: http// www.OECD.org/investments/due-diligence-guidance-for responsible Business conduct.htm (accessed 24.10.18).

RICS. *Conflicts of interest*. https://www.rics.org/uk/upholding-professional-standards/standards-of-conduct/conflicts-of-interest/

RICS. *Rules of conduct*. https://www.rics.org/uk/upholding-professional-standards/standards-of-conduct/rules-of-conduct/

Transparency International (2017). *FAQs on corruption*. Available: https://www.transparency.org/whoweare/organisation/faqs_on_corruption (accessed 24.10.18).

World Bank (2009). *Combating money laundering and the financing of Terrorism – A comprehensive training guide*. Available: http://siteresources.worldbank.org/FINANCIALSECTOR/Resources/CombattingMLandTF.pdf (accessed 24.10.18).

Appendices

1 These templates are intended to be helpful to RICS-regulated firms and RICS members but do not constitute formal RICS guidance. The templates are not intended to, nor should be construed as, providing a comprehensive guide to all required and/or appropriate actions.

2 These templates are relied upon at your own risk.

3 The level of relevant detail will largely depend on the type and size of the relevant firm and, to this end, this outline should be used flexibly in the context of the firm.

4 Some aspects of the template may not apply or be relevant to a particular firm.

5 It is for the RICS-regulated firm or RICS member to determine whether further detail and checks beyond those laid out in these templates are appropriate.

Appendix A

Template customer due diligence form

To: [subject of customer due diligence checks]

[For individuals]

Please provide for each an official identification document with photograph, for instance a current passport or drivers licence with recent proof of address.

[For entities other than individuals (e.g. a company, partnership or trust)]

Please provide unique identifier for the entity, for instance the company registration number or SSIP registration number.

Please provide evidence that you are authorised to act on behalf of this entity.

Please provide the address of your registered office, and if different, your principal place of business.

If you or your controlling/parent company are publicly quoted on a stock exchange, please provide proof of this. If not, please provide a structure chart disclosing the current ownership, control structure (including all entities that sit between the client and the ultimate beneficial owner) and identity of any individual/entity holding more than a defined percentage [e.g. 25%] of your voting and/or control rights.

Please provide a current excerpt from your registration documents, for instance an annual return, certificate of incorporation, certificate of good standing, articles of association, copy of the company accounts or trust document.

Appendix B

Draft of compliance checks to be carried out by firm

Those tasked with applying customer due diligence within the firm should undertake the following checks to verify the information provided by the potential customer or client in the customer due diligence form:

- meet the potential customer or client in person
- validate either a physical copy of the potential customer or client's identification documents, or a copy of them certified by an appropriate legal professional
- verify the validity of documents provided by an entity other than an individual
- check if the potential customer or client (or their ultimate beneficial owner) is a Politically Exposed Person (PEP), or a close associate or family member of a PEP
- check if the potential customer or client (or their ultimate beneficial owner) is under any relevant sanctions that would prohibit you from establishing a business relationship with them
- ascertain the purpose and intended nature of the potential business relationship and transaction
- check where the potential customer or client is principally based, and, if it is overseas, whether it is a high-risk third country
- check what the potential customer or client's principal business sector and activity is.

Based on these checks ascertain whether enhanced due diligence (EDD) checks should be applied to the potential customer or client.

Draft beneficial ownership enquiry

To: [complex or offshore structure about whose beneficial ownership you are enquiring]

[The relevant legislation] requires us to ascertain the beneficial owner(s) of the parties of a transaction, including those who trade as a company, partnership, trust or other entity (or a combination of these). Beneficial owner in practical terms means establishing the person or persons who own more than a defined percentage [e.g. 25%] of an entity as well as those who manage or control the entity if different from the owner(s).

Where we are not readily able to make our own enquiries (to establish beneficial ownership) via searching national databases of beneficial ownership, and in any of the following circumstances:

- a company is registered abroad

- there is a trust involved
- there is any type of partnership involved,

we request that you provide the necessary documents to demonstrate both your structure and, ultimately, who your beneficial owners are. Appreciating that terminology may differ, the following document types are likely to be helpful:

- **Companies:** recent Certificate of Incorporation, Annual Return or similar (detailing the identity of the shareholders) enabling us to identify the individual shareholders at the required threshold (e.g. at 25%) or more of its shares/voting rights.
- **Trust:** written confirmation provided by a lawyer (who may be a trustee) or trustee stating the identity of the beneficial owner(s) of the trust; generally these will be the beneficiaries or trustees, or if they are not yet known or are not specific individuals, then the trustees are generally treated as being the beneficial owners.
- **Partnership:** partnership deed, latest accounts, or solicitor's or accountant's letter confirming beneficial ownership.

These documents are also required for each layer of structure 'beneath' the beneficial owners.

Anti-money laundering checklist

Instruction ID: ..... **Client name**: .....

Property name: .....

Proof of ownership: National Land Ownership Registry: Lease copy:

Other: .....

Letter of authorisation to instruct (if required):

Level of due diligence (KYC): Normal: Simplified: Enhanced:

If simplified or enhanced, please explain the reasons:

.....

.....

Beneficial owners (persons)

Name: ..... Photo ID: Address proof: Online check:

Name: ..... Photo ID: Address proof: Online check:

Name: ..... Photo ID: Address proof: Online check:

Ownership structure (include entity names, % owned and hierarchy):

.....

.....

I CERTIFY THAT

I have verified the identity of the client and have seen the original documents and I can confirm that any associated photograph of the client bears a good likeness to the client AND/OR that any certified copies are signed. My AML checks have been completed according to the company's AML Policy & Procedures and I acknowledge that I am responsible for its completeness and correctness.

Negotiator's name: ..... **Signature**: .....

Office: ..... **Date**: .....

Appendix C

Template reliance letter

From: [insert name and address of person on whom you are relying]

To:

Date:

Dear [name]

[I/we] hereby acknowledge receipt of your letter dated [insert date] regarding your request to rely on [my/our] customer due diligence carried out in relation to [client] in accordance with [the relevant legislation].

In response to your request:

[I/we] [confirm/] that [I am/we are] an [estate agent] as defined by [local legislation];

[I/we] [confirm] that [I/we] have applied customer due diligence measures in relation to [client] as required under [the relevant legislation];

[I/we] consent to being relied on for the purposes set out in your letter and limited to the customer due diligence measures required by [the relevant legislation];

[I/we] [confirm] that [I/we] will retain the records relating to [my/our] customer due diligence as listed for the period required under [the relevant legislation];

[I/we] agree to make available to you as soon as reasonably practicable on request any information and copies of any identification and verification data relating to [client] [and any beneficial owner] which [I/we] obtained when applying customer due diligence measures; and

[I/we] confirm that [my/our] supervisor for money laundering purposes is/are [insert name e.g. the Commissioners for Her Majesty's Revenue and Customs] or that we follow standards equal to those maintained in EEA countries.

You agree and warrant that information we provide to you in accordance with this letter and [the relevant legislation] will be used for the sole purpose of your obligations under [the relevant local legislation of the relier] and not for any other purpose and that personal or sensitive data relating to any clients or individuals or entities provided by us to you in accordance with this letter will be treated accordingly. You also confirm you will observe all relevant data protection laws from time to time in force when processing and handing data provided.

You confirm by acceptance of this letter that we are not liable to you or any third party in relation to the confirmations in this letter or at all. Compliance with the relevant legislation is and remains your sole responsibility.

[Name of person on whom you are relying and position within the firm]