



Countering financial crime: bribery, corruption, money laundering, terrorist financing and sanctions violations

Global

2nd edition, September 2025

Effective from 17 December 2025

Countering financial crime: bribery, corruption, money laundering, terrorist financing and sanctions violations

RICS professional standard, global

2nd edition, September 2025

Effective from 17 December 2025

Published by the Royal Institution of Chartered Surveyors (RICS)

Parliament Square

London

SW1P 3AD

www.rics.org



No responsibility for loss or damage caused to any person acting or refraining from action as a result of the material included in this publication can be accepted by the authors or RICS.

ISBN 978 1 78321 557 7

© Royal Institution of Chartered Surveyors (RICS) September 2025. Copyright in all or part of this publication rests with RICS. Save where and to the extent expressly permitted within this document, no part of this work may be reproduced or used in any form or by any means including graphic, electronic, or mechanical, including photocopying, recording, taping or web distribution, without the written permission of RICS or in line with the rules of an existing licence.

This document applies globally. If any of the requirements contained in this document conflict with national legal requirements in the country or region in which the regulated member is operating, those national legal requirements take precedence and must be applied.

Acknowledgements

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

Technical author

Gillian Dixon (The Private Infrastructure Development Group)

Expert group

Co-chair: Alexander Aronsohn FRICS (International Valuation Standards Council)

Co-chair: Alex Ktorides (Bristows)

Nigel Astbury MRICS (Christie & Co)

Philip Bishop MRICS (Bouwinvest)

Giorgia Innamorato (Cocuzza)

Nigel Sellars FRICS (RICS)

Louise Shelley PhD (George Mason University)

Katarzyna Studzińska (Colliers)

Jo Upton MRICS (Pegasi)

Kalyani Vasan (Deloitte)

Ben Walker (Arrow Capital Partners)

Stephen Williams FRICS (JLL)

RICS staff

Professional standards lead: Steve Choi

Programme manager: Sara Saeed

Head of professional standards: Carys Rowlands

Editors: Jo FitzLeverson, Megan Reed and Judith Frost

Contents

Acknowledgements	ii
RICS standards framework	1
Document definitions	2
Glossary	3
Foreword	7
1 Introduction	9
1.1 Scope and application	9
1.2 Professional judgement	10
1.3 Effective date	10
2 Bribery and corruption	11
2.1 Bribery and corruption risks	13
3 Money laundering and terrorist financing	15
3.1 Money laundering and terrorist financing risks	17
3.2 Beneficial ownership	19
3.3 Accepting payments in digital currency	20
3.4 Data protection and privacy	20
4 Sanctions	21
4.1 Sanctions risks	22
5 Other considerations	23
5.1 Due diligence	23
5.2 Reliance	25
5.3 Politically exposed persons (PEPs)	25
5.4 Departures	26
5.5 Risk-based approach	26
5.6 Compliance and ethics champion	26
5.7 Code of conduct	27
5.8 Whistleblowing	27
5.9 Artificial intelligence (AI)	27

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

Term	Definition
Adequate knowledge	An appropriate understanding of the issues and responses connected to bribery, corruption, money laundering, terrorist financing and sanctions violations 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 was performed or bribe was paid or received, or the country in which a parent company is registered.
Artificial intelligence (AI)	A machine-based system that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations or decisions that can influence physical or virtual environments. Different AI systems vary in their levels of autonomy and adaptiveness after deployment. (OECD Explanatory Memorandum on the Updated OECD Definition of an AI System, March 2024, OECD Committee on Digital Economy Policy)
Beneficial ownership/owner	The natural person(s) who ultimately owns or controls a customer and/or the natural person on whose behalf a transaction is being conducted. It also includes those natural persons who exercise ultimate effective control over a legal person. (The Financial Action Task Force)
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 abuse of entrusted power, whether in the public or private sector, for private gain.

Term	Definition
Customer due diligence (CDD)/ know your customer/client (KYC)	Taking the appropriate steps to ascertain who the customer or client is and, if relevant, their ultimate beneficial owner and counterparty. These can be simple checks to verify the identity of the customer/client or might 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 a crime.
Money laundering	Concealing the source of the proceeds of criminal activity to disguise their illegal origin. This may occur through hiding, transferring and/or recycling illicit money or other currency through one or more transactions, or converting criminal proceeds into seemingly legitimate property.
Nominated reporting officer	The person nominated by a firm to receive and consider suspicious activity reports. The role holder has a legal obligation to report suspicion of money laundering to the relevant government agency or enforcement body. The role holder may also be known as the money laundering reporting officer (MLRO) or another title relevant in the role holder's jurisdiction.
Politically exposed person (PEP)	Individuals and 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.
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 judgement	The use of accumulated knowledge and experience, as well as critical reasoning, to make an informed decision.

Term	Definition
Professional money launderers	Those that specialise in enabling criminals to evade anti-money laundering and counterterrorist 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.
Proliferation financing	The act of providing funds or financial services for use, in whole or in part, in the manufacture, acquisition, development, export, trans-shipment, brokering, transport, transfer, stockpiling of, or otherwise in connection with the possession or use of, chemical, biological, radiological or nuclear weapons, including the provision of funds or financial services in connection with the means of delivery of such weapons and other CBRN-related goods and technology, in contravention of a relevant financial sanctions obligation. (Regulation 16A(9) of The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017)
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.
Sanctions	Economic and political measures that aim to influence the behaviour of a state or group of individuals. These measures can be imposed by international organisations such as the United Nations and the European Union, as well as national governments and agencies like the Office of Foreign Assets Control (OFAC).
Specially designated national (SDN)	An individual or entity located in a specific jurisdiction who is blocked due to a country or regional sanctions programme.
Suspicious activity report (SAR)	An alert made to a government agency when there is a reasonable suspicion that a transaction could involve laundering the proceeds of crime.

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 as 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.
Tipping off	A criminal offence where an individual informs a client or third party that a report has been made to a local crime agency and/or that there is an investigation ongoing. This is a criminal offence in most jurisdictions and could lead to a prison sentence.
Trade-based money laundering (TBML)	The process of disguising the proceeds of crime and moving value using cross-border trade transactions in an attempt to legitimise their illicit origins.

Foreword

Property is where life unfolds. It means homes that anchor families, offices where innovation is born and shared spaces that knit communities together. With clear standards and ethical conduct, RICS members can turn every project and transaction into a catalyst for the common good – boosting development and closing the door to financial crime.

RICS members sit at a pivotal junction. Your judgements shape markets, guide investment and build communities. When standards are strong and consistently applied, RICS members help safeguard the integrity of property markets, protect public funds and increase the resilience of communities. When standards falter, the consequences are stark: distorted markets, hollowed-out neighbourhoods and – worst of all – illicit financial flows that strip countries around the world of the resources needed for their sustainable development.

It is well established that real estate is a prime channel for laundering illicit funds. The property sector is particularly attractive to corrupt officials, their associates and organised crime networks seeking to convert dirty money into legitimate assets. Bad actors seek out opacity: complex ownership structures, cross-border layering and high-value property acquisitions that mask control and the origin of funds. But they cannot do so alone; they rely on the skills and expertise of professionals.

That is why it is imperative that the profession draws – and enforces – clear red lines.

The decisions taken by RICS members can either close or widen the door to abuse. Members who insist on clarity about a client's identity, source of funds and the purpose of a transaction help shut down schemes before they take root. Others may end up enabling financial crime.

The update to this RICS professional standard on countering financial crime arrives at a crucial moment – not because the risks are wholly new but because our understanding of them and the global consensus on how to mitigate them have grown. Around the world, there is stronger recognition that professionals in the non-financial sector are essential for preventing and detecting money laundering and illicit financial flows. Clear, robust professional standards are key to achieving that.

The new RICS professional standard is designed to strengthen professional conduct and move towards alignment with international expectations – including the risk-based approach to anti-money laundering. It is intended to complement, and in some cases exceed, local legal requirements – especially where legislation is weak, unevenly enforced or still evolving.

In daily practice, this means placing meaningful scrutiny at the centre of members' work: pausing when politically exposed persons, offshore vehicles or unnecessary complexity feature in a deal; asking questions when ownership is opaque; evidencing the source of funds and wealth; reporting suspicious activity; and refusing client requests that do not

meet the standard. It means systems that make good choices easier – clear risk assessments, robust due diligence and empowered compliance functions that equip teams to act, not merely to ‘tick the box’.

Financial crime is not an abstract risk. When professionals uphold high standards, stolen public funds are harder to launder and communities are less exposed to speculative surges powered by secrecy. When they do not, corruption and financial crime spread, and the costs are borne by the many so that a few may profit. The profession cannot be a bystander.

This standard is both an invitation and a commitment: an invitation to every RICS member to join a global effort to safeguard property markets from abuse; and a commitment that, wherever you practise, the public can rely on your integrity. Meeting that commitment, however, requires more than an individual effort. Preventing and combating financial crime demands that all actors – from other professional service providers and regulatory and law enforcement authorities to civil society – play their part.

At Transparency International, we will continue to push for stronger laws, effective enforcement, robust oversight and active public engagement, so that professionals like you can work in an environment where doing the right thing is not only possible but expected – and where those who seek to exploit the system find no easy way in.

Maíra Martini

CEO of Transparency International

1 Introduction

1.1 Scope and application

This professional standard applies globally to all RICS members and RICS-regulated firms. In cases where this standard contradicts local legislation, the legislation takes precedence.

This edition has been updated to address the evolving landscape of financial crimes, including those driven by the rise of new technologies such as artificial intelligence and the increasing use of digital currency. There has also been an increase in the use of natural resources such as gold and timber as tools for trade-based money laundering. These resources are often exploited in illegal activities like deforestation or unregulated mining to generate illicit funds, which are subsequently laundered through legitimate markets via online platforms.

RICS members and RICS-regulated firms may encounter risks relating to bribery, corruption, money laundering, terrorist financing and sanctions across various areas of professional practice. These risks can arise during property transactions such as sales and purchases, where illicit funds may be introduced into the financial system through real estate. During the lettings process, criminals may attempt to use rental properties to conceal beneficial ownership or the source of funds.

Additionally, construction and infrastructure projects can be vulnerable to corruption practices such as bribery, kickbacks and artificially inflated prices for contracts. These risks can significantly impact the integrity of a project and expose firms to legal, financial and reputational consequences. Other examples of unethical conduct may include:

- 'introduction payments', where a firm is put forward for an opportunity in return for a fee
- signing off timesheet submissions that include inflated hours and/or misrepresented personnel
- 'creative' accounting over the value of VAT payable, and
- questionable dealings relating to the granting of planning consent for developments.

These are only a few examples of how financial crime can be observed across the built environment sector. RICS members and RICS-regulated firms **must** remain vigilant, and if an unusual pattern is identified, it should be escalated through the appropriate channels within the firm.

As financial crimes continue to evolve, these updates are essential to ensure that RICS members and RICS-regulated firms remain equipped to effectively address a broad range of risks. This professional standard explains to RICS members and RICS-regulated firms how to detect, prevent and respond to emerging financial crime threats, while ensuring compliance with international regulations.

1.2 Professional judgement

The use of professional judgement is integral to the application of this professional standard. Given the complexity and evolving nature of financial crimes, all individuals working within RICS-regulated firms – whether RICS members or not – **must** make informed decisions that balance regulatory requirements with the practical realities of each situation. This approach enables effective risk assessment, tailored due diligence and appropriate responses to suspicious activities, ensuring that controls remain both robust and adaptable.

For example, in conducting periodic reviews, professional judgement allows RICS-regulated firms to determine the appropriate frequency and scope of reviews based on the risk profile and specific circumstances of each client or transaction. This ensures that resources are allocated efficiently, directed to areas of greatest potential risk to mitigate financial crime risks.

1.3 Effective date

This professional standard is effective three months after the publication date.

2 Bribery and corruption

In relation to bribery and corruption, RICS-regulated firms:

- **must not** offer or accept, directly or indirectly, anything that could constitute a bribe
- **must** have plans in place to comply with applicable laws governing bribery and corruption, and ensure that these are followed
- **must** report any activity that may give rise to suspicion that anti-corruption laws will be breached; where there is no local legislation the activity should be recorded and, if possible, reported to a senior manager
- **must** act with due diligence to perform periodic written evaluations of the risks facing the firm 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 it engages in and the environment in which it operates
- **must** document (in writing) and retain information detailing how the firm has met the requirements of this professional standard, including for the purpose of future compliance verification.

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 on, at least, an annual basis
- have appropriate governance and systems controls in place, proportionate to the type of work the firm does
- encourage transparency in the organisation by implementing a register including but not limited to:
 - gifts received or offered
 - hospitality, entertainment and expenses incurred
 - customer travel and hospitality arrangements
 - 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:
 - 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 or senior person responsible for such approval

- bribes
 - price-fixing to create a monopoly or cartel arrangement
 - failure to declare a conflict of interest (see the current edition of RICS' [Conflicts of interest](#))
- appoint a contactable person in the company or local office to discuss compliance and ethics matters. Best practice for the largest RICS-regulated firms is to formally appoint a local compliance and ethics champion; smaller firms may still elect to make such an appointment, depending on resource implications
 - publish a code of conduct for staff to follow
 - carry out appropriate due diligence on third-party suppliers to ensure they are operating in line with local anti-bribery and corruption legislation and standards where they exist.

In relation to bribery and corruption, RICS members:

- **must not** offer or accept, directly or indirectly, anything that could constitute a bribe
- **must** have adequate knowledge of bribery and corruption to be able to comply with the requirements of this professional standard
- **must** report any activity they are aware of that breaches applicable anti-bribery and corruption laws to the nominated reporting officer or senior manager(s) responsible for reporting such matters to the relevant authorities (as specified in local legislation).

RICS members should:

- declare any gifts, hospitality, entertainment, customer travel, charitable donations sponsorships or other relevant items to their employer, as required under internal policies
- 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, processes and code of conduct 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.

2.1 Bribery and corruption risks

RICS members and RICS-regulated firms:

- **must** be aware of the bribery and corruption risks they might face in the course of their regular business activities
- **must**, when conducting business in countries or sectors with a higher risk, have a plan in place to effectively address the challenges this may present.

RICS-regulated firms:

- **must** have clear rules setting out acceptable practices and appropriate limits to be made available to all staff.

Activities to help with education could include:

- conducting regular training sessions on bribery and corruption risks for all employees
- implementing and maintaining robust internal policies and procedures that address these risks and
- documenting risk assessments and the measures taken to mitigate identified risks.

Assessment of risk usually starts with a review of the types of risks most pertinent to the RICS-regulated firm. Typically, such risks are broken down in a risk register that also categorises the kind of industry standards that apply to the major business activities of the RICS-regulated 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 (for example, see the [Transparency International's Corruption Perceptions Index](#) and lists of high-risk countries published by [FATE](#)).

It is useful to consider how information can be shared between branches and offices on a common transaction or client 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.

Firms that believe their risks are higher should appoint a person or team to take responsibility for assessing the risks. The assessment should take place before designing and testing controls to mitigate the risks. Those with lower risks are advised to assess their risks on an ongoing basis and monitor these for changes.

Periodic review is necessary to make sure that the risks and the controls remain in line with the assessment. Regardless of risk exposure, all RICS-regulated firms **must** have clear rules setting out acceptable practices and appropriate limits to be made available to all staff.

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

Firms should be aware that some countries have zero tolerance for bribery committed by nationals in foreign jurisdictions, which includes bribery of foreign officials. These activities carry severe penalties for the firm, its senior managers and the individual.

3 Money laundering and terrorist financing

In relation to money laundering and terrorist financing, RICS-regulated firms:

- **must** exercise caution and **must not** facilitate or be complicit in money laundering or terrorist financing activities
- **must** have systems and training in place to comply with RICS standards and local legislation, and ensure these are followed
- **must** 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
- **must** comply with applicable anti-money laundering laws by ensuring concerns relating to money laundering are kept confidential to avoid tipping-off offences or otherwise compromising the investigation and those involved
- **must** retain confidential personal information such as identity documents and addresses securely and only for the period of retention that is strictly required to comply with anti-money laundering legislation
- **must not** ignore red flags for money laundering
- **must** evaluate and review periodically the risks that prospective and existing business relationships present in terms of money laundering or terrorist financing offences taking place, and terminate the business relationship when deemed necessary. The employee terminating the relationship **must** avoid the criminal offence of tipping off or otherwise alerting the individual or entity to the investigation or suspicion of illicit activity
- **must** in cases where a higher risk of money laundering exists (for example when there is a request for payments for real estate to be made via digital assets) carry out enhanced due diligence, which should include obtaining details of the source of funds
- **must** ensure that their responses to the risks identified are appropriate, including conducting checks on clients and customers, complying with applicable laws
- **must** use reliance only where there is an appropriate level of confidence in the quality of the information provided by the third party. Ultimate responsibility for the assessment of risk and actions taken based on this remains with the RICS member or RICS-regulated firm
- **must** take appropriate measures to understand the client and the purpose of the transaction
- **must** verify the identity of their client by undertaking identity checks, such as examining an identity document and obtaining proof of address
- **must** ensure that the supply chain is examined
- **must** record and retain information detailing how the firm has met the requirements of this professional standard

- **must** provide written terms of reference to any outsourcing (or third-party service) provider used to carry out compliance checks
- **must** be aware of and understand emerging asset classes such as digital currencies; if payments are to be tendered in digital currencies these should be referred to the nominated reporting officer
- **must** carry out appropriate customer due diligence, in a reasonable and proportionate manner based on the specific risks of each transaction, when they receive funds, including payments for the firm's fees.

RICS-regulated firms should:

- have a written policy addressing money laundering and terrorist financing risks that covers the following issues:
 - in high-risk situations enhanced due diligence should be undertaken
 - identifying PEPs, beneficial owners 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 [section 5.1](#))
- have appropriate governance and systems controls in place, proportionate to the type of work the RICS-regulated 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 RICS-regulated firm's systems to counter these risks
- keep reports of suspicion of money laundering and terrorist financing activity confidential (for guidance on whistleblowing see [section 5.8](#))
- carry out and document proliferation financing risk assessments
- ensure in real estate that appropriate checks are conducted on both buyers and sellers, particularly in jurisdictions where the risk of money laundering is higher
- identify the beneficial owner of an entity involved in a transaction
- only take reliance from third parties with standards conforming to the legal requirements, providing the obliged market participant with a complete exchange of all legally required anti-money laundering information regarding the identified party and only by confirming and verifying the identity of the client or counterparty in question
- appoint a senior person to be responsible for ensuring anti-money laundering and counterterrorist financing policies are in place and complied with
- retain evidence of the approach they have taken to money laundering and terrorist financing
- present, at least annually, to the board/senior managers setting out the effectiveness of the RICS-regulated firm's controls
- take a risk-based approach when carrying out due diligence.

In relation to money laundering and terrorist financing, RICS members:

- **must not** facilitate or be complicit in money laundering or terrorist financing activities
- **must not** ignore red flags for money laundering
- **must** 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
- **must** assess the unique characteristics and risks of each transaction to determine appropriate controls and investigative measures
- **must** avoid any potential tipping-off criminal offence or otherwise alerting the individual or entity to the investigation or suspicion of illicit activity.

RICS members should:

- keep abreast of current regulation and complete any training 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.

3.1 Money laundering and terrorist financing risks

Money laundered funds are often 'layered' via a single or 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 customer/client (KYC) or customer due diligence (CDD) requirements are now common, and in many countries are a legal and regulatory requirement. Before taking on a new client or transaction, appropriate steps should be taken to ascertain who the client is and, if relevant, who the ultimate beneficial owner of the client is and (where required by law) the counterparty to the transaction. These can be relatively simple identity checks or can involve deeper investigations where circumstances require them (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.

Ultimately, each RICS-regulated firm is responsible for its own due diligence and can be sanctioned even where reliance has been placed on another firm.

Other professionals in the purchase or sale cycle can also be targets for professional 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. RICS members and RICS-regulated firms should keep in mind that ultimate responsibility for risk assessment of the client and the resultant actions taken by the firm rests with the firm and can never be outsourced to another party. RICS members and RICS-regulated firms **must not** ignore red flags for money laundering. Failure to take appropriate action may constitute a breach of professional obligations under this standard.

Larger multi-service firms with overseas offices should consider how they will apply a common approach to money laundering across their offices. There is, however, less likely to be a need for an extensive money laundering programme in smaller or medium-sized firms that have local, known clients and operate in low-risk countries.

Training should be practical and accessible. Circulating anonymised money laundering decisions is a good way to familiarise staff with the issues the firm is facing in its day-to-day business. All firms, whether RICS-regulated or not, will benefit from effective training suitable for their staff and agents. RICS-regulated firms should retain evidence of the approach they have taken to money laundering and terrorist financing. In all but the smallest firms, presentations, at least annually, should be made to the board/senior managers setting out the effectiveness of the firm's controls.

Firms **must** comply with applicable anti-money laundering laws by ensuring concerns relating to money laundering are kept confidential to avoid tipping-off offences or otherwise compromising the investigation and those involved. This legal obligation applies to all firms, including RICS-regulated firms. RICS members and RICS-regulated firms **must** ensure that reports are made discreetly and to a small audience. Money laundering suspicions **must** be made known to the nominated reporting officer or person appointed internally as responsible, who can advise individuals on next steps.

3.1.1 Trade-based money laundering (TBML)

TBML can be difficult to detect, but RICS-regulated firms should be vigilant as this often occurs with high-value items. In real estate, this can occur where the organisation is requested to reissue an invoice and/or refund monies paid. Often the invoice will be addressed incorrectly, or funds received will be over- or underpaid.

RICS-regulated firms should take a risk-based approach to these matters, where applicable, and the compliance function (or those who hold responsibility for compliance activities) should be made aware when these issues arise so that appropriate checks can be carried out. Firms should ensure that their employees are familiar with TBML and that training is appropriately deployed to ensure that the firm is not inadvertently complicit in TBML.

3.1.2 Terrorist financing

The risk of terrorist financing is increasing at a significant level, and therefore RICS-regulated firms **must** ensure that they exercise caution. Terrorist financing involves the provision, collection or receipt of funds with the intent or knowledge that the funds will be used to carry out an act of terrorism or any act intended to cause death or serious bodily injury.

RICS-regulated firms **must** ensure that the supply chain is examined to prevent the facilitation of terrorist financing, and appropriate customer due diligence **must** be carried out when RICS-regulated firms receive funds, including payments for the firm's fees.

The [United Nations Security Council Resolution 2195](#) identified the following crimes that support terrorism:

- trafficking of arms, persons, drugs and artefacts, and
- from the illicit trade in natural resources including gold and other precious metals and stones, minerals, wildlife, charcoal and oil.

RICS-regulated firms should assess the source of funds they receive, especially where there may be an increased risk of links to these types of illicit activity. This may include verifying the identity of the payer, the legitimacy of the funding source and whether any red flags are present, such as payments from high-risk jurisdictions. RICS-regulated firms should ensure that this due diligence is proportionate to the level of risk.

3.2 Beneficial ownership

In the case of most entities (partnerships, 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% or more, others at 10% 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 certain documents 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.

3.3 Accepting payments in digital currency

There is an increasing trend in payments for real estate being made via digital assets, particularly cryptocurrencies. RICS-regulated firms **must** carry out enhanced due diligence when there is a request for funds to be paid in this way. This includes verifying the legitimacy of the transaction, the source of funds and compliance with relevant regulations to mitigate potential risks associated with money laundering and terrorist financing. RICS-regulated firms should be aware that digital currency is often used in funding terrorist groups.

Due diligence **must** be applied in a reasonable and proportionate manner, based on the specific risks of each transaction. Where practicable, RICS-regulated firms should verify the origin of digital assets and the identity of beneficial owners. RICS members in non-regulated firms are encouraged to apply professional judgement and uphold ethical standards but are not personally mandated to conduct enhanced due diligence under this professional standard if they are not required to do so by their employer.

Professional judgement is essential in determining the appropriate level of scrutiny. Given the evolving nature and complexity of digital assets, RICS members and RICS-regulated firms **must** assess the unique characteristics and risks of each transaction to determine appropriate controls and investigative measures.

3.4 Data protection and privacy

RICS-regulated firms are required to comply with data protection legislation applied in their jurisdiction. RICS-regulated firms should implement appropriate safeguards to protect client information and comply with privacy requirements set forth by applicable data protection legislation. Confidential personal information such as identity documents and addresses **must** be retained securely and only for the period of retention that is strictly required to comply with anti-money laundering legislation.

4 Sanctions

In relation to sanctions, RICS-regulated firms:

- **must not** engage in business transactions with specially designated nationals (SDNs) in any jurisdiction where the firm carries on any business relationship and may be subject to sanctions
- **must** implement effective systems and controls to avoid engaging in business relationships with SDNs
- **must** provide adequate training to employees on sanctions compliance
- **must** evaluate and review periodically the risks that existing business relationships present in terms of sanctions and
- **must** carry out adequate due diligence screening to ensure that business relationships do not breach sanctions legislation.

RICS-regulated firms should:

- adopt a written policy addressing matters relating to sanctions and the risks that non-compliance poses to both the firm and any individual who might engage in or facilitate prohibited dealings with sanctioned entities or persons
- establish appropriate governance and systems controls, proportionate to the firm's specific activities and the type of work it does
- provide appropriate, recurring training for staff to ensure they are familiar with the risks associated with sanctions and the firm's systems to counter these risks
- appoint a senior person to be responsible for ensuring sanctions policies are in place and complied with.

In relation to sanctions, RICS members:

- **must** conduct appropriate checks to ensure that they do not carry on any business relationships with SDNs.

RICS members should:

- keep abreast of current regulations and attend any sanctions training offered by their employer
- comply with their employer's policy and processes relating to money laundering, terrorist financing and sanctions.

4.1 Sanctions risks

Globally, there has been a significant increase in financial sanctions since 2014. Financial sanctions have broader implications. Historically, they applied to banks and other financial institutions, but other sectors, such as the real estate sector, now engage in the same transactions. Non-compliance can result in severe sanctions and penalties for the firm.

If an RICS member, or an individual working for an RICS-regulated firm, suspects a person with whom a firm is carrying on business is an SDN, they should seek advice from senior management.

5 Other considerations

5.1 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.
- Carry out additional checks where necessary, according to certain risk factors.

5.1.1 Simplified due diligence

Simplified due diligence (SDD) means that full CDD is not needed. In a situation assessed as having a lower risk of money laundering, applying basic verification may be appropriate. Internal policies and procedures should set out (subject to local laws) when SDD can be applied. Examples of where SDD is appropriate might include local councils, registered charities and companies listed on a recognised stock market.

Importantly, the obligation to report suspicious transactions remains in place, even when SDD is applied. RICS members and RICS-regulated firms **must** continue to assess all transactions with professional judgement and report any suspicious activity in accordance with applicable regulations.

5.1.2 Enhanced due diligence

RICS-regulated firms **must** apply enhanced due diligence (EDD) in situations (see [section 5.3](#) for the example of PEPs) where, under the RICS-regulated firm's 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.

EDD is required when clients, the transactions or the jurisdiction(s) present a higher risk of money laundering.

It is for each RICS-regulated firm to set up and consistently apply its approach to CDD. Some applicable laws provide for when either SDD or EDD **must** be utilised. In the UK, for instance, applying SDD is no longer an automatic option in any situation, and firms **must** be alert to red flags that may indicate money laundering risks are elevated and deeper due diligence is 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. It is important for RICS-regulated firms 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 does not match the commercial factors. Information such as bank statements, trust deeds or evidence of a bonus payment might be required 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 should generally be described in an RICS-regulated firm's procedures and in training.

Professionals, including RICS members and those working with RICS-regulated firms, should be mindful of the need to refresh CDD on their existing clients or customers from time to time and should 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 higher-risk transaction that follows later. The risk is then that the RICS-regulated firm does not elevate its due diligence because the client has already passed internal, lower-threshold checks. It is 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).

5.1.3 Electronic verification

Technology has evolved significantly and can improve the speed, quality and efficiency of due diligence. Using these solutions will also improve accuracy and identify areas of concern. Passports can be authenticated more easily, and facial recognition technology provides assurance in proving the authenticity of an individual. Many of these solutions can confirm the address of individuals, eradicating the need for a utility bill as proof of address.

These solutions can be costly and therefore may not be practicable where there are budget constraints.

5.1.4 Due diligence outsourcing

It is permissible for firms in general to outsource their due diligence to a reputable service provider. However, RICS-regulated firms **must** provide the outsourcing provider with written terms of reference to ensure that both parties are clear as to their responsibilities. For example, this should include details of who can sign off at each stage of the process and triggers that will require approval from a senior manager within the firm. It is important to emphasise that while outsourcing may be employed to manage certain due diligence tasks, the ultimate responsibility for filing a suspicious activity report (SAR) rests with the firm. The firm, including RICS-regulated firms, remains accountable for ensuring that any suspicious

activity is properly identified and reported, regardless of the involvement of third-party service providers.

5.2 Reliance

Reliance should 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, such as a law firm or large lending institution, it may be acceptable to rely on those checks. This means identification of the individual is reliant on the verification that has been carried out by the regulated entity.

However, this approach would not be acceptable 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 remains with the RICS-regulated firm even if it relies on checks undertaken by a third party.

There are some jurisdictions, such as the UK, where reliance can be placed on the due diligence undertaken by another party, provided it meets regulatory requirements.

5.3 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 is important to note that an individual identified as a PEP does not automatically require firms to 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) that 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 to the customer or client. As part of this process there should be a deeper assessment of the transaction type and potentially the source of funds being utilised. RICS-regulated firms should document decisions made about a PEP. 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 children).

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

5.4 Departures

A 'departure' is a circumstance where specific legislative, regulatory or court orders differ from some of the requirements of this professional standard.

RICS members and RICS-regulated firms **must** record in writing:

- conflict(s) 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.

5.5 Risk-based approach

For a risk-based approach, start by considering 'the three Ws':

- **who** you act for
- **what** you are doing, and
- **why** you are being asked to do something.

In a risk-based approach, a greater level of resources 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.

5.6 Compliance and ethics champion

Appointing a compliance and ethics champion is an effective way to 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 visibility of a department or office. RICS-regulated firms constrained because of their size and/or resources 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 promote good practice and are closer to the day-to-day risks that arise. They are therefore 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 may already be a champion responsible for CDD, and this role should therefore be formalised as part of an approach to money laundering governance. Firms constrained by resources might find champions a cost-effective way to cope with increased demand.

Compliance and ethics champions might find the [World Economic Forum's Partnering Against Corruption Initiative's workstream Gatekeepers advancing integrity and transparency](#) useful in their work.

5.7 Code of conduct

A code of conduct is a formal and typically short document that enshrines a firm's commitment to good ethics and what is expected of those acting for the firm. Such documents can set out the correct conduct in certain situations and whom to contact in the event of an issue.

As with a number of suggested measures, whether to have a written code of conduct will depend on the size, complexity and location(s) of each firm. However, where an RICS-regulated firm determines that a code of conduct is appropriate, it should publish a code of conduct outlining expected behaviours, ethical standards and procedures for reporting concerns, and should support staff in meeting their professional responsibilities.

5.8 Whistleblowing

Depending on 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 small or medium-sized firms, having a formal whistleblowing policy may represent a disproportionate expense and so is not a requirement. However, larger firms will find it difficult to justify why they do not have such a policy in place.

If relevant, this policy should provide guidance for whistleblowers 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.

Regardless of size, every RICS-regulated firm should encourage a culture of openness and provide their employees with the opportunity to speak up.

5.9 Artificial intelligence (AI)

AI is being used to an increasing extent and can be effective in reducing the risk of financial crime. For example, through the use of large datasets, AI can aid the detection of suspicious activity, the reduction of false positives during the screening process and the automation of complex investigations.

It is important to bear in mind that while AI can be used in the reduction of financial crime, it is also used by the perpetrators of criminal activity; for example, the use of deep fakes for

impersonation exacerbates identity theft. Therefore, RICS-regulated firms should employ efforts to stay ahead of emerging threats.

RICS-regulated firms should consider the following benefits of AI:

- improving customer due diligence processes through better automation and digitisation
- identifying the authenticity of its clients and other counterparties involved in the transaction
- streamlining operations for greater efficiency, and
- reducing false positives when carrying out due diligence exercises.

While AI can significantly improve compliance efforts, it can be costly to implement and therefore may not be appropriate for all RICS-regulated firms. Each RICS-regulated firm should consider the feasibility and scale of AI adoption based on their resources and specific business needs.

Delivering confidence

We are RICS. As a member-led chartered professional body working in the public interest, we uphold the highest technical and ethical standards.

We inspire professionalism, advance knowledge and support our members across global markets to make an effective contribution for the benefit of society. We independently regulate our members in the management of land, real estate, construction and infrastructure. Our work with others supports their professional practice and pioneers a natural and built environment that is sustainable, resilient and inclusive for all.

Enquiries
contactrics@rics.org



[rics.org](https://www.rics.org)