TRADING & SUPPLY
KNOW YOUR COUNTERPARTY (KYC) STANDARDS

August 2021

CONTENTS

VERSION CONTROL

Document name	Version	Date	Comments
KYC Standards	V1.0	09/08/2019	First draft of Standards issued, replacing Financial Crime Counterparty Due Diligence Operational Procedures November 2018
KYC Standards	V2.0	01/11/2019	Revised Standards issued in final
KYC Standards	V3.0	1/02/2021	Annual review 2020 for formal adoption by 1 April 2021
KYC Standards	V3.1	01/04/2021	Final version of annual 2020 refresh (minor wording changes – see Change Control Log Appendix 9)
KYC Standards	V3.2	13/08/2021	Minor wording changes within the glossary (See Change Control Log Appendix 9)

1. INTRODUCTION

1.1. Overview

Under the Trading and Supply ("T&S") Financial Crime[1] Policy, T&S is required to undertake risk based Know Your Counterparty ("KYC") measures on its counterparties and their related parties.

The references within this document to "T&S" shall be a reference to the Shell Trading and Supply organisation, as a business unit within the Royal Dutch Shell plc ("RDS") Group, or to each separate legal entity and Business Line within the Shell Trading and Supply organisation, as the context requires.

Documented KYC Standards are an important component of the Financial Crime risk management framework and ensure that T&S complies with applicable Financial Crime regulations as well as helping to prevent the organisation from being used to facilitate Financial Crime.

These KYC Standards (hereafter referred to as "Standards") set out the minimum, mandatory KYC requirements to be applied across T&S. This document may also be referred to as KYC Guidelines under the T&S Compliance Framework.

1.2. Objective

The objectives of these Standards are to:

- support the implementation of the T&S Financial Crime Policy by describing the minimum, mandatory KYC measures required to be undertaken by T&S in relation to its counterparties and business activities;
- provide guidance to enable a consistent interpretation and approach to KYC across T&S in applying the Financial Crime Policy requirements; and
- enable T&S to manage its Financial Crime exposure in accordance with its risk appetite.

1.3. Application

These KYC Standards must be complied with by all individuals or entities that establish business relationships[2] or undertake transactions with counterparties (as defined in these Standards) on behalf of T&S, that fall into the following categories:

[1] T&S has defined Financial Crime as any offence related to money laundering, terrorist financing, sanctions, bribery and corruption, tax evasion, fraud and the proceeds of crime from market abuse.

[2] A business, professional or commercial relationship between T&S and a counterparty, which (a) is connected to the business of Shell and (b) is expected by Shell, at the time when contact is established, to have an element of duration.

- all employees, including contractors and temporary staff (hereafter defined as "employees");
- all Business Lines and legal entities which form the T&S organisation; and
- all suppliers of outsourced services performing relevant functions or KYC measures on behalf of T&S.

Where there are conflicts between these Standards and applicable local regulations, the impacted T&S entity must ensure that it complies with local regulations in all cases. In these cases, a formal exception must be requested per the requirements set out within section 18.1 of these Standards.

1.4. Roles and responsibilities

Set out below are the key roles and responsibilities outlined within these KYC Standards:

Person	Role	Responsibility
T&S Money Laundering Reporting Officer ("MLRO")[3]	Owner of these Standards.	▪ Approves these Standards and any subsequent changes.
Head of Financial Crime and Deputy MLRO	Oversees the maintenance and implementation of these Standards.	▪ Undertakes an annual review of these Standards; ▪ Proposes updates to these Standards to reflect relevant changes in applicable Financial Crime regulations, laws, industry guidance or changes in the T&S Financial Crime risk appetite; and ▪ Oversees updates and amendments to these Standards.
Compliance Financial Crime Team, within the Second Line of Defence ("LOD2"), (hereafter referred to as the "FC Team")	Supports the maintenance of these Standards and implements the requirements of these Standards, as applicable through operating procedures.	▪ Implements operating procedures to comply with these Standards where applicable; ▪ Advises the Business Lines on the application of these Standards, in consultation with the Head of Financial Crime; and ▪ Proposes applicable updates to these Standards to reflect relevant changes in applicable Financial

[3] The MLRO is also the Chief Compliance Officer for T&S.

Person	Role	Responsibility
		Crime regulations, laws or industry guidance.
T&S Executive Vice President ("EVP") and Business Line Vice Presidents ("T&S VP")	Understands and communicates the requirements of these Standards to drive a culture of compliance within the Business Lines.	▪ Ensures that the T&S Business Lines comply with their Financial Crime responsibilities as set out in these Standards.
T&S Business Lines, within the First Line of Defence ("LOD1") e.g. Crude, Products, Energy, Shipping and Maritime, Distribution Operations, Commercial Operations and relevant central functions	Implements the requirements of these Standards, as applicable through operating procedures.	▪ Implements processes and operating procedures to comply with these Standards, where applicable; ▪ Ensures that KYC measures are undertaken on all relevant counterparties and business activities in line with these Standards; ▪ Undertakes Initial Due Diligence ("IDD") and supports the Financial Crime risk assessment of all relevant counterparties; and ▪ Ensures that third parties performing KYC on their behalf (where applicable), comply with these Standards.

1.5. Employee responsibility

Every T&S employee must understand the Financial Crime risks relevant to their role and how to manage them. All employees of T&S must seek advice from the FC Team, when unclear on the requirements within these Standards. The relevant Business Line or any central function must make sure that any third party contractors, agents or consultants that perform KYC-related activities on their behalf are aware that they are bound by the responsibilities within these Standards and that they should act accordingly. It is the duty of all T&S employees to report any suspected breach of these Standards.

1.6. Related documentation

These Standards must be read in conjunction with the T&S Compliance Manual, the T&S Financial Crime Policy, other related T&S Compliance policies and guidance and any other

associated Royal Dutch Shell ("RDS") Group Policy including, but not limited to the RDS Ethics and Compliance Manual and the RDS Code of Conduct.

The KYC Standards set out the minimum mandatory requirements to be followed when applying KYC measures and do not replace any other requirements mentioned in the above documentation nor additional counterparty onboarding requirements mandated elsewhere within T&S for example, those related to finance, tax or credit.

In addition, these Standards must be supported by processes and procedures or instructions to operationalise the requirements herein. Relevant Financial Crime documents are stored on the T&S Compliance SharePoint site.

2. HOW TO USE THE KYC STANDARDS

As set out in section 1, these Standards are mandatory and must be applied to all counterparties across T&S, unless an exception or deviation has been provided as set out in section 18. The specific KYC requirements to be applied will depend on the counterparty's Financial Crime risk, legal form and the business activity being undertaken with them, which must be understood.

These Standards should be used to understand the requirements in relation to:

- the definition of a counterparty and the different levels of due diligence applied within the KYC process, as set out in section 4 & 5;
- identifying and where required, verifying counterparty related parties, as set out in section 6;
- identifying and where required, verifying Ultimate Beneficial Owners ("UBO") and Ultimate Controllers, as set out in section 7;
- screening requirements for counterparties and related parties, as set out in section 8, with additional guidance in section 10;
- risk assessing and understanding Politically Exposed Persons ("PEP"), as set out in section 9;
- performing Ongoing Due Diligence ("ODD"), as set out in section 12;
- documenting the Financial Crime risk assessment and risk rating of counterparties and understanding approvals, as set out in section 13; and
- exiting or suspending a counterparty relationship, as set out in section 14.

A decision tree to assist users of this document in further understanding how to apply these Standards is contained in Appendix 1.

3. ACCOUNTABILITIES AND RESPONSIBILITIES

3.1. Introduction

As set out in the Financial Crime Policy, effective Financial Crime risk management involves ensuring that responsibilities and accountabilities for Financial Crime controls are apportioned appropriately and are clearly defined and documented across T&S. These Standards support the Financial Crime Policy through setting out the accountabilities and responsibilities in relation to KYC.

Sections 3.2 to 3.4 set out an overview of the accountabilities and responsibilities applied across the three lines of defence within T&S.

3.2. Line of Defence One ("LOD1")

LOD1 (the relevant Business Line) is accountable for the Financial Crime risk of its counterparties and business activities undertaken with them, including the performing of KYC measures in accordance with these Standards, and is required to:

- create operating procedures to implement the requirements of these Standards insofar as they relate to Business Line responsibilities;
- conduct IDD and obtain KYC documentation and information in line with the requirements set out in these Standards;
- undertake all outreach with a counterparty in relation to KYC documentation and requirements;
- monitor business and counterparty activities to ensure that trigger-based re-reviews of a counterparty's KYC information and Financial Crime risk profile are undertaken in line with section 12 of these Standards; and
- identify scenarios which require an exception and/or deviation in line with section 18 of these Standards.

3.3. Line of Defence Two ("LOD2")

The FC Team sits within the T&S Compliance function in LOD2 and is accountable for providing independent oversight of LOD1 in relation to their Financial Crime risk management activities and is responsible for:

- documentation of and maintenance of these Standards;

- providing advice and guidance to LOD1 in relation to Financial Crime related activities or issues;

- communication and training in relation to the Financial Crime Policy and these Standards;

- performing certain requirements within these Standards on behalf of the Business Lines, including review and analysis of KYC information and documentation, counterparty Financial Crime risk assessment and risk scoring, counterparty screening and screening alert dispositioning, and counterparty Financial Crime risk approvals;

- conducting assurance over LOD1 activity;

- review and approval of any requested exceptions or deviations;

- approving any remedial actions required in the event of a breach of these Standards; and

- escalation of any applicable High Risk counterparty to the High Risk Counterparty Committee ("HRCC") for review and approval.

3.4. Line of Defence Three ("LOD3")

The LOD3 within T&S comprises Shell Internal Audit ("SIA"), who are responsible for undertaking risk-based and periodic independent reviews of T&S's KYC control framework and T&S's compliance with the Financial Crime Policy and Standards. The results of all independent reviews, including any identified issues, must be reported to the MLRO and Head of Financial Crime. Any remedial actions required to address any identified issues will be the responsibility of the applicable Business Line or LOD1 or LOD2 function.

4. PRINCIPLES OF KNOW YOUR COUNTERPARTY ("KYC")

4.1. Introduction

This section sets out the key KYC principles applied by T&S in relation to its counterparties and other parties, both at the point of onboarding and throughout the business relationship.

4.2. Financial Crime risk appetite

T&S will not establish nor maintain relationships with counterparties, or related parties, nor offer products or services, where a counterparty business relationship falls outside of the T&S Financial Crime risk appetite or where it is prohibited by applicable laws and regulations. The T&S Leadership Team ("TSLT") retains the right to determine and amend the T&S Financial Crime risk appetite where required, for example, to reflect new regulatory requirements or where an activity is deemed to present unmitigated Financial Crime risk.

T&S employees must:

- not enter into a business, commercial or contractual relationship or commitment with a counterparty that has not been subject to KYC measures and approvals, where applicable, as set out in these Standards;
- not engage in any activity which involves individuals, entities or countries that violate any Financial Crime regulations, including sanctions;
- ensure all necessary approvals are in place before engaging in any activities or negotiations with any sanctioned individual, entity or country; and
- not deal in products or markets that are prohibited, as defined by the T&S Financial Crime risk appetite.

Where a prospective counterparty or business activity is identified as outside the T&S Financial Crime risk appetite, the counterparty relationship must be declined. Where this relates to an existing counterparty, the counterparty must be referred to the HRCC who will confirm the steps required to either exit the relationship or for any trading restrictions or suspensions to be applied. Section 14 of these Standards sets out further information to be applied to the decline or exit of a counterparty relationship.

4.3. What is KYC?

KYC is the due diligence and monitoring measures undertaken to ensure that:

- T&S confirms that a counterparty (as defined by these Standards) is who they claim to be and that any related parties are identified, and where required, verified;

- T&S establishes the purpose and intended nature of the relationship to enable effective monitoring of a counterparty's transactions and to confirm that activity is in line with their expected activity; and

- a business relationship or transaction with a counterparty is in line with the T&S Financial Crime risk appetite and is not prohibited by applicable Financial Crime laws and regulations.

KYC is not a one-off exercise to collect documents in relation to a counterparty and its related parties. All documentation and information gathered should be assessed to enable T&S to understand the potential Financial Crime risk posed by a counterparty in order to decide whether to commence or continue business with a counterparty in the context of risk appetite.

4.4. Who is a counterparty?

A counterparty for the purposes of these Standards is any party:

- with whom T&S establishes a business relationship, defined as a commercial or contractual agreement to buy/sell a commodity/asset[4], or with whom T&S enters a trade or supply arrangement (e.g. bilateral or multilateral agreements);

- to or from whom T&S sells or buys a service or product, e.g. through a sales office; and

- from whom T&S procures ancillary services[5] in relation to trading and supply activity, including, but not limited to:

    - Shipping, maritime and marine services, including lightering, expeditors and vessel charterers and operators;
    - Non-shipping transportation (rail/road/container/barge/other inland);
    - Brokers, agents, consultants, intermediaries[6] and introducers, including Business Development consultants used to support T&S business opportunities;
    - Storage/terminalling providers;
    - Cargo inspectors;
    - Pipelines, wires, grid and transmission operators needed to physically move commodities;

[4] Including mergers and acquisitions ("M&A") deal activity or another one-off asset purchase/sale.
[5] Ancillary services are products/services directly attributable to a specific T&S counterparty or transaction, or the supply or trade of commodities.
[6] Note, where agents and intermediaries are classified as Government Intermediaries ("GI") i.e. they interact with government officials, they are also subject to specific ABC requirements as set out in the RDS Ethics and Compliance Manual owned by the Shell Ethics and Compliance Officer ("SECO").

- Subcontractors engaged directly by T&S to perform any of the above services[7]; and
- Financing or credit providers e.g. banks and other financial institutions ("FI") used for trade finance or commodity based lending transactions.

All parties listed above, including those onboarded by T&S functions, including Contracts and Procurement, are considered to be a T&S counterparty and are subject to these Standards.

4.5. Counterparties subject to SECO Due Diligence process

Certain T&S businesses e.g. Commercial Fuels and Hydrocarbon Deal Making counterparties within Products, certain Shipping and Maritime ("S&M") counterparties and both Distribution Operations and Commercial Operations ("Operations") counterparties, are currently subject to the due diligence requirements prescribed by SECO. This includes the Group Screening Service ("GSS") process and associated escalations and approvals.

Where the GSS process results in a potential Financial Crime red flag (either from self-service screening, or enhanced screening Amber or Red reports) that requires further investigation and mitigation, the T&S Business Line must escalate the findings to the relevant Counterparty Onboarding Focal Point ("COF") team for review. The COF should consult with the FC Team where needed to assess the relevance of a red flag.

Where a Financial Crime red flag is confirmed, the counterparty must be subject to the application of full T&S KYC measures as set out in these Standards.

NB. If a T&S counterparty is registered in an EDD country (as defined by the FC Team), or is identified as requiring enhanced GSS screening, the use of GSS is no longer permitted. The counterparty must be escalated by the T&S Business Line to the relevant COF to be onboarded in line with these T&S KYC Standards.

4.6. General and Administrative ("G&A") and other vendors

Vendors from whom T&S purchases products and services for general business and office activities, but where these costs are not directly attributable to a specific counterparty or transaction, or the supply or trade of commodities, are referred to for the purposes of these Standards, as G&A vendors.

Examples of G&A vendors that are used by T&S are:

- General office supplies.

[7] Note, subcontractors/third parties engaged by T&S counterparties are not subject to T&S KYC measures unless there is a direct contractual or transactional relationship with T&S or where they act as a representative of T&S (e.g. Direct GIs).

- Real estate rent or leasing costs as well as office real estate maintenance and services.
- Professional services (general legal, accountancy, auditing, HR, consultancy).
- IT, database and technology licences/subscriptions for general use e.g. weather forecasting, counterparty due diligence, vessel screening and tracking.
- Sales and marketing costs (other than business consultants/introducers).
- Market and other research providers.
- General HSSE, inspection and insurance costs.
- Equipment rental providers.
- Suppliers of spares, consumables including additives, dyes and other specialist chemicals used by T&S.
- Parties to whom we pay mandatory licences/fees/memberships required to operate T&S business e.g. regulators, tax authorities, tender administrators.

T&S also uses other vendors for distribution, logistics and terminal, pipeline or shipping maintenance and operations within T&S. Examples of other vendors used primarily by S&M and Operations include:

- Terminal, pipeline and ship maintenance service providers.
- Spare parts and consumables for terminals, pipelines and vessels.
- Construction and demolition services.
- Engineering, operational and HSSE inspection and consulting services for terminals, construction, pipelines and vessels

Vendors are not typically set up in T&S trading systems, other than for information/modelling purposes, and, unless otherwise noted in section 4.4 above, are currently required to follow the SECO due diligence process.

Where they are required to be set up in T&S trading systems, or where they are onboarded via the T&S KYC process, vendors must be subject to BDD at a minimum.

BDD may be applied to vendors, regardless of jurisdiction of the counterparty, other than where the vendor is registered in a Generally Embargoed Country ("GEC") in which case, the T&S Trade Compliance Team ("TC Team") must be consulted before proceeding.

If potential Financial Crime red flags are identified from the SECO due diligence or T&S BDD process in relation to vendors, the T&S Business Line must escalate the findings to the relevant COF team for review. The COF should consult with the FC Team where needed to assess the relevance of a red flag.

Where there are confirmed Financial Crime red flags, the Business Line must consult with the FC Team for approval of these before proceeding with any business activities. The Head of Financial Crime (or delegate) is authorised to determine whether further KYC measures and risk

mitigations and/or escalation to the Chief Compliance Officer or HRCC are required, prior to proceeding.

Business Lines must ensure controls are in place to ensure that trading activity is not undertaken with vendors, without the correct KYC measures being applied in line with these Standards.

4.7. Financial trading: who is the counterparty?

Certain legal entities within T&S e.g. STASCO, SIETCO, trade both exchange-traded[8] products and financial products between parties 'over-the counter' ("OTC"). Trading may or may not result in physical delivery of the product, depending on the nature and terms of the trade.

Firms may deal in exchange-traded products as principal or as agent. In the financial and commodity derivatives markets, T&S deals as principal (other than where it acts as agent for other T&S entities e.g. STASCO acts as an agent for SEEL and STIL). Most exchanges have a Central Counterparty ("CCP") which stands between the exchange members that are buying and selling a product (becoming the buyer to the seller and the seller to the buyer). Where an exchange or trading platform does not have a CCP, the members contract directly with each other e.g. for T&S, this includes the Chinese Emission Exchanges.

OTC products may be bilateral agreements or multilateral agreements, depending on the settlement process, that are not traded or executed on an exchange. The terms of the agreement are tailored to meet the specific needs of the parties, i.e., there are not necessarily standardised terms, contract sizes or delivery dates. Where firms deal OTC, they usually deal as principal, and financial settlement is between the parties. OTC financial products can in some instances be submitted for clearing by a CCP.

Exchange-traded products are usually traded in a transparent manner on regulated markets, or between regulated parties (with other regulated parties or their clients) and typically pose lower inherent money laundering risk due to market transparency and the involvement of a CCP as a financial intermediary. OTC business will, generally, be less transparent.

When conducting KYC measures in relation to counterparties involved in financial trading, the following principles should be applied.

- Where T&S negotiates, contracts and/or transacts directly with a trading counterparty (OTC or exchange-traded), or where the counterparty takes physical delivery of products, the counterparty is subject to full KYC in line with these Standards;

[8] Exchange-traded products are financial products that are traded on exchanges e.g. Brent or Henry Hub futures traded on ICE or NYMEX regulated exchanges, which have standardised terms (e.g. amounts, delivery dates and terms) and settlement procedures and transparent arrangements. They can be traded through the exchange trading screen or, under specific rules, negotiated bilaterally between parties and registered on the exchange.

- Where T&S transacts on an anonymous central order book on a regulated market, and where the transactions are cleared centrally by a CCP, KYC is only required on the exchange, the CCP, and on any clearing member providing clearing/execution services to T&S. KYC is not required on the exchange member with whom we are matched, unless instructed by SECO or T&S Compliance due to Financial Crime risk concerns regarding the exchange's membership admission criteria and adequacy of Financial Crime controls based on the risk assessment of the exchange;

- Where an exchange-based trade is randomly, anonymously and automatically matched with an equal and opposite exchange trade, and a CCP is not used to match and settle the trades (i.e. we settle directly with the matched counterparty), KYC is required on the exchange member/trading counterparty, even if the name is not known until settlement e.g. Chinese Emission exchange members traded with by SIETCO, who are eligible for BDD as set out in section 5.3.1 of these Standards. BDD is undertaken on all exchange members at the point they are added to the exchange;

- The exchange/CCP must always be subject to KYC in line with these Standards; SDD may be applicable depending on the jurisdiction of the exchange and its regulated status;

- As part of KYC on the exchange, Business Lines, in consultation with the Compliance Team must document the risk associated with trading on the exchange e.g. what value can be placed on the exchange's admission procedure, whether the exchange carries out due diligence on potential members, including screening for sanctioned parties, and whether private individuals are permitted as members. Further guidance on the Financial Crime risk assessment of exchanges is given in section 10.10.

- Where T&S executes OTC and/or exchange traded derivatives (which must be cleared via a CCP) via a regulated third-party broker, KYC must be undertaken on the broker; note, introducers (generally unregulated parties) cannot typically execute/broker futures contracts; and

- Where T&S executes or accesses a market in any product via third party introducers, or distributors used to sell/market products on behalf of T&S, KYC must be carried out on the third party, with particular attention paid to any bribery and corruption risk associated with use of these types of counterparties.

If a Business Line has any doubt regarding whether KYC should be undertaken on a counterparty, CCP, exchange, exchange member or third-party entity, they must consult with the Compliance Advisory team or the FC Team.

4.8. Connected groups of companies and branches

KYC must be undertaken at the specific legal entity level for each counterparty in line with these Standards, regardless of whether the counterparty is connected to other counterparties in the same corporate group via common ownership or control. However, Business Lines may use KYC information and documentation already obtained for connected counterparties, as long as it is relevant and current, in line with the requirements of these Standards and the Approved Sources List in Appendix 6.

Where counterparty information is permitted by Appendix 6, to be identified and verified, or certified by an authorised representative of the counterparty, this also extends to a parent company of the counterparty who may provide information on behalf of a subsidiary entity. However, Business Lines must comply with any data privacy requirements when discussing KYC information with parties other than the counterparty itself.

Wholly-owned branches of counterparties that are not separate, legal entities in their own right can be treated as part of the relevant parent company legal entity KYC file, as long as the specific branch name, branch address and link to the parent company are verified. Other than for entities eligible for SDD, Branch managers should be screened for sanctions and PEPs where they are deemed to exercise control over the entity or the T&S business relationship.

4.9. Timing of KYC

No new business relationship may be entered into before KYC has been completed on the counterparty, unless permitted by these Standards. New counterparty accounts must not be established in the relevant trading/transactional systems until approval has been received from the FC Team confirming that KYC measures and approvals are complete.

KYC measures must be applied:

- before T&S establishes a business relationship with a counterparty; and

- on an ongoing basis, during the relationship in line with the requirements in section 12, to ensure that the counterparty information and Financial Crime risk profile is up to date.

4.10. General exception for tenders and prospective counterparties

Business Lines may submit or make non-binding tenders or bids for new business without completion of full KYC measures prior to the bid, provided the tender documentation submitted to the prospective counterparty includes a clause that any successful appointment of, or commitment by T&S, will be subject to satisfactory completion of KYC measures. Business Lines are accountable for any subsequent reputational or financial risk that may arise due to an inability to complete

KYC. For binding tenders, no deviation is permitted, and KYC measures must be undertaken prior to submission of the tender.

Business Lines must refer to the Shell T&S Sanctions Compliance Policy and associated guidance and Business Line procedures regarding the screening of prospective counterparties and their representatives, prior to engaging or forming a business relationship. Screening of prospective counterparties prior to engagement or forming a business relationship is not a substitute for the subsequent KYC measures to be completed in line with the timings noted in section 4.9 above.

5. PERFORMING KYC

This section sets out how to perform KYC, depending on the counterparty risk assessment and associated due diligence level for a counterparty.

5.1. Initial Due Diligence ("IDD")

The first KYC measure that must be applied is IDD. IDD is undertaken by the COF within the Business Lines to gather counterparty documentation and information, in line with the Approved Sources List set out in Appendix 6. This includes information about the proposed counterparty relationship, the counterparty's legal form, constitutional information, directors, shareholders, nature of business and operating locations. IDD must be undertaken before the counterparty is subject to the other KYC measures, including risk assessment and scoring.

Counterparty risk scoring cannot be fully completed by the FC Team and therefore may not be notified to the Business Line/COF until IDD is completed.

5.2. Counterparty Risk Scoring ("CRS")

The Financial Crime risk posed by each counterparty must be determined, assessed and documented as part of KYC measures. All counterparties, except for those eligible for Basic Due Diligence ("BDD"), which have already been assessed as Low, must be risk rated as either "High Risk", "Medium Risk" or "Low Risk", using the CRS methodology determined by the FC Team, before the establishment of a business relationship with the counterparty. The counterparty Financial Crime risk rating must also be reviewed and where needed, re-assessed, during any subsequent ODD review as set out in section 12 of these Standards.

The CRS methodology is owned by the Head of Financial Crime, with approval from the T&S MLRO and is based on the identified Financial Crime risks posed by the counterparty which in turn determines the applicable counterparty risk rating. The risk factors considered by the CRS include, but are not limited to:

- counterparty legal form and listed or regulated status e.g. a private company, publicly listed company;
- geographical connections;
- products/services traded and/or business activities undertaken with T&S;
- Financial Crime adverse media;

- sanctions connections;
- PEP associations; and
- other Financial Crime specific concerns such as bribery and corruption or fraud risk, or presence of opaque ownership structure.

The CRS risk rating drives the level of due diligence measures that must be applied. The risk rating also determines the frequency of the ODD re-review cycle applied. The table below sets out each risk rating and the associated due diligence level and ODD cycle.

CRS risk rating	Level of due diligence required	Frequency of ODD review
High	Enhanced Due Diligence ("EDD")	Annual
Medium	Counterparty Due Diligence ("CDD")	3 years
Low	Counterparty Due Diligence "(CDD") or Simplified Due Diligence ("SDD")	5 years[9]
N/A	Basic Due Diligence ("BDD")	N/A – overnight screening undertaken

An overview of each level of due diligence is set out in sections 5.3 to 5.6 below. In addition, section 8 sets out the screening requirements to be applied to counterparties and related parties such as directors, based on the legal form of the counterparty.

For all levels of due diligence, core information about the counterparty is required to be obtained and documented and the counterparty name is required to be screened against applicable sanctions lists. However, the individual requirements and need to verify the information against supporting documentation will vary depending on the level of due diligence being applied.

Where the Business Line does not agree with the CRS risk rating, a proposal for the downgrading or upgrading of the risk rating may be made to the FC Team which is subject to approval from the Head of Financial Crime, in consultation with the T&S MLRO. In all cases, the rationale for the change must be documented on the counterparty KYC file.

[9] Note, where SDD is applied, Business Lines must notify the FC Team if they become aware of any changes in regulated/listed status that may result in removal of eligibility for SDD; see section 12.4 for further guidance on trigger events.

5.3. Basic Due Diligence ("BDD")

BDD is the lowest level of due diligence permitted by T&S and can only be applied in restricted circumstances for defined counterparty types involved in physical or non-trading business activities that are not regulated for Anti-Money Laundering ("AML") or Counter Terrorist Financing ("CTF") purposes, and where the proposed relationship is considered to present limited Financial Crime risk as well as vendors.

5.3.1. BDD eligibility

BDD may only be applied to the following counterparty types and activities:

- Storage/terminalling providers;
- Bunker fuel end-users;
- Transmission and Distribution system operators, including government-owned transmission/distribution or "grid" operators, and national or regional commodity regulators/bodies where T&S pays for the use of a service or membership;
- Financial Institutions ("FIs") involved in credit or finance activities such as providing letters of credit ("LCs") to counterparties, or commodity based lending, where eligible for BDD as set out in sections 20 and 22;
- Vessels, watercraft and ships (subject to the specific requirements in section 5.3.4);
- Shell-owned entities, where 50% or more of the entity is owned and controlled by Shell companies e.g. joint ventures and subsidiary companies (see section 5.3.3 below for further information);
- Individual direct customers and direct suppliers e.g. crude leaseholders (or similar commodity leaseholder) in Low/Medium FC risk countries, including North American ("NA") crude leaseholders/producers who meet the eligibility criteria for BDD as set out in the Business Line and FC Team operating procedures.
- Shell Energy Commercial and Industrial ("C&I") physical end-user customers[10] including those who are government-owned municipalities, state schools and hospitals (or equivalent), even where there are connections to Low Risk PEPs (see section 9).

[10] Defined as an end user or consumer of a physical commodity for power purposes, where there is no resale (other than occasional buyback of surplus by T&S under net settlement or similar arrangements) and where the purpose is for the counterparty to consume the commodity rather than trade.

- Non-shipping transportation counterparties e.g. rail, road and air transport providers;

- Royalty payees and similar parties to whom T&S makes or receives payments on behalf of counterparties;

- Exchange members transacting with non-regulated T&S business, where T&S delivers to, or settles with the underlying counterparty directly (see section 4.7 for further guidance) e.g. Chinese Emission exchange members in SIETCO;

- Local commodity distribution companies in regulated markets, including rural US Electric Cooperatives, state-owned and managed US municipal electric utilities ("municipalities") and regulated, Asian distribution companies, who purchase wholesale gas and power from T&S for onward sale or local distribution to the end consumer, including where they sell occasional surplus volumes back to T&S or to third parties as part of supply balancing activities.

- Shell Products physical end-user customers in Low/Medium FC risk countries to whom we sell products/commodities for own consumption i.e. not for processing/refining/converting to other products for onward sale, or resellers/ traders/ wholesalers of products;

- Parties with whom Shell is obligated to transact to make or receive balancing payments under local, regulated market participation rules and arrangements e.g. Quality Bank companies in NA who collect balancing payments and Inland Freight Equalization Margin ("IFEM") pricing mechanism counterparties or equivalent[11];

- Providers of pipelines and wires (including those that are government-owned with Low Risk PEPs) used by T&S for distribution activities, whose primary business is the provision of these services (NB. this includes providers who are permitted to occasionally sell surplus volumes under local regulations e.g. Pipeline Loss Allowance ("PLA") barrels in the US);

- ERM Power counterparties where Shell Energy Australia ("SEAU") trades physical spot contracts with underlying participants; and

- Technical Operators/Managers of vessels who only purchase shipping inspection services from T&S and where there is no wider commercial/freight relationship.

[11] Including those in EDD countries, where approved by the Head of Financial Crime or delegate

Unless noted above and summarised in the table below, BDD is not permitted where any of the following is identified, without appropriate rationale and an approved exception from the Head of Financial Crime (or delegate):

- where the entity or relationship is classified as a Direct Government Intermediary ("GI")[12];
- where the entity is registered in an "EDD" country as defined by the FC Team[13];
- there are doubts about the veracity or accuracy of KYC documents, data or information obtained;
- where there is evidence of a PEP as a related party or UBO (both Low and High Risk PEPs) [14];
- where there is a Financial Crime risk red flag such as sanctions connections or material Financial Crime adverse media;
- where advised by the FC Team e.g. where a Suspicious Activity Report ("SAR") has been raised; or
- where a regulated T&S Business e.g. STASCO that is subject to specific AML regulation and associated KYC requirements, conducts trading activity with the counterparty.

Where BDD is not permitted, the counterparty must be subject to either SDD, CDD or EDD as per sections 5.4, 5.5 and 5.6. FIs used for non-trading activity or indirect relationships may be subject to reduced CDD and EDD requirements as set out in section 10.11.

If analysts have any concerns or doubts regarding BDD eligibility, they should consult with the FC Team.

[12] T&S requirements for GIs are set out within the RDS Ethics and Compliance Manual due diligence rules.
[13] This does not apply to vessels, 50% or more Shell-owned entities and joint ventures, or to FIs involved in non-trading activities where permitted in sections 20 and 22. These may still be subject to BDD.
[14] In the absence of other Financial Crime concerns, the presence of Low Risk PEPs for government-owned transmission/distribution or "grid" operators or commodity regulators/bodies, service providers (pipelines and wires, TSOs/DSOs, storage/terminalling). state-owned C&I or Products physical end users and local energy distribution companies or to FIs involved in non-trading activities does not result in BDD ineligibility.

A summary of the BDD-eligibility of counterparties is set out below:

BDD High level category	Regulated entity e.g. STASCO	EDD High Risk country	Government owned/Low Risk PEPs	High Risk PEPs	Unmitigated FC Adverse media	Sanctions nexus	Direct GIs	Indirect GIs*
Storage/terminalling providers	Y	N	Y	N	N	N	N	Y
Bunker fuel end-users	N	N	N	N	N	N	N	Y
TSOs/DSOs, Regulators, Grid Operators, Pipes and Wires	Y	N	Y	N	N	N	N	Y
FIs (non-trading)	Y	Y – where permitted in sections 20 & 22	Y	N	N	N	N	Y
Shell-owned entities/JVs	Y	Y	N/A	N/A	N/A	N/A	N/A	N/A
Direct customers/suppliers	N	N	N	N	N	N	N	Y
Energy C&I physical end-users	N	N	Y	N	N	N	N	Y
Products C&I physical end-users	N	N	Y	N	N	N	N	Y
Non-shipping transportation	Y	N	N	N	N	N	N	Y
Royalty payees (NA only)	N	N	Y	N	N	N	N/A	N/A
Anonymously matched exchange members that take physical delivery/payment	N	N	Y	N	N	N	N	Y
Regulated distribution companies	N	N	Y	N	N	N	N	Y
Mandatory regulatory payments	N	With approval of FC Team	Y	With approval of FC Team	N	N	N	Y
ERM physical spot deals (SEAU)	N	N	N	N	N	N	N	Y
Technical Operators: shipping inspection customers only	Y	N	N	N	N	N	N	Y
Vendors as described in 4.6	Y	Y	Y	With approval of FC Team	With approval of FC Team	With approval of FC/TC Team	N	Y

*subject to completion of SECO additional requirements for GIs, including Compliance questionnaire, memo and ABC SME approvals (High ABC risk countries)

5.3.2. BDD requirements

The following tables set out the minimum due diligence requirements for all counterparties (regardless of legal form) subject to BDD.[15]

Entities

Requirement	Identify	Verify	Section reference
Full legal name*	✓	✓	17.3
Trading name (if applicable)*	✓	N/A	17.3
Proof of legal entity type and active status*	✓	✓	17.11
Government issued ID number or equivalent*	✓	✓	17.5
Registered address and country of incorporation (if different)*	✓	✓	17.6, 17.9
Trading address (if different from registered address)*	✓	✓	17.7
Purpose and nature of intended relationship	✓	N/A	17.12
Nature of counterparty's business	✓	N/A	17.13

*NB for NA crude royalty payees, verification of name and Tax Identification Number ("TIN") to the Internal Revenue Service ("IRS") website is sufficient for verification purposes.

Individuals (NA crude leaseholders and royalty payees only)

Requirement	Identify	Verify	Section reference
Full legal name[16]	✓	N/A	17.3
Country of residence	✓	N/A	17.6, 17.9
Government issued ID number e.g. Tax Identification Number or equivalent	✓	✓	17.5
Purpose and nature of intended relationship	✓	N/A	17.12

Screening requirements – Entities and Individuals

Requirement	PEP	Sanctions	Adverse media	Section reference
Legal name	✓	✓	N/A	8

Business Lines must have appropriate processes in place to ensure that the eligibility for BDD in line with these Standards is subject to approval by a person who is independent of the sales originator and this approval must be recorded on the KYC file.

[15] Other information and documentation may be required to satisfy tax, credit or other onboarding requirements, as required by the relevant function e.g. Tax ID number, LEI or ACER codes.
[16] Identification is checked to the United States Internal Revenue Service website or equivalent.

Business Lines must ensure that controls are in place to ensure that trading activity is not undertaken with a counterparty that has only been subject to BDD and that counterparties subject to BDD are only used for the specific activity giving rise to the BDD eligibility. Trading activity should not be undertaken prior to completion of full KYC measures.

For any counterparty subject to BDD, there is no requirement to identify beneficial ownership or control, or record details of Directors. However, this does not remove the need for Business Lines to ensure they know who they are dealing with and only undertake transactions with individuals authorised to represent the counterparty.

5.3.3. BDD – Shell owned entities

Other Shell-owned entities e.g. joint ventures and subsidiary companies, where 50% or more of the entity is owned and controlled by Shell companies in any country, are eligible for BDD, subject to the other BDD eligibility requirements outlined in section 5.3.1.

T&S can utilise and rely on the internal RDS company file for KYC documentation as long as information is current.

Note Shell-owned entities do not require an escalation to HRCC, unless requested by the FC Team due to specific concerns. See section 5.6.2 for High Risk counterparty escalations and approvals.

5.3.4. BDD – vessels requirements

The following requirements apply to all vessels, watercraft and ships (other than inland barges and regional vessels in non-EDD countries, which are not subject to KYC requirements), where chartered by T&S (either directly or indirectly via a management company or operator), or nominated for use for shipping of T&S products by a counterparty:

Requirement	Identify	Verify
Vessel name	✓	✓
Country flag[17]	✓	✓
International Maritime Organisation ("IMO") number	✓	✓
Sanctions screening of vessel name and IMO number	✓	N/A

[17] All vessels should be marked as "Worldwide" accounts in the corresponding KYC file

5.3.5. BDD – use of public sources and review of third party reports

Due to the non-trading nature of these relationships and their lower AML/CTF risk, verification of KYC information may be undertaken using public sources. Where possible, Business Lines should obtain an approved third party KYC report e.g. Dun and Bradstreet, Orbis, Bankers Almanac, which triangulates multiple public sources for due diligence information and also screens the counterparty for Financial Crime red flags.

A list of approved third party report providers is included in the Approved Sources List set out in Appendix 6.

The relevant Business Line is responsible for reviewing the third party KYC report obtained. If any required information in sections 5.3.2 is missing, a PEP is identified (High or Low Risk, unless permitted under the exceptions noted in section 5.3.1), or any other high risk factors such as sanctions connections or material Financial Crime adverse media, the counterparty will no longer be eligible for BDD. It must be risk-assessed and subject to the relevant level of due diligence in accordance with the CRS risk rating and counterparty entity type, or the Business Line must decline to onboard the counterparty.

Certification of documentation used for verification purposes is not required for BDD.

5.3.6. BDD – Ongoing Due Diligence

Periodic ODD reviews are not required for counterparties subject to BDD, other than automated ongoing sanctions screening of the counterparty legal name. However, Business Lines are responsible for ensuring that the eligibility for BDD is re-assessed on an annual basis to ensure that it is appropriate.

If a trigger event e.g. change in a counterparty's name or address, is identified in relation to a counterparty subject to BDD, or it no longer meets the eligibility criteria for BDD, it is the responsibility of the relevant Business Line to notify the FC Team and trigger an ODD re-review of the counterparty in line with these Standards. Trigger events are set out in further detail in section 12.4.

5.4. Simplified Due Diligence ("SDD")

SDD measures may be applied to certain business relationships that present a low degree of Financial Crime risk, where there are mandatory public disclosure requirements around ownership, business activities and financial information and therefore enhanced transparency.

The Business Line, in consultation with the FC Team, must document the assessment and rationale for the application of SDD within the counterparty KYC file, including an assessment of any

factors which may indicate increased Financial Crime risk and why these are not considered to impact eligibility for SDD.

5.4.1. SDD eligibility

SDD may only be applied to the following counterparty types and activities:

- Publicly listed companies, whose securities are listed on an approved exchange[18]

- Subsidiaries of publicly listed companies whose securities are listed on an approved exchange (other than those registered or operating in "EDD" countries) where it is verified that the parent company directly or indirectly owns and controls more than 50% of the subsidiary company. For subsidiaries eligible for SDD, the following should be applied:

    - for shareholdings of more than 50% but less than 75%, verification of consolidation in the listed parent's financial statements is required; and
    - for shareholdings of 75% or more, consolidation by the listed parent may be assumed and does not need to be verified.

- Regulated Financial Institutions ("FI"), including investment fund managers, who are verified as regulated by an approved regulator[19].

- Subsidiaries and branches of regulated FIs who are regulated by an approved regulator, in any country (including those registered in "EDD" countries subject to the conditions noted below) where it is verified that the parent company owns and controls >50% of the subsidiary and the subsidiary is consolidated in the regulated parent's financial statements.

Note, where a FI is used only for credit or finance purposes only, different requirements may be applied. Please see the guidance in sections 10.11, 20 and 22 of these Standards.

Where a counterparty does not meet the criteria above, it must be subject to either CDD or EDD as set out in sections 5.5 and 5.6 below.

5.4.2. SDD ineligibility

Unless otherwise noted, SDD is not permitted in any of the following scenarios:

---

[18] A list of approved exchanges and markets is set out in Appendix 6 of these Standards. Where an entity is not listed on an approved market/exchange, the counterparty must be treated as a "private or unlisted company" as set out in section 10.2 of these Standards.

[19] A list of approved regulators is set out in Appendix 6 of these Standards and are those regulators which T&S has deemed to have appropriate Financial Crime regulatory oversight, typically in countries deemed to present lower inherent Financial Crime risk.

- where the entity is registered in an EDD country as defined by the FC Team, including countries classified by RDS as a GEC or HRC. Note, this does not apply to consolidated subsidiaries and branches of regulated FIs who are regulated by an approved regulator where the counterparty confirms it complies with its parent's Financial Crime policies;

- there are doubts about the veracity or accuracy of KYC documents, data or information obtained;

- where there is evidence of high risk factors e.g. High Risk PEPs (as defined in section 9), sanctions connections or material Financial Crime adverse media, including unmitigated bribery and corruption red flags;

- the Financial Crime risk of the business relationship is not considered to be Low, based on the CRS output; or

- where advised by the FC Team e.g. where a SAR has been reported.

SDD may still be applied where Low Risk PEPs are identified. However, EDD measures must still be applied to the PEP, which includes a PEP risk assessment and adverse media screening in accordance with section 8. Where the outcome of the PEP risk assessment results in a High Risk PEP, this will increase the risk rating of the counterparty to High Risk and SDD may no longer be applied.

Unless advised by the FC Team, the identification of enforcement actions or fines of SDD-eligible entities for Financial Crime control failures or violations, will not be considered material for the purposes of SDD eligibility, as long as there is no indication that the actions have not been settled, the issues do not appear to be ongoing/systemic and the entity has taken remedial action as required by the relevant regulator/enforcement body.

SDD may also be applied to listed or regulated companies (and their approved subsidiaries) who issue bearer shares, which is still common in certain EU countries, as long as the counterparty relationship is still considered to be low risk from a Financial Crime perspective. Bearer shares issued by SDD-eligible entities may be treated as "registered" bearer shares, and do not require HRCC approval unless advised by the FC Team.

5.4.3. SDD requirements

The following tables set out the due diligence requirements for listed entities and separately for regulated FIs.

Publicly listed entities (and relevant subsidiaries) on an approved exchange

	Identify	Verify	Section Reference
Requirements			
Full legal name	✓	✓	17.3
Trading name (if applicable)	✓	N/A	17.3
Proof of legal entity type and active status	✓	✓	17.11
Government issued ID number or equivalent	✓	✓	17.5
Registered address and country of incorporation (if different)	✓	✓	17.6, 17.9
Trading address (if different)	✓	✓	17.7
Operating region(s)	✓	N/A	17.10
Proof of listing/parent company listing on exchange	✓	✓	17.11
Where the counterparty is a >50% subsidiary, proof of ownership/control by the listed parent	✓	✓	17.11
For subsidiaries owned >50% but <75%, proof of consolidation in parent company's financial statements	✓	✓	N/A
Purpose and nature of intended relationship	✓	N/A	17.12
Nature of counterparty's business	✓	N/A	17.13
Names of current Board of Directors (or equivalent)	✓[20]	N/A	6.2
Related Parties			
Board of Directors (or equivalent)[21]	✓	N/A	6.2
Ultimate Controller(s)	N/A	N/A	7.5
UBO(s)	N/A	N/A	7.4
PEP and Sanctions screening			
Entity name	✓		8
Board of Directors names	✓		8
Adverse Media screening			
Entity name	✓		8
Board of Directors names (PEPs only)	✓		8

Note, it is not necessary to identify, record and screen the intermediate layers between the subsidiary and parent company, nor is it necessary to identify and verify the UBO or Ultimate Controller.

[20] An approved source must be used to identify the names of the current Board of Directors i.e. the composition of the Board. This is separate to the requirement to verify the identifies of individual directors as set out in sections 6.2 and 6.3.

[21] Note, reliable public sources may be used to identify names and other identifying information required per section 6.3, as long as sufficient information is available to screen and disposition screening hits.

FIs (and relevant subsidiaries) regulated by an approved regulator

	Identify	Verify	Section reference
Requirement			
Full legal name	✓	✓	17.3
Trading name (if applicable)	✓	N/A	17.3
Proof of legal entity type and active status	✓	✓	17.11
Government issued ID number or equivalent	✓	✓	17.5
Registered address and country of incorporation (if different)	✓	✓	17.6, 17.9
Trading address (if different)	✓	✓	17.7
Operating region(s)	✓	N/A	17.10
Proof of regulation by an approved regulator.	✓	✓	17.11
Where the counterparty is a >50% subsidiary/branch, proof of ownership/control and consolidation by the regulated parent	✓	✓	17.11
Purpose and nature of intended relationship	✓	N/A	17.12
Nature of counterparty's business	✓	N/A	17.13
Ownership structure	✓[22]	N/A	17.14
Names of current Board of Directors (or equivalent)	✓	N/A	6.2
Related Parties			
Board of Directors (or equivalent) [23]	✓	N/A	6.2
Ultimate Controller(s)	✓	✓[24]	7.5
UBO(s)	✓	✓	7.4
PEP and Sanctions screening			
Entity name	✓		8
Board of Directors	✓		8
Ultimate Controller(s)	✓		8
UBO(s) >25%	✓		8
For SPVs only, legal name of sponsoring entity	N/A		8, 10.4
Branch Managers (where required)	N/A		4.8

[22] For regulated FIs (unless also eligible for SDD by virtue of being publicly listed on an approved exchange), the ownership structure must show all shareholders and layers (beneficial owners) between the counterparty and any UBO(s) owning or controlling more than 25%, considering shareholding aggregations across all layers and branches.
[23] Note, reliable public sources may be used to identify Director names and other identifying information required per section 6.3, as long as sufficient information is available to screen and disposition screening hits.
[24] Where there is no identifiable Ultimate Controller and the Chairman and CEO are noted as Ultimate Controller by default, reliable public sources may be used to identify and verify the identifying information required per section 6.3, as long as sufficient information is available to screen and disposition screening hits.

	Identify	Verify	Section reference
Adverse Media screening			
Entity name	✓		8
Board of Directors (PEPs only)	✓		8

In addition to the above minimum requirements for SDD, Business Lines must also establish controls to ensure that they know who the representatives of the counterparty are and that these representatives are authorised to act on the counterparty's behalf.

Where SDD is not permitted, the counterparty must be subject to either CDD or EDD as outlined in section 5.5 and 5.6 based on the risk rating determined by the CRS.

5.4.4. SDD – Use of public sources

Due to the lower inherent Financial Crime risk of counterparties subject to SDD, verification of counterparty and related party KYC information may be undertaken using public sources or an approved third party report or database e.g. Dun and Bradstreet, Orbis, Bankers Almanac. A list of approved third party report providers and approved sources is included in the Approved Sources List set out in Appendix 6.

As noted above, for Directors, Ultimate Controllers and UBOs of entities eligible for SDD (where identification and verification is a requirement), reliance may be placed on reliable public information (e.g. annual reports or official counterparty websites) to identify personal information regarding individuals, as long as at a minimum, the full legal name and country of residence is identified and sufficient information is identified to enable screening and dispositioning of any screening hits. Any missing information should be clearly noted on the KYC file.

Certification of documentation used for verification purposes is not required for SDD.

Where due to a Financial Crime red flag, EDD is required to be applied to an entity that would otherwise be eligible for SDD e.g. a subsidiary in an EDD country, of a publicly listed company on an approved exchange, Business Lines may still utilise reliable public information (e.g. regulatory/exchange filings, annual reports or official counterparty websites) to identify and verify KYC information required by these Standards. However, the requirements for EDD, such as PEP risk assessment and adverse media screening of the counterparty and related parties, must be completed.

5.4.5. SDD – Ongoing Due Diligence

Section 12 sets out the ODD requirements to be applied to counterparties eligible for SDD.

If a trigger event is identified, it is the responsibility of the relevant Business Line to notify the FC Team and trigger an ODD review of the counterparty in line with these Standards. Examples of trigger events are set out in further detail in section 12.4.

5.4.6. Publicly listed and regulated entities not eligible for SDD

Whilst SDD is only permissible for low risk publicly listed and regulated entities and relevant subsidiaries as set out in section 5.4.1, it is accepted that other entities e.g. those on unapproved exchanges or regulated by unapproved regulators in higher risk jurisdictions, may also have publicly available documentation to support KYC measures, including ownership and control, personal information for Directors, business activities and financial performance. Whilst the requirements for CDD and EDD must be met, including the assessment and documentation of full ownership and control structure and screening of UBOs and other related parties, Business Lines should leverage available, reliable public sources where possible, to complete the KYC requirements.

In particular, public information regarding Ultimate Controllers who are the CEO or Chairman, as well as the Board of Directors may be used for identification and verification purposes, as long as sufficient information is available for screening purposes and to enable the discounting of any screening hits.

5.5. Counterparty Due Diligence ("CDD")

CDD refers to the minimum level of due diligence measures which must be performed at the start of each counterparty relationship and reconfirmed as part of ODD for all counterparties who are not eligible for either BDD or SDD.

CDD provides a more comprehensive assessment of a counterparty's information and related parties such as directors and UBOs.

5.5.1. CDD requirements

The following table sets out the minimum due diligence requirements for all counterparties (regardless of legal form) subject to CDD.

	Identify	Verify	Section reference
Requirement			
Full legal name	✓	✓	17.3

	Identify	Verify	Section reference
Trading name (if applicable)	✓	N/A	17.3
Proof of legal entity type and active status	✓	✓	17.11
Government issued ID number or equivalent	✓	✓	17.5
Registered address and country of incorporation (if different)	✓	✓	17.6, 17.9
Trading address (if different)	✓	✓	17.7
Operating region(s)	✓	N/A	17.10
Purpose and nature of intended relationship	✓	N/A	17.12
Nature of counterparty's business	✓	N/A	17.13
Source of Wealth for UBO (75% or more ownership or control)	✓	N/A	16.2
Ownership structure	✓[25]	N/A	17.14
Names of current Board of Directors (or equivalent)	✓	✓[26]	N/A
Related Parties			
Board of Directors (or equivalent)	✓	N/A	6.3
Ultimate Controller(s)	✓	✓[27]	6.3
UBO(s)	✓	✓	6.3
Shareholder layers between entity and UBOs	✓	N/A	7.3
PEP and Sanctions screening			
Entity name[28]	✓		8
Board of Directors	✓		8
Ultimate Controller(s)	✓		8
UBO(s) >25%	✓		8
Shareholder layers between entity and UBOs	✓		8
For SPVs only, legal name of sponsoring entity	✓		8, 10.4

[25] The ownership structure must show all shareholders and layers (beneficial owners) between the counterparty and any individual UBO(s) owning or controlling more than 25%, considering shareholding aggregations across all layers and branches.

[26] An approved source must be used to identify and verify the names of the current Board of Directors i.e. the composition of the Board. This is separate to the requirement to verify the identifies of individual directors as set out in sections 6.2 and 6.3.

[27] Where there is no identifiable Ultimate Controller and the Chairman and CEO are noted as Ultimate Controller by default, reliable public sources may be used to identify and verify the identifying information required per section 6.3, as long as sufficient information is available to screen and disposition screening hits.

[28] If an entity has changed its legal name within the past 12 months, the former name should also be screened.

	Identify	Verify	Section reference
Branch Managers (where required)	✓		4.8, 8
Adverse Media screening			
Entity name[28]	✓		8
Board of Directors (PEPs only)	✓		8
Ultimate Controller(s) (PEPs only)	✓		8
UBO(s) >25% (PEPs only)	✓		8
For SPVs only, legal name of sponsoring entity	✓		8, 10.4

Business Lines must also establish controls to ensure that they know who the representatives of the counterparty are and that these representatives are authorised to act on the counterparty's behalf.

Where CDD is not permitted, based on the risk rating determined by the CRS, the counterparty must be subject to EDD (refer to section 5.6 for further information).

5.5.2. CDD – Ongoing Due Diligence

Section 11 sets out the ODD requirements to be applied to counterparties eligible for CDD, with an ODD review required either every three years (Medium Risk) or five years (Low Risk), based on the CRS risk rating.

If a trigger event is identified in relation to a counterparty subject to CDD, it is the responsibility of the relevant Business Line to notify the FC Team and trigger an ODD review of the counterparty in line with these Standards. Trigger events are set out in further detail in section 12.4.

5.6. Enhanced Due Diligence ("EDD")

Where a counterparty presents increased risk of Financial Crime, EDD must be applied. EDD requires additional due diligence measures in addition to the CDD measures referenced above. EDD must be applied in the following circumstances:

- when a counterparty is determined to be a High Risk counterparty by the CRS;
- where the counterparty is registered in, whose principal place of business is in or who has a substantial presence (i.e. 50% or more of its operations or customer base) in an EDD country, as defined by the FC Team and approved by the HRCC;
- where the counterparty is connected to a High Risk PEP as defined in section 9.8.2;

- where there are doubts about the veracity of KYC information presented, or as instructed by the FC Team or HRCC;

- where a counterparty has "opaque" ownership as defined in section 7.8;

- when T&S suspects a counterparty of Financial Crime including money laundering, terrorist financing, bribery and corruption or where a new sanctions breach is identified;

- where there are confirmed material Financial Crime adverse media findings in relation to the counterparty or a related party, as set out in section 8.3.3; and

- in any case where the structure and nature of a counterparty transaction:

    - is unusually complex or large[29]; or there is an unusual pattern of transactions and
    - has no apparent economic or legal purpose and requires further review.

The list above is not exhaustive and the application of EDD may be required where a counterparty is higher risk for other factors not included above.

Some of the factors above, such as complex or unusually large transactions may trigger EDD after a business relationship has commenced. These factors may be identified through trade monitoring or ODD of the counterparty as outlined in section 12.

5.6.1. EDD requirements

In addition to the CDD measures set out above, the following EDD measures must be applied at a minimum:

- independently verifying and evidencing information about a counterparty and its related parties using Approved Sources List as set out in Appendix 6;

- assessing and documenting the specific risks arising from the red flags that give rise to the higher risk rating and taking necessary measures to mitigate those risks;

- verifying UBOs and Ultimate Controllers owning or controlling more than 10% of a counterparty (rather than more than 25% for counterparties subject to CDD);

- identifying the Source of Funds ("SoF") of the counterparty and verifying the Source of Wealth ("SoW") for certain UBOs, where required; and

[29] There is no generic definition of unusually large or complex as this will vary from Business Line to Line. Business Lines should consult with the Compliance Advisory Team where required.

- conducting more frequent ODD of High Risk counterparties, in line with the requirements set out in section 5.6.3.

The following table sets out the minimum due diligence requirements for all counterparties (regardless of legal form) subject to EDD.

	Identify	Verify	Section reference
Requirement			
Full legal name	✓	✓	17.3
Trading name (if applicable)	✓	N/A	17.3
Proof of legal entity type and active status	✓	✓	17.11
Government issued ID number or equivalent	✓	✓	17.5
Registered address and country of incorporation (where different)	✓	✓	17.6, 17.9
Trading address (if different)	✓	✓	17.7
Operating region(s)	✓	N/A	17.10
Purpose and nature of intended relationship	✓	N/A	17.12
Nature of counterparty's business	✓	N/A	17.13
Source of Funds of counterparty	✓	N/A	16.4
Source of Wealth for a UBO who is a High Risk PEP (more than 10% ownership or control)	✓	✓	9.7.1, 16.2
Source of Wealth for all other UBO(s) (more than 25% of ownership or control)	✓	✓	16.2
Ownership structure[30]	✓	✓	17.14
Names of current Board of Directors (or equivalent)	✓	✓[31]	N/A
Related Parties			
Board of Directors (or equivalent)	✓	✓ *(minimum two)*	6.2
Ultimate Controller(s)	✓	✓	7.5
UBO(s)	✓	✓	7.4
Shareholder layers between entity and UBOs	✓	✓	7.3
PEP and Sanctions screening			
Entity name[32]	✓		8
Entity trading name(s)	✓		8, 17.3
Board of Directors	✓		8
Ultimate Controller(s)	✓		8

[30] The ownership structure must show all shareholders and layers (beneficial owners) between the counterparty and any UBO(s) owning more than 10%, considering shareholding aggregations across all layers and branches.

[31] An approved source must be used to identify the names of the current Board of Directors i.e. the composition of the Board. This is separate to the requirement to verify the identifies of individual directors as set out in sections 6.2 and 6.3.

[32] If an entity has changed its legal name within the past 12 months, the former name should also be screened.

	Identify	Verify	Section reference
UBO(s) >10%	✓		8
Shareholder layers between entity and UBOs	✓		8
For SPVs only, legal name of sponsoring entity	✓		10.4
Branch Managers (where required)	✓		4.8, 8
Adverse Media screening			
Entity name[32]	✓		8
Entity trading name(s)	✓		8, 17.3
Board of Directors	✓		8
Ultimate Controller(s)	✓		8
UBO(s) >10%	✓		8
Shareholder layers between entity and UBOs	N/A		8
For SPVs only, legal name of sponsoring entity	✓		10.4

5.6.2. High Risk counterparty approvals

In addition to the application of EDD, certain types of High Risk counterparties require referral to the HRCC for additional review and approval, in line with the T&S Financial Crime risk appetite. These include, at a minimum:

- counterparties who have a connection with a High Risk PEP;
- confirmed material Financial Crime adverse media in relation to the counterparty, a PEP or a related party (see section 8.3.3);
- the counterparty has a confirmed sanctions connection (see section 8.3.1);
- counterparties who issue unregistered bearer shares, or where it becomes known that unregistered bearer shares are within the ownership chain; or
- counterparties (excluding 50% or more Shell-owned entities and vendors, vessels and relevant FIs as permitted in sections 20 and 22) located in, or with a substantial presence (see section 5.6 above) in an EDD country.

For all other High Risk counterparties, the relationship is subject to review and approval by the FC Team in line with the approved manual of authorities ("MoA").

5.6.3. EDD – Ongoing Due Diligence

Section 12 sets out the ODD requirements to be applied to counterparties eligible for EDD, with an ODD review required on an annual basis.

If a trigger event is identified in relation to a counterparty subject to EDD, it is the responsibility of the relevant Business Line to notify the FC Team and trigger an ODD review of the counterparty in line with these Standards. Trigger events are set out in further detail in section 12.4.

5.7. Missing information

It is the responsibility of the Business Line to obtain relevant counterparty documentation and information to enable the counterparty KYC review, screening, risk assessment and approval in line with these Standards. Where there is missing documentation or information, it is the Business Line's responsibility to contact the counterparty to obtain the missing information. Partial KYC information in relation to counterparties should be deleted from T&S systems after a maximum period of 12 months, if the KYC file is not completed and approved within this timeframe.

Business Lines must not enter into transactions with counterparties where KYC has not been completed, unless expressly authorised by the MLRO (or delegate) or the HRCC.

5.8. Failure to provide information

If a Business Line is unable to complete the measures required by these Standards (for example, if the counterparty will not cooperate in supplying the requested information or, instances where the information cannot be independently verified), the Business Line must decline the counterparty relationship, unless it is able to mitigate what has not been fulfilled under an approved deviation or exception.

Failure of, or refusal by, a counterparty to provide KYC information within a reasonable timeframe and without adequate explanation may increase the Financial Crime risk associated with a counterparty and is a potential suspicious activity indicator. In such cases, the suspicion must be reported promptly as per the SAR requirements set out in the T&S Compliance Manual.

6. RELATED PARTIES

6.1. Overview

A related party is an individual or entity who is considered to exercise control and/or influence over a counterparty through ownership or being otherwise able to influence the actions of a counterparty or make management decisions in respect of the counterparty. For the purposes of these Standards, T&S have designated the following as related parties:

- Board of Directors or equivalent (see section 6.2 below);
- UBOs (see section 7.4) which includes trustees, beneficiaries and settlors of trusts where applicable;
- Ultimate Controllers of a counterparty (see section 7.5); and
- Fund managers and advisers, and other third parties acting on behalf of or making payments or providing guarantees/security (see section 21) on behalf of counterparties in an authorised capacity.

Further information on who is considered to be a related party and the associated screening requirements for specific entities can be found in section 10.

6.2. Board of Directors

Other than for counterparties subject to BDD, the full names of all current directors must be identified, and where verification of directors' identities is required, a minimum of two directors' identities must be verified.

The two directors for verification must be the Chief Executive Officer ("CEO") and the Chairman, or equivalent, where these roles exist on the Board of Directors. These individuals are typically the most senior Board members and, in some cases, may also meet the definition of an Ultimate Controller as set out in section 7.5.

6.3. Information required

The table below sets out the information required to be identified and verified for related parties where required in section 5, to enable proper identification and discounting of potential screening alerts.

Individuals i.e. natural persons

	SDD		CDD		EDD	
Requirement	Identify	Verify	Identify	Verify	Identify	Verify
UBO(s) more than 25% (SDD and CDD)/more than 10% (EDD) and Ultimate Controller(s), including those of corporate trustees of trusts						
Full name[33]	✓	✓	✓	✓	✓	✓
Residential address[34]	✓	N/A	✓	N/A	✓	N/A
Date of birth (month and year as a minimum)	✓	✓	✓	✓	✓	✓
Nationality or citizenship	✓	N/A	✓	N/A	✓	N/A
For UBO only: percentage of shareholding (indirect/direct)	✓	✓	✓	✓	✓	✓
For UBO only: Source of Wealth ("SoW") (All High Risk PEPs + UBOs > 75% (CDD) and > 25% (EDD))	N/A	N/A	✓	N/A	✓	✓
Other related parties e.g. Board of Directors, Ultimate Controllers of Corporate Directors						
Full name[34]	✓	N/A	✓	N/A	✓	✓
Residential address (minimum country of residence)[35]	✓	N/A	✓	N/A	✓	N/A
Date of birth (month and year as a minimum)	✓	N/A	✓	N/A	✓	✓

Where personal information for individuals e.g. address, date of birth or nationality, is refused due to confidentiality/privacy reasons, Business Lines should identify as much information as possible using reliable public sources (seeking more than one corroborating source where possible) and record any gaps on the file in line with the deviation requirements set out below.

If screening hits cannot be discounted as a result of a lack of identification information, further information will need to be provided by the counterparty or Business Line.

The KYC approver will make the ultimate decision regarding appropriateness of any permanent deviations.

[33] If any known aliases or former names within the past 3 years are known, these should also be recorded on the KYC file for information purposes and to assist with discounting of potential screening hits.

[34] Residential address does not need to be verified for individuals. The only verification requirement is to obtain a government issued photographic ID document showing full name, and date of birth or residential address. Where this is not available, please consult the FC Team for further guidance.

Legal entities e.g. Corporate Directors, Corporate Trustees, Fund Managers, Guarantors, Sponsoring Entities (SPVs)

Counterparty due diligence level	SDD		CDD		EDD	
Related Party requirement	Identify	Verify	Identify	Verify	Identify	Verify
Full legal name	✓	N/A	✓	✓	✓	✓
Registered address and country of incorporation (where different)	✓	N/A	✓	✓	✓	✓
Government issued ID number or equivalent	✓	N/A	✓	✓	✓	✓
Ultimate Controller of entity (individual)	✓	N/A	✓	✓	✓	✓
Corporate trustees only: Ownership and control structure	✓	N/A	✓	N/A	✓	N/A
Corporate trustees only: UBO(s) of entity > 25% (SDD/CDD) or >10% (EDD)	✓	N/A	✓	✓	✓	✓

Note, it is not necessary to perform full KYC measures on related parties who are legal entities (including corporate trustees), but the information above must be identified and verified, along with identification of the person(s) deemed to be the Ultimate Controller(s) of the entity. This may be confirmed in writing by an authorised representative of the counterparty/related party.

For corporate trustees, given their status as UBOs of a trust (see section 7.10), Business Lines must understand the ownership and control structure of the trustee entity, sufficient to identify the UBO(s) and Ultimate Controller(s) whose identities should be identified and verified as related parties in line with these Standards. Business Lines should consult with the FC Team where required.

Business Lines must also establish controls to ensure that they know who the representatives of the counterparty are and that these representatives from Corporate related parties are authorised to act on the counterparty's behalf.

7. BENEFICIAL OWNERSHIP AND CONTROL

7.1. Scope

This section sets out the minimum requirements to be applied when the beneficial ownership and control of a counterparty needs to be identified and verified.

7.2. Purpose

For all counterparties that are not eligible for BDD or who are not natural persons i.e. individuals, understanding the ownership and control structure, including beneficial ownership is important when assessing the Financial Crime risk posed by a counterparty.

As part of KYC measures, it is important that T&S identifies, and verifies where required, the individual(s) who has either ultimate beneficial ownership or control over the counterparty.

Understanding the ownership and control of an entity can be complex. It is necessary to look at both the legal shareholders of a company through all layers i.e. the entities or individuals in whose names the shares are registered, as well as the beneficial owners of companies i.e. those individuals who actually benefit from the ownership of an entity or control it by other means. Reviewing the entity's constitutional or governing documents may assist in understanding the ownership and control of the entity.

It should be noted not all UBOs are shareholders and not all shareholders are UBOs, although in many cases they will be the same.

7.3. Beneficial owners

Beneficial owners are any immediate or intermediate shareholders that sit between the counterparty and the UBOs e.g. intermediate parent companies and holding companies.

Other than for publicly listed entities eligible for SDD, all intermediate layers and shareholder entities who are beneficial owners need to be identified within the ownership structure to enable an assessment of jurisdictional and potential sanctions risk and determine whether the ownership structure is considered to be complex or opaque.

The following must be identified and recorded for each shareholder entity on the counterparty KYC file:

- full legal name;
- country of incorporation;

- actual (direct) and effective (indirect) shareholding percentage held; and
- results of screening requirements, where applicable, in line with section 8.

7.4. Ultimate Beneficial Owners ("UBO")

A UBO is defined as any individual[35] who ultimately owns more than 25% of a counterparty (more than 10% where EDD is required), both directly or indirectly, or otherwise controls the counterparty (see section 7.10 for UBO rules for trusts). Ownership includes shareholding, voting rights or any other controlling interest.

Other than for counterparties who are publicly listed and are eligible for SDD, all UBOs must be identified and their identities must be verified.

7.4.1. Identification of UBOs

As the applicable due diligence level may not be known at the point of IDD, all shareholders of a company should be identified through all intermediate layers, calculating the effective ownership at each layer, until an individual or a publicly listed entity on an approved exchange is reached.

Business Lines must also consider obvious relationships and/or linkages between shareholders, such as family, business or contractual relationships such as joint voting arrangements. Appendix 3 sets out examples of potential relationships and/or linkages between shareholders where aggregating shareholdings may be applicable.

All shares or other instruments or rights that give rise to an entitlement to profits, capital or voting rights in respect of the counterparty, must be considered when determining ownership percentages. The Business Line must document the share types held, which may be identified from official documents such as annual reports, or a counterparty's constitutional documents. Where information is not contained within company documentation, it may be obtained from external sources such as company registers or directly from an appropriate representative of the counterparty such as the Company Secretary or the counterparty's legal department.

Shares can only be excluded from the analysis where a share class has no rights to a share of profits, assets, votes or decision making, which is expected to be extremely rare. Where this occurs, guidance must be sought from the FC Team.

[35] When determining ultimate beneficial ownership, it must be a natural person i.e. an individual. Therefore, a legal entity cannot be a UBO.

7.4.2. UBOs and Ultimate Controllers for Publicly Listed Companies

Where a counterparty is eligible for SDD as a result of being publicly listed on an approved market or exchange (per section 5.6), there is no requirement to identify and verify the UBO or the Ultimate Controller. Reliance is placed on the transparency of public information in relation to the counterparty and its ownership and control, which is subject to a degree of oversight by the relevant listing authority.

However, this does not apply for publicly listed companies that are listed on an unapproved market or exchange. These companies are treated as private and unlisted companies as per section 10.2.

Where, for listed companies, there is no natural person who is the UBO via ownership above the relevant threshold of 25% or 10%, the Ultimate Controller(s) should be listed as UBO(s) in line with section 7.5 below.

7.5. Ultimate Controller

T&S requires the identification of the individual(s) (natural persons) with ultimate control, directly or indirectly, over the management of a counterparty (the "Ultimate Controller").

With the exception of BDD and publicly listed entities eligible for SDD, the Business Line is required to understand and document the ownership and control structure of the entity and consult with the FC Team where needed to review, assess and determine the individual(s) that is/(are) the Ultimate Controller(s).

The management structure of the counterparty must be assessed to determine if there are any individuals, in addition to the UBO(s), which meet one or more of the following conditions.

- directly or indirectly holds the right to appoint or remove a majority of board of directors; and/or

- has the right to exercise, or exercises, significant influence or control of the entity or over the activities of a counterparty e.g. via voting rights or power of veto.

Where the counterparty is considered to be state owned[36] the Ultimate Controller is typically considered to be the State, but this should be determined and the rationale documented, as part of the KYC measures applied.

[36] State ownership is defined in section 10.8 of these Standards.

There may be instances where the Ultimate Controller is a person outside of the counterparty and is not the same individual as the UBO or a Board Director. For example, with private equity funds, it may be a director of the fund manager or general partner who can sell or change the assets who is the Ultimate Controller, rather than the investors or limited partners who "own" the fund. An entity's constitutional documents or Annual Report will typically identify those individuals who are Ultimate Controllers.

There may be instances where there is no clearly identifiable individual who holds ultimate control. If after having exhausted all other possible means of identification, and provided there are no grounds for suspicion, and no other high risk factors have been identified, the Business Line must consider both the counterparty's Chairman and the Chief Executive Officer or equivalent, as the Ultimate Controllers. If in doubt, guidance must be sought from the FC Team.

For counterparties subject to SDD, there is no requirement to verify the identity of Ultimate Controllers who are noted as the Chairman and the Chief Executive Officer by default, as long as reliable public information is available to enable name screening and dispositioning of hits.

7.6. Requirements for EU registered counterparties

Under EU AML regulations, there is a requirement for EU countries to maintain a register of beneficial ownership for entities and trusts registered in their jurisdictions.

When onboarding or undertaking CDD or EDD on an EU-registered entity, a search of the relevant beneficial ownership register (where available) must be undertaken, or the counterparty must be requested to provide a certified extract of the relevant country register, and the extract must be stored on the counterparty KYC file. The entity's constitutional or incorporation documents e.g. Memorandum and Articles of Association, Partnership Agreement, or equivalent, should also be obtained in order to understand the ownership and control of the entity.

Where during the due diligence process, T&S becomes aware of material discrepancies[37] between the information in the register (for example Ireland's Central Register of Beneficial Ownership) and the beneficial ownership information obtained, this must be reported to the FC Team as soon as reasonably practicable. The FC Team will assess whether this is required to be reported to the relevant country registry for further investigation or whether any further action needs to be taken in relation to the counterparty, such as the raising of a SAR.

Where specific confidentiality requirements or non-disclosure requirements apply to a counterparty relationship, the FC Team must consult with T&S Legal, prior to making this disclosure.

[37] For example, a material discrepancy would arise when there is a different person (legal or natural) identified from counterparty due diligence, compared to the information on the official register.

Note, reliance may not be placed solely on the beneficial ownership register extract for verification of the identities of UBOs and Ultimate Controllers. Identities must be verified through the use of independent, reliable documentation as set out in Approved Sources List.

7.7. Complex ownership structures

The ownership structure of an entity should identify the different levels of ownership, indicating how much is owned by each entity or individual at each layer. A counterparty's ownership structure must be assessed to identify the presence of any characteristics or beneficial owners whose legal form or jurisdictions may increase the counterparty's inherent Financial Crime risk.

There are certain entity or shareholding types where the true beneficial ownership or control may be difficult to identify. As a result, these may present a higher inherent Financial Crime risk and where these are found in an ownership structure, these could result in the overall ownership structure being classified as complex. Analysts should note that these complex structures may be for valid legal and commercial reasons such as efficient tax planning.

A counterparty is considered to have a complex ownership structure when two or more of the following types are identified in the ownership chain, or unless otherwise stated below:

- Holding or "shell" companies: the purpose of a holding company is to own the shares of other companies rather than to conduct commercial business or activities. The presence of holding companies can be common and is not always considered to be complex. However, it will constitute a complex ownership chain where there is more than one holding company within the ownership chain and the holding companies are incorporated in more than one jurisdiction

- Sovereign Wealth Funds ("SWF"): SWFs are owned by national governments and there is a potential that these may be used to meet political rather than financial objectives;

- Special Purpose Vehicles ("SPV"): legal entities set up for a specific and sometimes temporary purpose, normally to finance a project and typically in offshore jurisdictions. SPVs structures can be complex and make ownership difficult to trace (see section 10.4 for further guidance);

- Trusts: identifying who benefits from a trust can be challenging as the beneficiaries are not always a named individual but can be a whole family or defined group of people and the information is not typically available; or

- Nominee shareholders: named individuals or entities who hold the shareholding on behalf of the true beneficial owner. In such cases the true beneficial owner may be more difficult to determine.

Where an ownership structure appears to be complex, this does not automatically result in increased Financial Crime risk. However, the Business Line must review and understand the nature of the ownership structure and document the rationale for the structure in the counterparty KYC file.

7.8. Opaque ownership structures

Where the ownership is considered to be complex and there is no commercial or legal rationale for the complexity, or where the UBO(s) and/or Ultimate Controller cannot be identified, the ownership structure must be classified as opaque. The existence of unregistered bearer shares (see section 7.9 below) is automatically considered to constitute opaque ownership. Where there is an opaque ownership structure, this automatically increases the risk rating of the counterparty to High Risk and will require EDD measures to be applied.

Opaque ownership must be escalated to the Head of Financial Crime or delegate for further guidance.

7.9. Bearer shares

For counterparties who issue or who, based on their constitutional documents, are permitted to issue bearer shares, or where it becomes known that bearer shares are within the ownership chain, the Business Line must confirm with the counterparty whether bearer shares have been issued, and if so, establish if the shares are held with a registered custodian (registered bearer shares) or not (unregistered bearer shares). If bearer shares have not been issued, the Business Line should obtain and undertaking from the counterparty that they will be notified if bearer shares are issued.

Depending on the type of bearer share, the Business Line must either:

a) Registered bearer shares:

- confirm ownership percentage held by each owner;
- confirm the amount and to whom the shares have been issued/given;
- obtain proof of custodian's registered or regulated status, if applicable; and
- obtain an undertaking from the custodian, such that the custodian must inform T&S as soon as possible of any changes in ownership structure.

b) Unregistered bearer shares:

- confirm ownership percentage held by each owner;
- confirm the amount and to whom the shares have been issued/given;

- obtain an undertaking from a Director or Company Secretary of the counterparty, that they will inform T&S of any changes in the ownership structure as soon as possible; and
- obtain HRCC approval for the counterparty relationship[38].

Where unregistered bearer shares are also found in a counterparty's ownership structure, this will result in the counterparty's ownership structure being considered as opaque.

Where publicly listed entities eligible for SDD issue bearer shares (e.g. in certain EU jurisdictions where bearer shares may be issued but are required to be immobilised), these may be treated as registered bearer shares and HRCC approval is not required unless advised by the FC Team.

7.10. Trusts and foundations

T&S does not typically directly contract with trusts and foundations as counterparties but trusts and foundations may form part of a counterparty's ownership structure. Where a trust exists in an ownership structure, as set out in section 7.7, this will not automatically make the ownership complex or opaque, but this must be considered in light of other information held about the counterparty.

Trusts and foundations can be used to obscure beneficial ownership of assets and may lack transparency regarding source of wealth and funds. Therefore, trusts may present a higher inherent Financial Crime risk. Trusts are frequently associated with tax planning and as such these entities may present an increased tax evasion risk.

There are many types of trusts and foundations and it is important to understand and document the type of trust e.g. charitable, private, discretionary and consider whether it is reasonable that a trust is the beneficial owner of a counterparty. Business Lines must understand those individuals who created and benefit from the trust (or foundation) and those that control it on a day to day basis and obtain sufficient documentation to understand the reason for use of a trust, the Source of Wealth ("SoW") and Source of Funds ("SoF") used to establish the trust by the settlor.

A trust will typically have the following parties involved:

- settlor(s) – the entity or person(s) who established the trust and "settled" the funds or assets into the trust;

- trustee(s) – the entity or person(s) who are tasked with the management of the trust in accordance with the settlor's wishes;

[38] HRCC approval is not required if the counterparty has the ability to but has not yet issued bearer shares. If bearer shares are subsequently issued, this a trigger event for an ODD review (see section 12) and Business Lines should notify the FC Team accordingly.

- protector or controller, if any – is a person or entity who has powers under the trust deed to control or direct the actions of the trustees; and

- beneficiaries – is a defined list of persons who can benefit from the trust or a class of persons where the individuals who will benefit have yet to be determined or where their interest has not yet vested.

The individuals above, or any other identified individuals who control or benefit from the trust, are all considered UBOs and must be subject to the requirements of these Standards. Where a trust has been set up for a class of beneficiaries, it is not necessary to identify all individuals within the class. Instead, the Business Line must identify the scope and nature of the class which is typically found in the trust deed or equivalent document.

Where there are a large number of named beneficiaries to a trust, at a minimum, those whose interest exceeds the 10% or 25% beneficial ownership threshold, and whose interested has vested (i.e. they entitled to access or have already withdrawn a benefit from the trust) must be identified, verified and screened in accordance with these Standards.

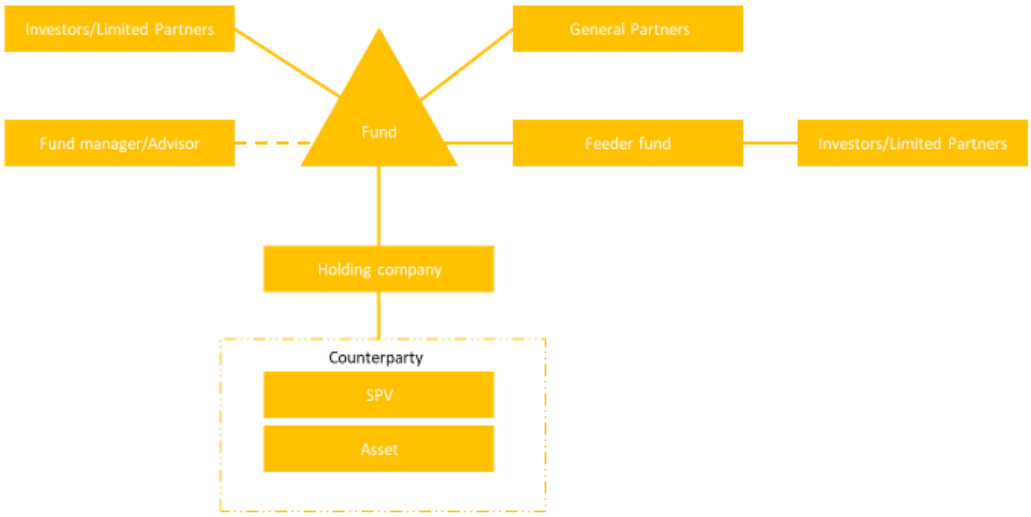
Trustees may be individuals, or entities. Where a trustee is an entity e.g. a law firm, trust and company services provider or family office, Business Lines must understand the ownership and control of the entity and must treat the UBO(s) and Ultimate Controller, as UBOs of the Trust in line with these Standards (see section 6.3).

Where information on trusts, trust assets, SoF, SoW or beneficiaries is refused for confidentiality or privacy reasons, Business Lines must consult with the FC Team for guidance.

7.11. Funds

T&S does not typically directly contract with funds as counterparties, but a fund can form part of a counterparty's ownership structure. Where a fund exists in an ownership structure, this will not automatically make the structure complex or opaque, but this must be considered in light of other information held on the counterparty.

Funds, particularly private equity funds or unregulated funds, may share common characteristics with trusts and foundations, including a lack of transparency around ownership or SoW. As a result, these entities present a higher inherent Financial Crime risk. A typical, basic private fund structure is set out below:



Where a counterparty is owned by a fund structure or multiple fund structures, the ownership is likely to be complex and contain multiple layers and sub-funds or SPVs. Funds are typically formed as Limited Partnerships, with a large number of intermediate entities in the ownership chain between the counterparty and the Limited Partners (i.e. the investors in or owners of the fund assets) and a Fund Manager (or General Partner) that manages the day to day business of the fund on behalf of the investors.

Business Lines must obtain sufficient documentation to understand the ownership and control of the fund, including the identification of the Fund Manager and any additional Fund Advisor. For larger funds, this information would typically be found on the Fund or Fund Manager's website or in its Annual Report, or the fund prospectus.

Where a Fund is managed or advised by a Fund Manager who is regulated by an approved regulator as set out in Appendix 6, Business Lines may accept an attestation from a Director of the regulated Fund Manager, confirming the ownership or control structure of the fund, the identity of the directors or UBOs and whether there are any individuals that own or control more than 25% or more than 10% of the fund. Where this is confirmed, there is no need to add all of the intermediate layers or shareholders in the fund to the KYC file as beneficial owners.

The Fund Manager and the Fund Advisor at a minimum, must be added to the KYC file as related parties, as well as all UBOs and any Ultimate Controller(s). The Business Line must consult with the Fund Manager or Fund Advisor as required, to determine whether any individuals employed by those entities, should be considered an Ultimate Controller.

8. SCREENING REQUIREMENTS

8.1. Scope

The Business Line is accountable for ensuring that all counterparties and their related parties are screened in accordance with these Standards. The FC Team is responsible for the performance of screening as part of its Financial Crime risk review and assessment of the counterparty.

8.2. Purpose

All counterparties and their related parties must be screened as part of KYC measures to identify any potential PEPs or sanctions connections. For SDD, CDD and EDD the counterparty, and certain related parties, must also be screened for Financial Crime adverse media, in accordance with section 8.3.3. These are important factors which need to be considered when assessing the overall Financial Crime risk of a counterparty.

8.3. Definition

8.3.1. Sanctions screening

Sanctions screening is undertaken to identify any entities and/or individuals which have a connection to a sanctioned country, sanctioned entity, sanctioned person or sanctioned or restricted activity, also referred to as "nexus".

Sanctions risk associated with a counterparty may arise even where the direct counterparty is not sanctioned but there is another element in the transaction or business relationship with a connection to a sanctioned country (GEC or HRC) or sanctioned party (referred to as "Indirect Sanctions Nexus").

As part of KYC measures, Business Lines should be vigilant for sanctions and trade controls red flags and should not solely rely on screening of counterparty and related party names to identify sanctions nexus.

If not indicated from KYC information, counterparties should be asked to confirm whether they trade with or operate in GECs and HRCs and this should be recorded in the KYC file.

8.3.2. PEP screening

PEP screening is undertaken to identify any individuals who are PEPs. Where the screening results identify any potential matches, the FC Team must follow the requirements set out in section 8.5 to discount or confirm any matches.

Section 5 sets out the parties required to be screened, depending on the due diligence level applied. A summary is given in 8.4 below.

8.3.3. Financial Crime adverse media screening

Financial Crime adverse media or negative news is unfavourable information related to either the counterparty or any related party such as its directors, its parent companies, shareholders or UBOs. Section 5 sets out the parties required to be screened, depending on the due diligence level applied. A summary is given in 8.4 below.

For BDD there is no requirement to conduct adverse media screening. In addition, there is no requirement to conduct adverse media screening on national or regional governments e.g. the government of France, if they are the beneficial owner or Ultimate Controller of a counterparty.

Where the screening process identifies any potential Financial Crime adverse media, the screener must follow the requirements set out in section 8.5 to discount or confirm any matches.

8.4. Timing of screening

At a minimum, screening is conducted on all counterparties, and related parties (as defined within section 6), where required, at the following intervals:

- at the point of the counterparty onboarding, prior to establishing the relationship; and
- automatic overnight screening via GoldTier for those counterparties contained within this system.

In addition, Financial Crime adverse media screening is re-performed as part of the ODD re-review of a counterparty file or more frequently where placed under enhanced monitoring measures by the FC Team or the HRCC. For PEP and sanctions, as this screening is conducted daily, there is no need to re-perform the screening during an ODD re-review. Instead, the FC Team must review the most recent daily screening results to identify if there are any red flags which need to be considered as part of the re-review.

8.5. Screening requirements

The extent to which entity and related party names are required to be screened, depending on the level of due diligence, is set out in section 5. A summary is provided below for reference.

PEP and Sanctions screening

	BDD	SDD – Publicly listed	SDD – Regulated FIs	CDD	EDD
Entity legal name[39]	✓	✓	✓	✓	✓
Entity trading name(s)	N/A	N/A	N/A	N/A	✓
Board of Directors current names	N/A	✓	✓	✓	✓
All UBOs	N/A	N/A	✓	✓	✓
Ultimate Controllers	N/A	N/A	✓	✓	✓
Shareholders between entity and UBOs	N/A	N/A	N/A	✓	✓
For SPVs only, legal name of sponsoring entity	N/A	N/A	✓	✓	✓
Branch Managers (where required in section 4.8)	N/A	N/A	N/A	✓	✓

Adverse media screening

	BDD	SDD – Publicly listed	SDD – Regulated FIs	CDD	EDD
Entity legal name[39]	N/A	✓	✓	✓	✓
Entity trading name(s)	N/A	N/A	N/A	N/A	✓
Board of Directors current names	N/A	N/A	N/A	N/A	✓
PEPs only (Directors, UBOs and Ultimate Controller)	N/A	✓	✓	✓	✓
All UBOs	N/A	N/A	N/A	N/A	✓
Ultimate Controllers	N/A	N/A	N/A	N/A	✓
Shareholders between entity and UBOs	N/A	N/A	N/A	N/A	N/A
For SPVs only, legal name of sponsoring entity	N/A	N/A	N/A	✓	✓

The names screened must exactly match the official legal names as contained in the approved source used to identify or verify the information obtained.

8.6. Review and dispositioning of potential matches

A review and assessment of any confirmed match associated with a counterparty needs to be undertaken to determine whether it is true or false, and if true, whether it poses any incremental Financial Crime risk.

[39] For CDD and EDD, former legal names in the past 12 months should also be screened where identified.

All screening matches must be reviewed (unless otherwise stated in relevant operating procedures) to determine if any can be discounted as a false match. A false match is a where a match does not directly relate to a counterparty or related party.

Where matches cannot be discounted due to insufficient information, the Business Line must obtain additional information or documentation in order to discount the match. Where a match is confirmed, the next steps depend on the nature of the confirmed match:

- where the screening process results in a confirmed PEP match, the FC Team must apply the PEP requirements set out in section 9; or

- where the screening process results in the identification of a sanctions nexus, the FC Team or Business Line must follow the requirements in section 8.

- Where the screening process results in potential Financial Crime adverse media, the requirements in section 8.6.1 and Appendix 4 must be followed.

8.7. Risk assessment of Financial Crime adverse media

The following steps must be applied, at a minimum, when assessing the risk posed.

- Credibility of the source: Review and confirm the credibility of the source to confirm whether the content reported in one or more credible sources such as the Financial Times or Wall Street Journal, industry news wires Bloomberg or Reuters and independent news website such as BBC News or Channel News Asia or was it from less credible sources such as unsubstantiated blogs?

- Age of the source: When determining the relevance of any confirmed Financial Crime adverse media, the age of the relevant source must first be considered as follows:

    - Entities: where the adverse media relates to an entity, only adverse media that is five years old or less should be considered. Where a source is more than five years old, it should not be considered in the risk review unless there is evidence that judicial processes are still being pursued; or

    - Individuals: where the adverse media relates to an individual, only adverse media that is ten years old or less should be considered, unless there is evidence that a matter is ongoing and the individual still has significant control or influence over the counterparty i.e. is a Director, Ultimate Controller or UBO.

- Status of the adverse media: Review and confirm if the Financial Crime adverse media is proven or an allegation.
    - If this is an allegation, is this supported by other media?
    - Where this is proven, has the Financial Crime risk been mitigated e.g. were the responsible persons removed from positions?

- Nature of the adverse media: Assess the nature of the Financial Crime risk and if this relates to a one-off incident or systematic issue:
    - What type of Financial Crime does the adverse media relate to;
    - Does this relate to a one-off incident or systematic failure; and
    - Has the counterparty taken any action to address the adverse media e.g. if the adverse media is related to a sanctions regulatory fine, is there evidence that remedial action was undertaken?

- Proximity of adverse media to specific counterparty: Assess the relevance of the adverse media to the specific counterparty and our business activities with it:
    - Does the adverse media relate to the specific counterparty or a related party (director, UBO, beneficial owner, subsidiary or another affiliate);
    - If it relates to a related party, is it suitably remote/ringfenced from our counterparty to be mitigated?

Each step must not be considered in isolation and the FC Team must consider all steps as part of the risk assessment.

8.7.1. Classification of materiality

Following the risk assessment, true matches must be classified as either:

- Material Financial Crime adverse media: which refers to information which would impact on a counterparty's risk rating; or
- Immaterial Financial Crime adverse media: which refers to information which would not impact on a counterparty's risk rating.

Examples of material and immaterial adverse media are set out in Appendix 4.

8.7.2. Material Financial Crime adverse media

Where material Financial Crime adverse media is confirmed, the counterparty must be classified as High risk and EDD measures must then be applied.

All counterparties with confirmed material Financial Crime adverse media must be escalated to the HRCC. The HRCC has the authority to approve counterparties with or without conditions, request additional information, prevent new business or exit counterparty relationships.

The FC Team, under its documented MoA, has the authority to approve the continued acceptance of adverse media previously risk-accepted by the HRCC, where:

- For existing counterparties undergoing ODD, there are no material changes to the facts of the adverse media, or other red flags or developments that may otherwise impact the previous risk appetite decision; or
- For new counterparties with adverse media previously identified for connected entities and related parties, the facts and impact of the adverse media on the new counterparty are the same and there are no other red flags or developments that may otherwise impact the previous risk appetite decision.

However, the rationale for not seeking re-approval from the HRCC must be clearly documented in the risk review.

8.7.3. Immaterial Financial Crime adverse media

All counterparties where the Financial Crime adverse media is immaterial and where the counterparty overall is either Low or Medium risk will be subject to approval by the FC Team in line with the approved MoA.

If immaterial adverse media is found on the counterparty, the rationale for continued use of BDD, SDD or CDD must be documented in the risk review of the KYC file.

8.8. Review and escalation of potential sanctions matches

Where screening identifies a potential Sanctions Nexus, the FC Team, in consultation with the T&S TC Team and Business Line where required, must review the hit to confirm whether it can be discounted and if not, whether business activities may continue.

Confirmed Sanctions or Indirect Sanctions Nexus will be assessed by the FC Team and will be escalated to the TC Team for advice in line with documented procedures.

It is the responsibility of the Business Line or relevant function (e.g. Credit or Finance) to follow the requirements of the T&S Sanctions Compliance Policy and any relevant SECO Trade Controls requirements within the RDS Ethics and Compliance Manual, with regards to business activities with counterparties with a Sanctions or Indirect Sanctions Nexus.

The TC Team advice must be stored on the counterparty KYC file.

The commencement or continuation of business with a counterparty with identified Sanctions or Indirect Sanctions Nexus, must be submitted to the HRCC for a risk appetite discussion regarding the acceptance of the counterparty relationship per the requirements set out in section 14.

9. POLITICALLY EXPOSED PERSONS ("PEP")

9.1. Scope

This section sets out the minimum requirements to be applied where a PEP has been identified.

9.2. PEP risk overview

PEPs may pose increased Financial Crime risk as their positions make them vulnerable to corruption and there is a potential that these individuals may misuse their power and/or influence for gain or personal advantage, for either themselves, or family members or known close associates. A PEP designation also covers a PEP's immediate family members and known close associates due to the potential risk that these individuals may be used to conceal funds or assets that have been misappropriated and a PEP has abused an official position.

Where an individual holds a PEP status, it means that additional measures are required to understand the risks presented, as PEPs do not present the same level of risk.

9.3. PEP relationships

The entity with which T&S establishes a business relationship, either commercial or contractual, is the direct counterparty of T&S. A PEP is an individual associated with the counterparty and with whom T&S is considered only to have an indirect relationship arising from the business relationship formed with the counterparty – there is no direct relationship formed with the PEP.

In addition, whilst a PEP may be associated to a counterparty, the counterparty itself is not treated as a PEP.

9.4. PEP definitions

T&S has defined a PEP as "*an individual who is or has, at any time in the preceding three years, been entrusted with a prominent public function, or an immediate family member, or a known close associate, of such person*[40] *".*

Prominent public functions include the following[41]:

- Heads of State, Heads of Government, Ministers and Deputy or assistant ministers;
- Members of Parliaments or of similar legislative bodies;

[40] UK Money Laundering Regulation 2017 35(12)
[41] As set out in JMLSG Part 1, section 5.5.17

- Members of supreme courts, of constitutional courts or of other High level judicial bodies the decisions of which are not subject to further appeal, except in exceptional circumstances;

- Members of courts of auditors or of the boards of central banks;

- Ambassadors, Chargés d'Affaires and High ranking officers in the armed forces (other than in respect of relevant positions at Community and international level);

- Members of the administrative, management or supervisory boards of State-owned enterprises (see section 10.8 for definition); and

- Directors, deputy directors and members of the board or equivalent function of an international organisation.

Immediate family member of a PEP will include[42]:

- A spouse or partner;

- Children, including step-children, and their spouses/partners;

- Parents and those of a spouse/partner; and

- Siblings and those of a spouse/partner.

Known close associates of a PEP include[43]:

- an individual who is known to have joint beneficial ownership of a legal entity or legal arrangement, or any other close business relations, with a PEP; and

- an individual who has sole beneficial ownership of a legal entity or legal arrangement which is known to have been set up for the benefit of a PEP.

The positions set out above are not a definitive list and there may be other functions or associations that indicate PEP status, particularly in jurisdictions outside of the UK.

Where there is a positive PEP screening hit, but it is unclear whether the individual meets the definition of a PEP under these Standards, Business Lines should consult with the FC Team who may, under their documented MoA, determine whether it meets the definition or whether it may be declassified as appropriate, with appropriate rationale documented on the KYC file.

[42] JMLSG Part 1, section 5.5.17
[43] JMLSG Part 1, section 5.5.17

Whilst the PEP definition above assumes a senior or prominent public role or position, Business Lines must be vigilant for counterparties owned or controlled directly or indirectly, by any public official. If there are any concerns or red flags, in particular in relation to their control or influence over the counterparty, source of funds or evidence of bribery or corruption related adverse media, they should consult with the FC Team for guidance.

9.5. PEP status

T&S considers that an individual holds a PEP status for a minimum of three years following their departure from office. For some individuals, the PEP status may remain for a longer period based on the individual circumstances presented by the PEP e.g. for well-known former PEPs or where a PEP maintains known associations with other prominent PEPs.

Where a PEP is no longer entrusted with a prominent public function, T&S will not consider family members or close associates of the PEP as PEPs themselves.

9.6. PEP risk assessment

As a PEP relationship is always considered to be higher risk, additional steps must be applied to mitigate this risk. Higher risk is not, however, the same as High Risk. This also does not mean that the associated counterparty is automatically considered as High Risk solely due to the presence of a PEP connection. An assessment is required to first determine the level of risk presented by the PEP before the counterparty's overall risk rating is determined. Individual PEPs are classified as either Low or High Risk.

Where a PEP is determined to be High risk through the risk assessment, EDD must then be applied to the counterparty as a whole.

In order to perform a PEP risk assessment, it is important to understand the level of seniority and influence of the current public role(s) of the PEP, their role and level of control in relation to our counterparty and the T&S business with it, whether there is any adverse media or sanctions concerns regarding the PEP, and then answer and document the following:

1. Does a related party of our counterparty meet the definition of a PEP (or an immediate family member or close associate of a PEP) per these Standards?
    a. Yes – go to question 2
    b. No – not a PEP

2. Is the PEP still in the public role that gives rise to their PEP status or did they leave it recently i.e. within the past 3 years?
    a. Yes
        i. If the related party of our counterparty is an immediate family member or close associate of a PEP, has the PEP left the public role that gives risk to its PEP status?
            1. Yes – family member or close associate is not classified as a PEP
            2. No – go to question 3

    b. No – not a PEP, as long as political influence is no longer present

3. Is the PEP a UBO (NB. this does not include state-owned companies where the UBO is the state) or Ultimate Controller of our counterparty?
    a. Yes
        i. Is the counterparty eligible for SDD and the PEP is the Chairman or CEO who has been classified by default as UBO/Ultimate Controller due to no "true" UBO?
            1. Yes – go to question 4
            2. No – PEP is a High Risk PEP

    b. No – go to question 4

4. Is the PEP a related party of a counterparty registered or operating in an EDD country, or do they have significant political influence i.e. a prominent government role in a High FC (see Glossary) Risk or EDD country?
    a. Yes – PEP is a High Risk PEP
    b. No – go to question 5

5. Is the PEP subject to material, unmitigated Financial Crime adverse media or sanctions?
    a. Yes – PEP is a High Risk PEP
    b. No – go to question 6

6. Is there any other unmitigated Financial Crime risk concern regarding the PEP, its influence over our counterparty, the T&S business or its political influence?
    a. Yes – PEP is a High Risk PEP
    b. No – PEP is a Low Risk PEP

The rationale for the PEP risk classification, including the supporting analysis used to declassify individuals as PEPs either due to leaving office or not meeting the definition of a PEP, or to downgrade a PEP from High to Low Risk, must be documented on the KYC file. All PEP relationships require approval from the FC Team in line with the documented MoA.

9.7. PEP due diligence requirements

9.7.1. Requirements

T&S must identify all PEPs related to a counterparty regardless of the jurisdictions connected to the PEP, in line with the related party guidance information requirements in section 5. At a minimum, the following steps must be applied to all PEPs:

REQUIREMENT
1. Identify, and verify where required, the PEP in line with the related party requirements in section 6.3[44]
2. Undertake a PEP risk assessment as set out in section 9.6 above
3. Determine the risk rating applied to the PEP, being either Low or High Risk
4. Document the rationale behind the PEP risk classification within the counterparty KYC file

The assessment of and rationale for a PEP's risk rating must focus on the Financial Crime risk associated with the PEP and the extent of their influence over the counterparty and the specific business being undertaken with T&S. It is not acceptable for this rationale to be based solely on the commercial advantages of the counterparty relationship.

For those PEPs determined to be High risk, the following steps must also be applied in addition to the steps set out above:

REQUIREMENT
▪ Where the High Risk PEP is a UBO as set out in section 7.4, verification of the PEP's identity along with identification and verification of SoW must be undertaken.[45]
▪ Where a High Risk PEP is not a UBO, determine if SoW is required on a risk sensitive basis for the PEP. The rationale for the decision must be documented within counterparty KYC file.
▪ Undertake EDD measures on the associated counterparty as set out in these Standards.
▪ Submit counterparty file for Senior Management approval via the HRCC.

Where a PEP's SoW is <u>not</u> relevant to the relationship, for example, their personal wealth is not used to fund the business, and there are no other risk factors (e.g. adverse media or high risk factors in relation to the counterparty), the PEP's SoW does not need to be verified. However, the rationale for not verifying SoW must be documented in the counterparty KYC file.

[44] Where required information is refused for a PEP, guidance must be sought from the FC Team.
[45] Where source of wealth cannot be obtained for a PEP, guidance must be sought from the FC Team.

9.7.2. Risk rating

Based on the risk assessment, PEPs must be classified as either High or Low Risk. Where there is more than one PEP associated with a counterparty, consideration must be given and documented as to the need to increase the risk rating of the counterparty to High based on the information presented.

9.7.3. Enhanced Due Diligence ("EDD") measures

Only when a PEP is determined to be High Risk, will this result in the associated counterparty being automatically High Risk. In this scenario, the full set of EDD measures must be applied to the counterparty and PEP as set out in these Standards.

Where a PEP is determined to be Low Risk, and the counterparty itself is considered overall as either Medium or Low Risk, EDD measures are not required on the counterparty. However, the risk of the PEP and the rationale for not performing EDD measures on the counterparty must be documented. Where EDD measures are required, then both the PEP and/or counterparty classification of Low Risk is not appropriate.

9.8. PEP approval

9.8.1. Low Risk PEPs

The Head of Financial Crime or appointed delegate(s) can approve all Low Risk PEPs and the rationale for any decision must be recorded in the counterparty KYC file. Approvers must record the date of the PEP risk rating and approval and consider and document the following:

- whether the rationale included in the risk review supports the PEP's risk rating and therefore whether the PEP risk rating is appropriate; and

- confirm if the ODD frequency for the PEP and counterparty is appropriate as per section 12.

Quarterly Management Information ("MI") on the number of Low Risk PEPs approved will be provided by the FC Team to the HRCC for noting by senior management.

9.8.2. High Risk PEPs

All counterparties with identified High Risk PEPs must be escalated to the HRCC for senior management approval. The HRCC has the authority to approve counterparties with PEP relationships with or without conditions, request additional information, prevent new business and exit counterparty relationships under the risk-based approach. Evidence of HRCC approval of all High Risk PEPs must be included in the counterparty KYC file.

Where a PEP has been approved by the HRCC previously in relation to a specific counterparty, it does not need to be reapproved by the HRCC during subsequent ODD reviews, or during KYC on new counterparties with the same ultimate beneficial ownership as the previously approved counterparty, as long as there are no new Financial Crime red flags in relation to the counterparty or PEP that would require HRCC discussion. For example, if a PEP is identified and approved by the HRCC for a state-owned company, other companies owned by the same state with the same PEP, do not require HRCC approval in the absence of any other EDD risk factors.

In addition, where a PEP relationship was previously classified as High Risk but where the risk rating has been determined to have changed to Low, this downgrade must be approved by the Head of Financial Crime or delegate as set out in the FC Team Manual of Authorities ("MoA"), with evidence of approval stored in the counterparty KYC file.

9.9. SECO requirements for politically exposed counterparties and mitigation of bribery and corruption risk

The following approach has been agreed between T&S Compliance and SECO regarding the application of SECO due diligence rules to T&S counterparties that are politically exposed or who perform GI services for T&S.

9.9.1. GIs

- For GIs in High ABC Risk countries (as set out in the RDS Ethics and Compliance Manual) that are subject to KYC under these Standards, there is no automatic requirement to undertake EDD in the absence of other T&S EDD override red flags (e.g. High Risk PEPs, material unmitigated Financial Crime adverse media or opaque ownership).
- As part of the SECO Compliance questionnaire and memo and ABC SME approval process, SECO may require additional ownership information from the T&S business on a case by case basis.

9.9.2. Counterparties owned by Government Officials ("GO")

- SECO has specific rules around counterparties owned by GOs which, similar to GIs, include the need in some instances for a Compliance Questionnaire and memo, as well as ABC SME approval.
- T&S may follow these KYC Standards regarding identification of PEPs, noting that the SECO definition of GO is slightly different. The T&S PEP definition will be used as equivalent to the SECO definition of GO.
- A separate Compliance questionnaire and memo is not required for T&S counterparties owned by PEPs, who are subject to KYC under these Standards.

- HRCC approval (required for all PEPs who are UBOs of counterparties which are automatically classified as High Risk PEPs), will be considered by the SECO ABC SME as a proxy for the SECO ABC SME approval. HRCC submission must explicitly discuss the risk of ownership of a counterparty by a PEP.

The SECO ABC SME is a recipient of the HRCC agenda and minutes as an "informed" party and may attend and contribute to discussion on such counterparties as required.

10. FURTHER GUIDANCE PER ENTITY TYPE

10.1. Overview

The following section sets out additional guidance and requirements specific to particular counterparty types, primarily based on legal form and/or nature of each entity's business activities. Where a counterparty type is identified that does not align with those set out in this section, the FC Team should be consulted for further guidance.

10.2. Private and unlisted companies

A private company is a company limited by shares or guarantee whose securities are either not listed or not traded on an approved exchange or market. These entities are subject to a lower level of disclosure as compared with publicly listed entities. As a result, their ownership and control and source of wealth may be less transparent and there is an increased inherent Financial Crime risk.

For private entities who are registered in countries with publicly available (either free of charge or otherwise) company register and/or beneficial ownership registers, a search of the relevant register should always be undertaken to ensure the company is properly registered, active and to identify and verify basic information.

The table below shows the minimum requirements for related parties.

	CDD		EDD	
Requirement	Identify	Verify	Identify	Verify
Board of Directors or equivalent	✓	N/A	✓	✓ *(minimum two)*
Beneficial Owners more than 25% (CDD)/more than 10% (EDD)	✓	N/A	✓	N/A
UBOs more than 25% (CDD)/more than 10% (EDD)	✓	✓	✓	✓
Ultimate Controller(s)	✓	✓	✓	✓

10.3. Partnerships and unincorporated associations

Partnerships differ from corporate entities as the equity is held by partners (or members) who provide the capital and share the responsibility of running the business based on an agreement between its members. Partnerships may be incorporated and have a distinct legal form, for example LLPs. However, the concept of partnerships also includes unincorporated associations with no distinct legal form. In addition, partnerships are not subject to the same level of disclosure and are less transparent when compared to regulated or listed entities. As a result, these entities may present a higher inherent Financial Crime risk. When undertaking KYC on a partnership, it is important to understand the type of partnership, its ownership and control structure and the roles of any partnership management boards to determine the individuals who may be considered related parties.

Appendix 7 sets out additional guidance on different types of partnership arrangements and guidance on individuals and entities to be considered as a UBO, Ultimate Controller or director.

The table below shows the minimum requirements for related parties.

	CDD		EDD	
Requirement	Identify	Verify	Identify	Verify
Partnership Board or equivalent	✓	N/A	✓	✓ *(minimum two)*
UBOs more than 25% (CDD)/more than 10% (EDD)	✓	✓	✓	✓
Ultimate Controller(s)	✓	✓	✓	✓

10.4. Special Purpose Vehicles ("SPVs")

SPVs or Special Purpose Entities ("SPEs"), collectively referred to hereafter as SPVs, are legal entities (either privately or publicly owned) set up for a specific purpose. Typically, a SPV is used by a parent company (i.e. the "sponsoring entity") to ringfence or securitize specific assets, e.g. vessels or revenue streams so that they are held "off-balance sheet" from the parent company.

SPVs typically have limited activities, i.e. the acquisition or financing of specific assets, and are used to isolate risk. The ownership of SPVs can be complex, particularly where SPVs are "orphaned" i.e. the equity is held by a third party with no legal relationship to the actual true parent or "sponsor" of the SPV. While this third party legally "owns" the equity of the SPV, the way in which their ownership is structured gives them no control over the SPV. Therefore, these third parties are effectively "nominees" for the beneficial owner.

Orphaned structures allow lenders to separate the asset finance, from the asset user(s), thus enabling them to move the asset to other users(s) should the situation arise (e.g. bankruptcy of a user), without having to recreate a new SPV and/or re-raise new loans.

SPVs may present increased Financial Crime risk if they are used to obscure assets from their true beneficial ownership, or to commit tax evasion. So, Business Lines must be vigilant for red flags in relation to this entity type and must fully understand and document the purpose of the SPV and the rationale for using it.

Within T&S, SPVs are commonly used by shipping/vessel owners or managers to ringfence ownership and cashflows of a vessel in a single entity but may be found in all Business Lines. Where a counterparty contracts with T&S on behalf of a ship owner or other third party, i.e. as an agent, the underlying ship owner or third party on whose behalf the counterparty is transacting with T&S, must be subject to KYC measures in line with these Standards.

SPVs must be subject to either CDD or EDD in line with their entity type and risk rating per the requirements set out in section 5 and the guidance in this section. For SPVs subject to KYC, it is important to identify and document the following additional requirements on the KYC file:

- The purpose of the SPV and rationale for using the structure;
- The legal and beneficial ownership of the SPV, including the identity and ownership of the parent or "sponsoring entity" of the SPV where different to the legal owners; and
- The nature of our contractual/payment relationship with the SPV.

The table below shows the minimum requirements for related parties.

	CDD		EDD	
Requirement	Identify	Verify	Identify	Verify
Sponsoring entity (if not the same as the legal owner)	✓	N/A	✓	N/A
Board of Directors or equivalent	✓	N/A	✓	✓ *(minimum two)*
Beneficial Owners more than 25% (CDD)/more than 10% (EDD)	✓	N/A	✓	N/A
UBOs more than 25% (CDD)/more than 10% (EDD)	✓	✓	✓	✓
Ultimate Controller(s)	✓	✓	✓	✓

10.5. Joint Ventures ("JV")

A JV is a commercial arrangement between two or more participants who agree to co-operate to achieve a particular objective. A JV may be formed by establishing a separate legal entity (e.g. incorporated company, limited partnership) or may be an unincorporated joint arrangement based on a contractual agreement e.g. a production sharing agreement.

T&S may participate in a joint venture as a partner in order to expand, develop new products or markets or may be undertaking T&S business with an already-established JV.

The following requirements apply.

- A. Trading with a JV (of which Shell is a member): Where the JV is 50% or more owned and controlled by RDS, BDD may be applied in line with the requirements in section 5. Where BDD is not applicable, KYC must be applied in line with these Standards. RDS internal company file documentation may be relied on to identify and verify the JV and its related parties, where available and where information is confirmed by the RDS shareholder representative (or equivalent), as current.

- B. Shell joining as party to a joint venture: Where forming a new JV in which Shell will be a member, KYC must be undertaken on each of the JV partners in line with their underlying entity type and risk score as outlined in these Standards.

- C. Trading with a JV (of which Shell is not a member): When trading with a JV in which Shell is not a member, KYC must be undertaken on the JV in line with its underlying entity type and risk score as outlined in these Standards.

10.6. Natural persons (individuals), including well-known persons

T&S does not typically directly establish or maintain relationships with individuals. Therefore, due to the unusual nature of these relationships, individuals present a higher inherent Financial Crime risk to T&S e.g. a consultant or broker who is a sole trader. Where this occurs, the individual is considered to be a counterparty and the requirements below must be applied.

The tables below show the minimum requirements for identifying and verifying individuals.

	CDD		EDD	
Requirement	Identify	Verify	Identify	Verify
Full legal name	✓	✓	✓	✓
Government issued ID number or equivalent	✓	✓	✓	✓

	CDD		EDD	
Requirement	Identify	Verify	Identify	Verify
Residential address[46]	✓	✓	✓	✓
Date of Birth[46]	✓	✓	✓	✓
Nationality	✓	N/A	✓	N/A
Purpose and nature of intended relationship	✓	N/A	✓	N/A
Source of funds ("SoF")	✓	N/A	✓	✓
Source of wealth ("SoW")	✓	N/A	✓	✓

Note, where it is identified that individuals who are counterparties or UBOs of counterparties, are deceased and an individual's estate is being dealt with by a third party such as an executor, the executor is deemed to assume the rights of the counterparty (or UBO) until such time as the estate has been settled. If the executor undertakes business with T&S on behalf of the estate, they are subject to KYC in line with these Standards.

10.7. Well-known persons

A well-known person (typically a high net worth individual or public figure) is defined as an individual who has a substantial, well-known and widely reported public profile e.g. celebrities, members of royalty or prominent entrepreneurs.

Business lines must have access to sufficient information to enable them to know and understand the business relationship with the well-known person and be able to adequately verify their identity. Due to their prominent status, T&S may verify the identity and SoW (where required) of these counterparties using credible publicly available sources rather than approved documentation sources, if external documents or media sources can adequately support a well-known person's identity and wealth -generating activities. Where a well-known person is a PEP, use of non-approved verification sources requires the approval of the Head of Financial Crime (or delegate).

Business Lines may be aware of special sensitivity in relation to a counterparty's legitimate commercial activities or need for personal security. Care must be exercised to ensure requests for confidentiality do not lead to unwarranted levels of secrecy that suit potential criminal intentions.

[46] Whilst date of birth and residential address needs to be identified for all counterparties who are individuals, where a correctly certified photographic government issued ID is used for verification of full name and either date of birth or residential address, there is no requirement to verify date of birth AND residential address

10.8. State owned entities

A state-owned entity is a legal entity created by a government to undertake commercial activities on behalf of the government e.g. National Oil Companies. These entity types are not to be confused with other "public" companies (private or publicly listed), which may happen to have a level of state ownership through direct shareholdings by a government.

State-owned businesses may engage in a wide range of activities, some of which might involve higher risk factors. Such entities may be partly publicly funded or may derive some or all of their revenues from trading activities.

A counterparty is state owned where the following shareholding thresholds are held by a state:

- a single government owns more than 50% of the counterparty;
- a single government owns more than 30% of the shares and holds veto rights; or
- a single government can appoint or remove the majority of the board of directors.

State owned entities are subject to the requirements of these KYC Standards in line with their risk assessment and relevant due diligence level. Particular vigilance should be given to the existence of PEPs.

Senior employees e.g. Board Directors or other Senior Management of state-owned entities are likely be classified as PEPs under the PEP definition included in these Standards.

If it has been determined from above that the counterparty is not state owned, an assessment must still be undertaken of all related parties to ensure that there are no PEPs who meet the definition in line with guidance in section 9.

10.9. Public administration bodies, government departments and supranational bodies

Public bodies engaged in public administration are different from state-owned entities which conduct commercial business. Public administration involves a different revenue/payment stream from that of most commercial businesses, as they are typically funded from government sources, or from some other form of public revenues.

Public administration bodies include government departments (including regulatory bodies), publicly-funded educational institutions, hospitals, educational institutions, municipalities (who may be customers of T&S) and similar.

Where T&S has a commercial relationship with counterparties in non-EDD countries, who are public administration bodies (e.g. municipalities or government departments), reliable public sources and official government websites may be used to fulfil documentation requirements for

KYC purposes, such as verification of legal existence, ownership and control, nature of business and directors/Ultimate Controller information.

In addition, there is no requirement to verify the identities of the Board of Directors or Ultimate Controllers (even where they are Low Risk PEPs) of public administration bodies using government issued identification documents, as long as sufficient information is identified to enable screening of the related parties and discounting of any alerts.

These exceptions do not apply to publicly listed or private companies operating a commercial business that may have an element of state-ownership as per section 10.8 above.

10.10. Exchanges

The following risks must be considered and mitigated when on-boarding a commodity exchange, on which a T&S entity will trade; or a central clearing party (CCP) that will be used to clear exchange-traded transactions.

The exchange must be on-boarded in line with its underlying entity type and risk rating in line with these Standards.

The business must understand:

- The regulated status of the exchange for AML/CTF purposes;
- The role/contractual structure of T&S on the exchange and whether it will buy and/or sell, and whether it acts as agent or principal;
- The trading model i.e. how will T&S contract and transact with the exchange, at what point will T&S know who it is matched with, and whether it uses a CCP to settle transactions or settles directly with the underlying buyer/seller;
- The membership admission criteria for the exchange, including the types of members admitted i.e. entities, individuals, and whether they permit cross-border members;
- Whether the exchange and/or CCP has an ABC, Sanctions and AML policy, screens members against OFAC and other sanctions lists, and prevents sanctioned parties from accessing the exchange;
- Whether our contract with the exchange and/or CCP includes the standard T&S ABC and TC clauses; and

- Whether T&S will use any intermediaries, agents or brokers in relation to accessing the exchange.

Where, as a result of the risk assessment of the exchange, there is concern regarding the exchange's membership admission and monitoring controls, or its willingness to agree to relevant T&S contractual provisions regarding Financial Crime prevention, the business must consult with the Compliance Advisory Team or FC Team regarding the extent to which it is necessary to conduct KYC measures on exchange members.

10.11. Banks and other FIs

T&S may form business relationships with banks and other FIs in several ways and the level of due diligence required depends on the nature of the relationship with the bank or FI, which must be understood. The following principles should be applied:

Role	Due Diligence level	Further guidance
Trading counterparty: trading with a commodity trading desk	SDD, CDD or EDD as required	N/A
Vendor: provider of general banking services, including credit or financing to T&S as a customer	BDD as per rules for G&A vendors	N/A
Issues of security/guarantees on behalf of counterparties, where T&S is beneficiary	BDD (non-EDD countries) or reduced EDD as per below	Section 21
Issuers of trade finance LCs on behalf of counterparties, where T&S is beneficiary (i.e. seller)	BDD (non-EDD countries) or reduced EDD as per below	Section 20
Co-lenders or other parties in a structured finance transaction where T&S is one of a syndicate of lenders to a counterparty to acquire or develop an asset, in return for offtake	BDD/SDD or reduced CDD/EDD depending on specific role	Section 22

If banks are used for multiple types of relationship, the highest level of due diligence should be applied.

<u>Reduced CDD/EDD for banks and other FIs in non-trading relationships</u>

Where a bank or other FI (e.g. an investment fund) is used by T&S for non-trading purposes but is subject to CDD or EDD, the entity may be subject to reduced, public-records based CDD and EDD requirements.

This includes:

- Using a full Bankers Almanac report (or equivalent approved third party data aggregator report) and official bank/entity website for identification and verification of the bank's legal existence, active status, nature of business, operating region, legal name, registered and trading addresses, ID number and Source of Funds.
- No requirement to identify full personal information for the Board of Directors, or to verify two directors' identities as long as sufficient information is identified in reliable public sources to enable screening and dispositioning of screening hits.
- Ownership and control verification via reference to the counterparty website and annual report (where available), or a signed attestation from the counterparty (signed by a Board Director, in-house lawyer or qualified accountant), corroborated with public sources.

Requirements to verify the identities of any UBO and Ultimate Controller (excluding the Chairman or CEO) and to verify the Source of Wealth for UBOs (including High Risk PEPs), still apply.

10.12. Counterparties acquired via M&A

When a T&S legal entity acquires a company or group of companies ("acquired business"), either from a third party as part of a Mergers and Acquisition ("M&A") transaction, or from another Shell legal entity ("previous owner"), the Business Line must consult with T&S Compliance in line with the relevant Group Investment Proposal or Deal Approval procedure, prior to the acquisition.

At a minimum, the legal names of all counterparties transacted with by the acquired business, must be screened against applicable sanctions lists prior to said counterparties entering into a business relationship or transaction with T&S (including transactions with the acquired business post-acquisition).

Initial reliance may be placed on screening undertaken by the previous owner, as long as the screening is deemed to be equivalent to the T&S screening standard set out in the T&S Sanctions Compliance Policy and these KYC Standards.

Full KYC in line with the T&S KYC Standards and the risk profile of the counterparty, must be completed within a reasonable timeframe after acquisition of the counterparty by T&S, as agreed with the Chief Compliance Officer.

11. NON-FACE TO FACE COUNTERPARTIES

There may be occasions where a representative of a T&S Business Line meets a counterparty face-to-face during the onboarding process. Where this occurs, this would be considered face-to-face onboarding. During the face-to-face contact, the T&S representative is able to view and take copies of original counterparty or related party documents as well as discuss and ask for KYC information and questions directly from the counterparty.

Non face-to-face counterparty relationships are where no representatives of the counterparty have been met in person e.g. where a relationship is over an exchange or via an intermediary. This type of onboarding channel is not considered to materially change the Financial Crime risk as compared to face to face onboarding. However, there is an increased risk of impersonation fraud and as a result, Business Lines are required to apply and document additional non-face to face measures to address this risk, which may include, for example:

- contacting the representative of the counterparty by telephone or post using a phone number or address that can be independently verified e.g. to a public register or other T&S approved source or using certified/registered mail;

- ensuring that payment and contractual controls are in place to only accept instructions from verified Authorised Representatives; or

- requiring document copies used for KYC to be certified by an approved certifier who has met the counterparty face to face as set out in section 15.4.

12. ONGOING DUE DILIGENCE ("ODD")

12.1. Overview

To effectively monitor and manage the Financial Crime risks associated with counterparty relationships, T&S must ensure that ODD is conducted as part of the KYC measures applied to a counterparty relationship. ODD must be a continuous process, which will allow T&S to review the counterparties' activities throughout the course of the business relationship and keep the KYC information up to date.

Having up to date information about the counterparties and their expected trading or business activity is key to identifying and reporting potentially suspicious transactions. T&S must therefore ensure it:

- holds updated information on counterparties and their associated risk profile;
- identifies and verifies, as required, any new material/relevant information identified on a counterparty; and
- continues to know and understand its counterparties.

12.2. Timing of ODD

ODD must be undertaken either:

- based on the periodic cycle determined by the counterparty's risk rating as set out in section 12.3 below; or
- when a trigger event materialises as set out in section 12.4 below.

12.3. Timing of periodic reviews

The counterparty's risk rating will drive the frequency of the periodic review cycle as shown in the table below:

CRS risk rating	Frequency of ODD review
High, including High Risk PEPs	Annual refresh
Medium	3 years
Low – CDD or SDD	5 years

CRS risk rating	Frequency of ODD review
Low – BDD	N/A – ongoing screening for sanctions only and annual reconfirmation by the Business Line of eligibility

Periodic reviews must consist of, but are not limited to, the following steps:

- Business Lines to review existing counterparty information to check whether the information is still valid and up to date;
- Business Lines to review and document a summary of all trading or transactional activity since the last review of the counterparty to ensure it aligns with the expected nature and purpose of business relationship;
- FC Team review of the counterparty risk rating to ensure this remains unchanged considering any additional information;
- where the risk rating has increased to high, the FC Team will instruct the Business Line to perform additional due diligence measures be in line with the EDD requirements set out in section 5.6.1;
- FC Team to re-perform screening checks in accordance with the risk profile of the counterparty; and
- FC Team to screen any new UBOs and related parties or instances of change of names.

Note, in addition to the formal ODD process, all counterparty and related party names must be screened on an overnight basis for sanctions risk at a minimum.

Where a counterparty was previously onboarded under a former version of the KYC Standards, the ODD review will be used to uplift the counterparty file to any new requirements in the current version of the Standards.

12.4. Trigger events

There are several trigger events that would prompt an ODD review outside of the ODD periodic review cycle. The trigger events could include, but are not limited to the following:

- any change in the purpose or nature of the business relationship e.g. where a counterparty seeks to trade in a new product or service that was not previously captured;
- change of ownership or UBO of entity;

- change in Ultimate Controllers or previously identified directors;
- identifying a PEP, or an increase in the risk rating of an existing PEP;
- identifying a sanctioned connection for a counterparty which did not previously exist;
- identifying relevant Financial Crime adverse media or news reports in relation to the counterparty, a UBO or a related party;
- becoming aware of an increased risk of the counterparty being involved in money laundering, terrorist financing or other Financial Crime through monitoring and surveillance of the counterparty's activity;
- becoming aware of information that suggests the counterparty may be doing business in a jurisdiction or with an individual/entity that is restricted by the T&S Sanctions Compliance Policy;
- one or more SARs or Suspicious Transactions and Order Reports ("STOR") submitted on the same counterparty, unless otherwise advised by the MLRO or Head of Financial Crime;
- change in eligibility for either BDD or SDD e.g. loss of approved regulator/exchange status or change in business relationship; and
- information that gives cause to doubt the information or legitimacy of the documents, data or other information previously obtained in relation to the counterparty.

Note, where a change in address occurs, but the jurisdiction risk remains the same, no formal review is required.

12.5. Refresh of existing KYC documentation

Business Lines are not required to re-verify the existence of a counterparty or any of the counterparty's related parties where there has been no change to the counterparty's underlying KYC information, including but not limited to name, country of operation, address and legal form etc.

However, where a counterparty has changed its country of incorporation and/or registration then, in all cases, it must be subjected to full re-review and the applicable level of due diligence must be applied. Business Lines may rely on existing KYC information and documentations where this has not changed and remains accurate such as ownership information.

12.6. Expiration of KYC documentation

Where documentation held on file was valid and in date at the time of the counterparty onboarding, there is no requirement to obtain new valid documentation except where there are specific legal or regulatory requirements to do so or if the risk profile of the associated counterparty has changed. For example:

- Where official entity or related party verification documentation (such as a passport or constitutional documents) was valid and in date at the time of the counterparty onboarding or previous ODD review, there is no requirement to obtain new documentation, except where there have been changes to underlying KYC information, such as a change in name or legal form, or there are specific legal or regulatory requirements to do so.

- Other documentation which is more than 12 months old e.g. ownership or control information, must be refreshed and where not able to be verified as current using approved public sources, new documentation should be obtained.

- Where a deviation has been previously documented and approved in line with these standards there is no requirement to refresh that deviation during ODD, unless there has been a material change to the circumstances detailed in the deviation (such changes to the individuals or entities that the deviation applied to).

12.7. Application of Ongoing Enhanced Due Diligence ("OEDD")

OEDD is applied to High Risk counterparties due to the increased Financial Crime risk associated with these counterparties. Specific measures applied will vary by counterparty but include the following:

- increasing the frequency of OEDD Reviews for High Risk counterparties (i.e. annual reviews);

- where applicable, applying stricter thresholds and parameters when monitoring the counterparty's trading or transactional activities; and

- where applicable i.e. as advised by HRCC, undertaking enhanced monitoring of the counterparty for Financial Crime adverse media.

As part of OEDD, there is no need for the HRCC to review a High Risk counterparty that the committee previously approved unless a new red flag is identified, which would require the counterparty to return to the HRCC. Instead, the HRCC will be provided with regular MI on the status of the OEDD reviews performed to enable the HRCC to monitor adherence with OEDD measures.

13. COUNTERPARTY APPROVAL

13.1. Risk rating and rationale

The FC Team must provide a recommendation to either accept or reject the counterparty relationship, based on the KYC information gathered and Financial Crime risk review and analysis or, in the case of an existing counterparty, a recommendation whether to continue the relationship.

A Financial Crime risk review must be undertaken and documented on the KYC file and must include a summary of the KYC information obtained and any Financial Crime red flags identified. The risk review and analysis must record the rationale for accepting or declining the Financial Crime risk.

Where Financial Crime red flags are identified, and the FC Team or Business Line recommends approval or continuation of the counterparty relationship, any red flags related to the counterparty must be clearly documented along with mitigating actions to support the approval, for example, undertaking enhanced monitoring of the counterparty where there is emerging Financial Crime adverse media identified.

13.2. Approval of a counterparty

The minimal approval level for a counterparty within the FC Team depends on both the risk level of the counterparty and the level of due diligence applied:

	BDD	SDD	CDD	EDD	EDD (HRCC)
Business Line in line with the approved MoA (note, must be independent of sales originator)	✓				
FC Team in line with the approved MoA		✓	✓		
MLRO, Deputy MLRO ("DMLRO") or appointed delegate				✓	
HRCC					✓

	Low Risk PEPs	High Risk PEPs
MLRO, DMLRO (or delegate in line with the approved Financial Crime MoA)	✓	
HRCC		✓

14. COUNTERPARTY EXIT

There may be circumstances when counterparties are required to be rejected, exited or suspended due to Financial Crime risk concerns or other reasons (referred to hereafter as a "Restricted Counterparty"), such as where a Business Line no longer wishes to do business with a counterparty for Financial Crime reasons or where the relationship is inactive[47].

Set out below is guidance on how to treat Restricted Counterparties.

14.1. New counterparties – rejection

At any point during the completion of KYC measures, when a new counterparty or business activity falls outside of the T&S Financial Crime risk appetite, T&S can decide to reject or decline a relationship with a counterparty.

In all cases, the name of the rejected counterparty must be added to the DNDB list maintained by the FC Team within the counterparty KYC Tool, GoldTier. Monthly MI will be produced by the Business Lines to the FC Team to confirm that no entity listed on the DNDB list has been traded with and breaches will be reported to the MLRO and EVP T&S.

14.2. Existing counterparties – suspensions

There may be occasions where T&S determines that a relationship with an existing counterparty is to be temporarily or permanently restricted or suspended, for example where the counterparty is subject to an internal investigation or where KYC information is identified as missing during the ODD process.

In all such cases, the relevant Business Line or function must suspend the counterparty within the applicable T&S trading system, which means that T&S is not allowed to trade or engage in new deals or business with that counterparty whilst the relevant investigation or information gathering is concluded. Existing business may continue with suspended counterparties, unless advised by the FC Team. The Business Lines must have systems and controls in place to ensure new business is not conducted with restricted or suspended counterparties.

14.3. Existing relationships – exit

T&S will exit any existing counterparty relationships where there has been no trading activity or transactions for 24 months or when an existing counterparty or business activity falls outside of the T&S Financial Crime risk appetite. This includes deactivating the counterparty accounts in all trading systems and GoldTier and ceasing all business activities and transactions. Exit will be undertaken in the following circumstances:

[47] Inactive is defined as a counterparty that has had no active trades within the prior 24 month period.

- where T&S has determined that the counterparty may have used T&S to facilitate, or that the counterparty has been involved in Financial Crime; or

- where T&S determines that a counterparty relationship is outside of the Financial Crime risk T&S appetite.

Potential red flags are set out on the T&S Financial Crime Sharepoint site. Most red flags for existing counterparties would have been identified at onboarding, therefore, where a new red flag is identified in relation to an existing counterparty this must be sent to the FC Team for further review. The FC Team will:

- assess the impact of the red flag on the counterparty risk rating, and, where relevant, determine appropriate action required to mitigate the risk;

- determine whether exiting the counterparty relationship is necessary and if so, the proposed exit strategy;

- escalate any proposed exits that are of a sensitive nature or which may bring about additional reputational risk, to the HRCC; and

- determine if there are any regulatory reporting requirements e.g. a SAR is required.

In all cases where the counterparty relationship is exited for Financial Crime, including sanctions risk reasons, the name of the counterparty must be added to the DNDB list maintained by the FC Team.

The HRCC are responsible for advising on the extent to which existing business may be settled or whether transactions may still be undertaken, prior to any
exit.

In all cases where a Business Line is unsure of the status of a suspended or deactivated counterparty, the FC Team must be consulted. Further guidance on suspended counterparties can be found on the Compliance SharePoint site.

14.4. Guidance on continuation of business with suspended or exited counterparties

Where a Restricted Counterparty has been suspended or exited for Financial Crime risk appetite reasons, Business Lines must not undertake new direct business activities with a Restricted Counterparty unless expressly approved by the HRCC.

Due to the complexities of the T&S business, there will be occasions where a Restricted Counterparty is indirectly involved in T&S business activities (with or without the knowledge of T&S), for example, when dealing with aggregated or blended commodities or as a result of complex buying/selling chains where the Restricted Counterparty is potentially present in the chain. Whilst indirect business activities are not prohibited, Business Lines must ensure that trading activity is not deliberately structured to circumvent the requirements in respect of Restricted Counterparties. Business Lines should consult with the FC Team where it is unclear whether business activities may be undertaken.

Where a counterparty is subject to sanctions restrictions, the TC Team must be consulted in all circumstances.

15. DOCUMENTATION STANDARDS

This section sets out the requirements on the quality of documentation received for KYC purposes.

15.1. Documentation copies

T&S will accept documentation submitted in both softcopy (e.g. PDF format) or hardcopy. T&S will also accept electronically generated documentation such as digital bank statements, provided they are contained within the Approved Sources List set out in Appendix 6 and there are no concerns regarding the veracity of the document.

Copies of all counterparty documents obtained as part of the KYC measures must be retained and recorded on the counterparty KYC file. These copies must be legible, accurate and retrievable when required to enable T&S to demonstrate that it has undertaken the required KYC measures.

To ensure that all copies of documents provided by the counterparty for KYC purposes are true and accurate, the requirements on certification must be followed, where relevant, as set out in section 15.4.3 of these Standards.

Copies of documentation must only be held in accordance with the T&S record keeping requirements as set out in the Financial Crime Policy.

Business Lines must be vigilant for counterfeit documents, which can be challenging when documents are provided electronically. Guidance must be in place to enable those processing KYC information provided by counterparties to assist them in identifying counterfeit/false documents.

Where there are doubts as to the veracity of information or documents provided, Business Lines should consult with the FC Team for guidance.

15.2. Approved sources

T&S has created a list of approved documentation sources, databases or other electronic sources permitted to be used for identification or verification of KYC information ("Approved Sources List" – Appendix 6). These sources are approved by the Head of Financial Crime, in consultation with the MLRO, who will consider the quality, reliability and independence of sources.

Only approved sources may be used for the purposes of identification and verification. Where an approved source is not available, or an alternative source is proposed by a Business Line, a deviation request must be submitted in line with section 18.2 of these Standards. An alternative

source must not be used until a deviation is approved or the source is added to the Approved Sources List is approved by the Head of Financial Crime.

Documentation providing evidence of identity may emanate from several sources and these documents differ in their integrity, reliability and independence. There is a broad hierarchy of documents, which the Business Lines must consider when obtaining documentation or when requesting an alternative source to be added to the Approved Sources List. The hierarchy is set out below:

- certain documents issued by government departments and agencies, or by a court;
- certain documents issued by other public sector bodies or local authorities;
- certain documents issued by regulated firms in the financial services sector;
- documents issued by other firms subject to equivalent AML/CTF regulations or legislation; and
- documents issued by other independent organisations.

Note, whilst the approved sources will typically be sufficient to satisfy the KYC requirements in these Standards, there may be occasions when additional documentation may be required to discount or confirm KYC information. This will be advised by the FC Team on a case by case basis.

Where the business lines wish to add a new source to the Approved Sources List, for ongoing use, they must submit their request to the FC Team. The request must include an assessment of the reliability and independence of the data source and the specific KYC information that the source is proposed to be used to identify and verify.

Occasional or one-off use of non-approved sources for specific counterparties should be dealt with using the deviations process set out in section 18.2.

15.3. Translation of documents

All counterparty KYC information must be entered into T&S systems (including GoldTier) in English. The translation requirements to be applied are set out in Appendix 5.

Where non-English documentation is received, the relevant Business Line must obtain a translation. The relevant Business Line must also obtain a written attestation from the translator confirming that the translation is a true, accurate and complete translation of the text of the original document.

Translation of documents is acceptable from either:

- a professional translation firm;
- a T&S staff member who is not only fluent in the relevant language but understands the relevant language in its written form; or
- "Shell Translate" translation tool

Online translation tools e.g. Google must not be used to translate counterparty information due to data privacy. However, they may be used to translate extracts of publicly available KYC information e.g. extracts from publicly available annual reports or counterparty websites in foreign languages.

All translations must be of original documents, or copies of the original documents which have been certified in line with the certification requirements set out in section 15.4. below.

15.4. Certification

15.4.1. Overview

Certification is the confirmation by an independent party that a copy of an official document is a true and proper copy of the original, meaning that it accurately reflects the content of the original document, including the likeness of any photograph to the person presenting the document.

Certification must not be confused with "attestation". Attestation refers to confirmation in writing by a party, of the completeness and accuracy of certain information e.g. the ownership of an entity. Attestations from a counterparty or approved third party are an acceptable source of evidence for the verification of certain KYC information, where specified in the Approved Sources List at Appendix 6.

Where copies of original documents are used for identification or verification purposes, T&S must ensure that the documents are appropriately certified before being considered acceptable for the ID&V purposes.

15.4.2. Eligibility

Certification is only required for official documents that are not viewed directly by T&S in their original form, or where evidence cannot be directly sourced from approved public sources. Certification is only required for documents used for verification. It is not required for KYC documentation used for identification only or obtained as part of the BDD or SDD process.

The Business Lines are accountable for ensuring that documents have been correctly certified. Where documents are not certified by an appropriate person, these documents must not be accepted, unless a deviation has been approved.

For a certified document to be accepted, the following criteria must be met:

- documents are only accepted where certified by an appropriate individual, whose professional body membership credentials or professional status can be appropriately verified;

- certification of a copy document must be made with reference to sight of the original document. Certification of a copy document must not be accepted;

- where there is more than one copy document being used, each individual document is required to be certified individually; or

- for documents with more than one page, in addition to the certification requirements on the first page, the certifier must also, initial and date each individual page.

15.4.3. Certification Requirements

To fulfil certification requirements, the following must be recorded on each document by the certifier:

- name of the certifier;
- signature of the certifier;
- date of certification – this must be within three months of the receipt of the document by T&S; and
- position held by the certifier, and where applicable the name and membership reference of their relevant professional organisation.

For instances where photographic documentation is being certified, the photo and document must be legible, and it will be necessary for the Business Lines to ask the certifier to confirm that the photo in the document is a true likeness of the individual presenting it. The following wording, or equivalent, is required:

"I confirm that this is a true copy of the original document and, (where applicable), is a true likeness of the person presenting the document".

15.4.4. Appropriate certifier

To guard against the risk that the documentation is fraudulent or does not correspond to the individual whose identity is being verified, T&S must ensure that only an appropriately professional, independent certifier is used. This will be effective only if the certifier has seen the original documentation and where applicable, has met the individual face to face.

The following are approved certifiers:

- qualified lawyer or attorney registered with the relevant national professional body;
- qualified accountant registered with the relevant national professional body;
- notary public;
- member of the judiciary, a senior civil servant or a serving police or customs officer in a Low ABC risk country as per the RDS Ethics and Compliance Manual;
- embassy, consulate or high commission officer of a Low ABC risk country as per the Ethics and Compliance Manual.
- T&S employee, on a face to face basis;
- An individual who is of equivalent status or authority to those listed above;
- For CDD only, members of the counterparty's board of directors; or
- For CDD only, members of the parent (either immediate or ultimate) company's board of directors. [48]

Certification by individuals who are employed by the counterparty or a beneficial owner i.e. parent company of the counterparty from the above list of approved certifiers are acceptable provided the Business Line can verify and evidence their professional body membership or status in line with independent certifiers, and as long as there are no concerns or red flags regarding the veracity of documentation provided.

Where concerns are identified e.g. where information found in internally certified documents is inconsistent with other KYC information provided or obtained from public sources, the FC Team may request that the counterparty provides additional corroborating documentation or independently-certified documentation to explain or mitigate the issues.

[48] NB. Members of the counterparty and parent company's board of directors cannot certify their own identification documents e.g. passport copies.

16. SOURCE OF WEALTH ("SOW") AND SOURCE OF FUNDS ("SOF")

16.1. SoW definition

SoW refers to the origin of the wealth of an entity or individual as well as how this wealth has been generated and maintained throughout the years. This is distinct from identifying the source of the specific funds used by an entity or individual for the transaction or specific business relationship.

The purpose of identifying the SoW is to understand an entity or individual's financial background and to assess whether their wealth has accumulated from a legitimate source.

16.2. SoW requirements

The requirements to identify and verify SoW are based on the due diligence level applied to the counterparty as follows:

- SDD: SoW does not need to be identified or verified;
- CDD: The Business Line must identify the SoW of any counterparty who is a natural person, or individual UBO owning or controlling 75% or more of the counterparty, using the Approved Sources List set out in Appendix 6; and
- EDD: The Business Line must identify and verify the SoW of all counterparties who are natural persons, and High Risk PEPs who are UBOs, as well as all other individual UBOs owning more than 25% of the counterparty, using the Approved Sources List set out in Appendix 6.

16.3. SoF definition

SoF refers to the origin of the funds involved in the business relationship with T&S. It refers to the activity that generated the funds. Funds are a subset of wealth. Funds must only be transferred and received via electronic means. Cash payments are prohibited by T&S and are not to be accepted.

The purpose of identifying the SoF is to better understand the counterparty's financial profile and to assess whether the funds used for the business relationship originated from a legitimate source.

The SoF of the business relationship will help identify the origins of the funds which will be used by the counterparty to finance its expected relationship with T&S.

16.4. SoF requirements

The requirements to identify and verify SoF are based on the due diligence level applied to the counterparty as follows:

- SDD: SoF does not need to be identified or verified;

- CDD: SoF must be identified and verified for counterparties who are natural persons and where T&S receives funds from the counterparty. SoF does not need to be identified or verified for counterparties who are legal entities. However, Business Lines must obtain latest financial information as part of understanding the nature of the counterparty's business, in line with the guidance below.

- EDD: SoF must be identified and verified for counterparties who are natural persons and where T&S receives funds from the counterparty. The Business Line must also identify the SoF for counterparties who are legal entities and must obtain latest financial information as part of understanding the nature of the counterparty's business, in line with the guidance below.

For all counterparties who are entities and subject to CDD or EDD, every effort should be made to obtain the latest financial statements (audited or unaudited) as part of understanding the nature of the counterparty's business. If financial statements are unavailable, a third party aggregator tool (e.g. Dun & Bradstreet, Orbis) may be used as an alternative to obtain basic financial information.

For smaller companies where financial statements are not prepared, a note should be added to the file to confirm that financial statements are not available, and where alternative information is available, this must be noted on the KYC file.

Business Lines must notify the FC Team of any concerns or red flags, including those raised by the relevant credit team, in respect of the counterparty's SoF.

Red flags may include but are not limited to:

- A negative working capital value. Where this occurs, the Business Line should identify if the expected business is to purchase or sell products to the counterparty and highlight any concerns to the credit team.

- A large positive working capital for a relatively new company. In this scenario, the Business Line should investigate and document where the assets of the counterparty originate from.

- Where the size of the counterparties' working capital does not align with the expected business relationship e.g. where the value of the expected relationship is a similar size or greater than the working capital.

- Where the most recent annual turnover figure is not proportionate with the size of the expected business relationship e.g. where value of the expected relationship is a similar size or greater than last year's turnover.

Where financial statements are not prepared or are not provided by the counterparty, this should be noted in the counterparty KYC file.

SoF is not required to be identified for UBOs. The exception to this is where there is evidence to suggest that SoF for a business activity or transaction with T&S is obtained directly from a UBO, for example, where a counterparty is newly incorporated and has not yet generated any business profits and has been established with start-up capital provided by a single UBO. In this instance, the SoF must be identified.

17. IDENTIFICATION AND VERIFICATION GUIDANCE

The following concepts are important to understand when conducting KYC and gathering counterparty documentation.

17.1. Identification

Identification is the process undertaken to obtain and record minimum information in relation to counterparties, and their related parties. This information is used by T&S to understand the identity and existence of its counterparties.

Identification of the required KYC information may be via publicly available sources such as the counterparty's website, company registries or obtained directly from the counterparty itself.

17.2. Verification

Verification is the process undertaken by T&S to evidence the information identified in relation to counterparties, and their related parties, to confirm that the information obtained is complete and accurate.

Verification must be based on reliable and independent sources. Where documents are provided directly by a counterparty these may be regarded as being independent where the documents were issued by or filed with an official authority e.g. passports, constitutional documents, extracts from trade registers. Certification of such documents is, however, still required, where copies of official documents are received, in line with section 15.4 of these Standards.

Approved sources that may be used for identification and verification of KYC information are set out in Appendix 6. The minimum information requirements and definitions to be applied to all counterparties are as follows:

17.3. Legal and trading name

The legal name of a counterparty may be either:

- its registered name where the counterparty is an incorporated entity. This name must be set out on the counterparty's incorporation document or subsequent official name change records filed with an official authority;

- legal name in the case of a counterparty formed under a legal agreement. The name must be contained in the legal agreement such as a partnership agreement or trust deed; or

- the trading name in the case of an unincorporated body.

A counterparty may use a name, other than its legal name, under which it operates or trades to the public. This is referred to as its trading name. Business Lines are required to identify all current trading names used by a counterparty. All current legal names must be screened as per the guidance set out in section 8 above. In addition, for counterparties subject to EDD measures, all trading names used by a counterparty must also be screened.

A counterparty's legal name must be verified for all counterparty types. Where a counterparty's legal name has been amended since its formation, additional evidence must be obtained to support the amended name. The Business Lines should ensure any evidence collected is sufficient to link the previous name to the counterparty's new name, ensuring they are still dealing with the same counterparty. For CDD and EDD, where a counterparty's legal name has changed within the past 12 months, the former name should be screened for PEPs, sanctions and adverse media, as set out in section 8.

There is no requirement during ODD to re-verify a counterparty's legal name where there is no change to this information. Where a counterparty's name has changed this must be verified.

17.4. Known aliases

An "alias" is an alternative name that is used by an individual. The individual might be known informally by this alias on a day to day basis. Known aliases must be documented if identified during the KYC process[49]. However, it is not necessary to record shortened versions of names on the counterparty KYC file e.g. Rob instead of Robert.

17.5. Government issued ID number or equivalent

Government issued ID numbers refer to any official, government issued unique number given to identify a counterparty. This may include, but is not limited to, a company registration number, tax identification number or number issued by a regulator or exchange. The ID source used, ID number and the jurisdiction which issued the identification number must be recorded.

There is no requirement to confirm or re-verify Government Issued ID numbers for the purposes of ODD.

17.6. Registered address

The registered address is the official address at which a counterparty is registered. This address is typically used to receive official correspondence and formal notices and is typically recorded in a counterparty's incorporation or legal formation documentation. T&S require that the

[49] There is no requirement to perform screening on any known aliases, unless advised otherwise by the FC Team or HRCC.

verification document obtained identifies the address as "registered address", "registered office" or equivalent.

If a physical registered address is unavailable to satisfy the registered address requirement, a Post Office ("PO") Box is acceptable to use in Low and Medium FC risk countries as long as the trading address is a verified physical address. For High FC risk countries, if only a PO Box is available, Business Lines must consult with the FC Team for guidance.

Where a counterparty has no registered address but uses the services of an agent or similar (e.g. corporate service provider), the address of the agent must be recorded as the registered address.

Where a counterparty's registered address changes, this must be verified.

17.7. Trading address

A trading address is a counterparty's principal place of business or main location from which it operates. For some counterparties, the trading address may be the same as the registered address. For larger entities it is common for a counterparty to have multiple trading addresses due to the scale of its operation, particularly where they operate across several jurisdictions (see section 17.10 below). For the purposes of these Standards, T&S considers that the counterparty's main place of business (or "headquarters" or "head office") is its trading address.

Where a counterparty's trading address changes, this must be verified.

17.8. Alternative to registered or trading address

In exceptional circumstances, a counterparty may not be able to provide a registered or trading address by virtue of their legal form. For example, trusts do not typically have business activities or physical operations so may not have a business address as a result.

In these instances, T&S must record the address associated with the entity's Ultimate Controller as the counterparty address.

17.9. Country of incorporation

The country of incorporation is the jurisdiction in which the entity is legally incorporated or formed. In the case of unincorporated entities formed by the execution of a legal agreement, the country of incorporation will be the jurisdiction under which the agreement is governed.

When determining the country of incorporation, this will typically also identify the law to which the entity is subject to and its constitution. This information must also be recorded on the counterparty file.

Where a counterparty changes its country of incorporation and/or registration an ODD review should be triggered to ensure the correct level of due diligence has been applied.

17.10. Operating regions

The operating regions are where the counterparty conducts its main business activities, has its offices or from where it generates more than 20% of its annual revenues or turnover. Where a counterparty has a global or a regional reach, i.e. a multinational operating in many jurisdictions across the world, this should be stated.

However, Business Lines must try to be as specific as possible to ensure that higher risk jurisdictions that may impact the counterparty Financial Crime risk score, are not captured inadvertently.

Connections to EDD countries, including GECs and HRCs must be highlighted as part of the KYC process, where identified.

17.11. Legal entity type and active status

The legal entity type and active status of a counterparty refers to the legal entity type of the counterparty and the status of its legal registration or establishment e.g. a private company limited by shares or a limited partnership. In addition, Business Lines must determine that a counterparty has an active status and is not bankrupt or dissolved. Section 10 sets out additional guidance on specific entity types. It is important that the Business Lines correctly identify the counterparty's legal entity type to ensure the correct related parties are identified and where required by these Standards, verified

It may be difficult to determine a counterparty's legal entity type in some scenarios, for example where a counterparty may have been established under an informal arrangement such as an informal partnership. Guidance must be sought from the FC Team on the due diligence requirements to be applied.

Where a counterparty's legal entity type has changed, it must be treated as a new counterparty and the applicable level of due diligence must be applied.

17.12. Purpose and nature of intended business relationship

Recording information on the intended purpose of relationship enables T&S to assess whether the intended business relationship is in line with the firm's risk appetite and the counterparty's business profile and provides meaningful basis for ongoing monitoring. It is important to analyse whether the intended business relationship is consistent with the counterparty's nature of business.

Business Lines must record a succinct summary of the proposed commercial activities that the specific counterparty will be undertaking, including the nature, values, volumes and frequency of transactions where known, e.g. trading of a particular commodity on a spot or term basis, structured finance or setting up of a joint venture.

The nature of the relationship across all T&S Business Lines must be updated and reviewed during the ODD process to ensure this remains consistent with the recent trading and/or activity undertaken with the counterparty and the other information recorded on the counterparty file. The analysis should consider the last 24 months of activity, or activity since the last review (whichever is shorter) and should also include expected future activity for the next 12 months.

17.13. Nature of counterparty's business

The nature of business of a counterparty refers to the industry sector and nature of the commercial or business activities that the counterparty undertakes, as well as the locations from which it undertakes those activities. T&S must identify and understand the nature of business of a counterparty to ensure it is consistent with the intended business relationship with T&S and to support the onboarding decision reached. Understanding the role of a prospective counterparty in the market, and the counterparty's reasons for trading, will help inform decisions on the risk profile the counterparty presents.

Business Lines must identify and record as part of IDD, the following, where relevant:

- country(ies) of operation, including any links to sanctioned countries (GECs and HRCs);
- age of counterparty e.g. when established;
- main business activities/industry sector of the counterparty; and
- size and scale of the company's business i.e. annual turnover and main sources of income (e.g. trading activities, holding company, investments), number of offices, number of employees, where known.

For each counterparty, the recorded nature of business must be meaningful and descriptive to provide insight on the counterparty's nature of business as opposed to the intended relationship with T&S.

Where a Sanctions or Indirect Sanctions Nexus is identified as set out in section 8.3.1, i.e. a link to a GEC HRC, the FC Team or Business Line must consult with the TC Team as appropriate, for further advice.

The nature of business must be reviewed and updated during the ODD process, where required.

17.14. Ownership structure

The ownership structure of an entity refers to the different levels of ownership or intermediate layers between the counterparty and the UBO(s).

It is necessary to understand and document the intermediate layers of beneficial ownership until one of the following is reached:

- an individual/a natural person;
- a publicly listed entity on an approved exchange;
- government body; or
- until the percentage ownership/control is diluted below an effective 25% (more than 10% for EDD) of the shares, capital, profits or voting rights of the counterparty.

Total ownership in the structure must always add up to 100% (considering dilutions through the various layers and branches) and the percentage shareholding at each layer/branch must be identified.

18. DEVIATIONS, EXCEPTIONS AND BREACHES

As set out in section 1, compliance with the requirements of these Standards is mandatory. However, there may be exceptional circumstances where a requirement cannot be met, for example where local laws or regulations conflict with these Standards, or where a counterparty cannot comply with a specific requirement for a legitimate reason. In these circumstances, an exception or deviation may be requested as outlined below.

18.1. Exceptions

Where circumstances prevent a Shell T&S legal entity or Business Line from complying with requirement(s) within these Standards, the impacted T&S entity must request an exception via the Shell T&S Compliance Team in line with the Compliance Policy Exceptions Process.

18.2. Deviations

Deviations are different to exceptions as these relate to either a counterparty or group of counterparties, who cannot comply with a specific requirement or set of requirements set out in these Standards, for example where a newly formed counterparty does not have the standard identification and verification documentation required. In these scenarios, the applicable Business Line must request a deviation from the FC Team, providing the following information at a minimum:

- Name of requestor;
- Business Line and area;
- Summary of request;
- Rationale for the deviation with supporting evidence;
- Any identified mitigating action or alternative proposed;
- Relevant information on the counterparty(ies) including:
  - risk rating of the counterparty;
  - country of incorporation;
  - summary of the counterparty's business and risk profile; and
  - results of any screening performed on the counterparty and its related parties.
- Where applicable, proposed timeframe for the deviation and for completion of any outstanding actions, unless a permanent deviation is required.

All requests for deviations from the Business must be approved by either a relevant Business Line General Manager ("GM") or appointed delegate prior to submission to the FC Team. The FC Team is authorised to propose and approve deviations directly, in line with the documented MoA.

All deviation requests must be documented within the GoldTier file as part of the risk review and must contain sufficient information (including the above data points) to enable an understanding of the requested deviation and the mitigating factors.

The FC Team is responsible for the review and approval decision for all deviation requests and approvals may be subject to relevant conditions or may require additional mitigating actions. The applicable Business Line is accountable for ensuring that any conditions or actions required are tracked and completed.

18.3. Breaches

All non-compliance with any requirement in these Standards which has not been approved as a deviation or exception must be reported to both the Head of Financial Crime and the T&S Compliance Policy Team without delay and will be treated as a breach of these KYC Standards.

All identified breaches will be reviewed and investigated. The associated Business Line and Head of Business is responsible for the completion of any required mitigation plan which must be approved by the Head of Financial Crime with oversight from the MLRO.

As set out in the Financial Crime Policy, a breach of these KYC Standards may lead to disciplinary action. Where non-compliance is also a potential breach of any Financial Crime laws or regulations, this will also be escalated to the T&S MLRO who is responsible for the reporting of such matters to competent authorities, where required.

18.4. Exceptions, deviations and breach recording.

The Compliance Team is responsible for logging all exceptions and breaches (confirmed and suspected) within a central register. Breaches of Compliance policies, including the KYC Standards will be subject to the Compliance Incident Management Process as set out in the Compliance Manual.

For all KYC deviation requests specific to individual counterparties, these will be recorded as part of the relevant counterparty KYC file in GoldTier.

19. THIRD PARTY PAYMENTS

During the course of normal T&S business activities, T&S must only send or receive payments to/from entities with whom it has a contractual relationship and on whom KYC has been undertaken. Where payment transactions are undertaken with third parties who are not part of the contractual relationship, and who have not been subject to KYC measures in line with these Standards, it is the responsibility of the Business Line to ensure it knows the origin or destination of the payments. Where known at the time of onboarding, a third party payor or payee must be added as a related party to the counterparty KYC file and treated in line with the related party requirements.

There may be legitimate reasons for a counterparty to make a payment via a third party, such as following a company name change or where a parent company or affiliate responsible for group treasury or payments wishes to make a payment on behalf of a subsidiary. However, it is important that the Business Line understands and documents the nature of the relationship between the payor and the counterparty and obtains confirmation from the contractual counterparty that the payor/payee is authorised by them. Where any red flags are identified, the Business Line must consult with the FC Team who will assess the risk and screen the payor/payee name for sanctions, PEPs and Financial Crime Adverse Media.

The Business Lines must:

- ensure they understand the nature of the relationship between the payor and the counterparty;

- ensure payments are made electronically via the banking system and must not be made in cash, without approval of the MLRO or appointed delegate.

- obtain appropriate documentation to verify the relationship in line with the Third Party Payments Policy i.e. written or emailed confirmation of the relationship between the counterparty and the third party from an authorised signatory of the counterparty. The confirmation must be dated and on company letterhead/email to confirm it is from a legitimate source;

- ensure that any third party payor is added as a related party to the counterparty KYC file as soon as it is identified; and

- in conjunction with relevant functions e.g. credit, finance, have in place appropriate controls to monitor third party payments and must be vigilant for fraud, sanctions circumvention and money laundering risk e.g. unauthorised or frequent changes to bank account details, when making or accepting payments to/from third parties and must escalate any concerns to the FC Team.

Third party payments notified to the FC Team, where the Business Line is unable to provide supporting documentation, may be escalated to the EVP T&S or the MLRO as appropriate.

When a third party payment is rejected or accepted, the FC Team must communicate the decision to the relevant Business Line or function who must keep a record of the approval.

20. TRADE FINANCE

20.1. Definition

The majority of the world's trade is conducted in 'open account' whereby the goods are shipped and delivered, or services performed before payment is due. This introduces the risk to the seller of non-payment. Trade finance represents the financial instruments and products that are used by companies to facilitate trade or commerce and mitigate this risk of non-payment by the buyer, as well as non-performance by the seller. Trade finance generally involves the movement of goods and services between two points – it can therefore be domestic or international. The trade finance component may only be part of the overall financial arrangement, comprising a mix of money transmission instruments, default undertakings and provision of finance.

20.2. Overview of risk

The international trade system is subject to a wide range of risks and vulnerabilities which can be exploited by criminal organisations to disguise the proceeds of crime and transfer value in an effort to legitimise their illicit origins.

Trade based money laundering can be achieved through the misrepresentation of the price, quantity or quality of imports or exports and is frequently used in combination with other money laundering techniques to further obscure the money trail. The money laundering risk is significantly higher where the parties to an underlying commercial trade transaction collude to disguise the true nature of a transaction (for example through over and under invoicing, the presentation of false documents, spurious calls under default instruments; or, in more complex situations, through asset securitisation, trade receivables generated from fictitious parties or fabricated transactions). Given T&S's role as the buyer or seller, trade finance transactions are not considered to pose a materially increased money laundering risk as compared to open account trade transactions.

Consistent with open account physical trade, transactions that include a trade finance instrument pose a risk of facilitating trade in violation of sanctions regimes and are susceptible to bribery due to, for example:

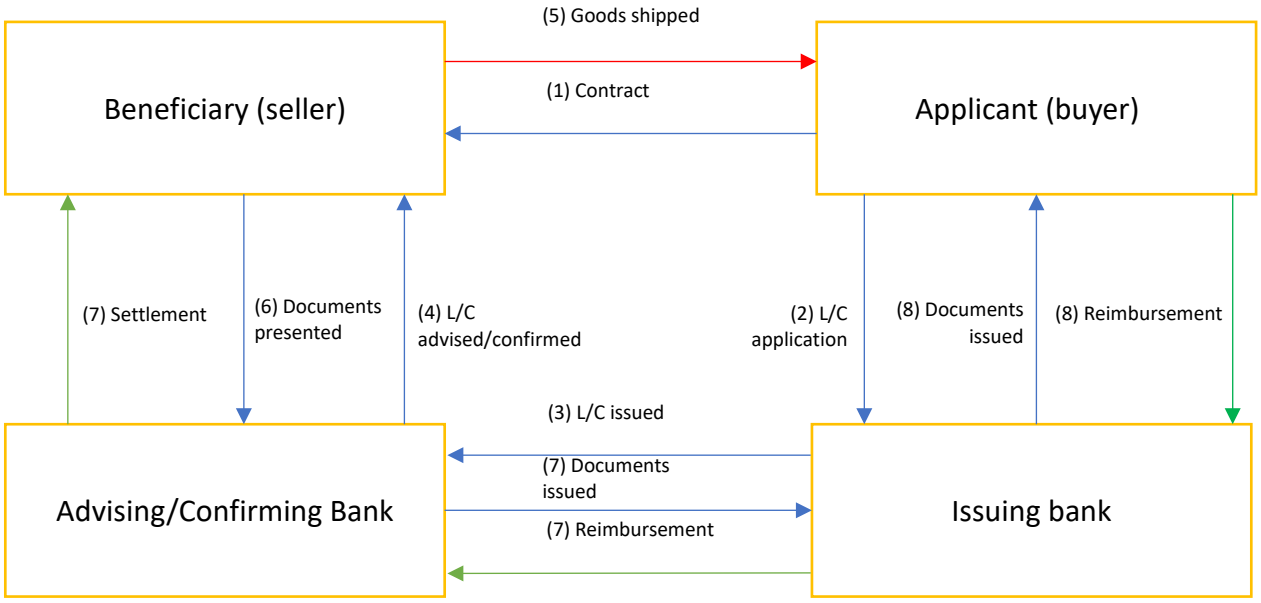
- the jurisdictions involved;
- transportation of dual-use goods;
- interaction with public officials (e.g. to obtain certificates and negotiate customers procedures); and
- reliance on local agents, often operating in jurisdictions with more corrupt environments.

In addition, the manual, often paper-based controls, can make the effective identification of a Sanctions or Indirect Sanctions Nexus even more challenging.

20.3. Application of trade finance to T&S

A typical trade finance transaction will have a beneficiary/seller and an applicant/buyer. The nature of T&S' activities means that it could be a buyer or seller depending on the transaction.

An example of a typical structure within a trade finance transaction and the documentary and payment cycle is set out in the diagram below:



The role of the issuing bank is to issue the letter of credit ("LC") to the buyer as a promise to pay the seller for the goods or services on receipt of the documents evidencing fulfilment of the terms of the LC. While the issuing bank pays the seller, the funds are the applicant's (buyer's).

The role of the advising bank is to authenticate the LC issued by the issuing bank to mitigate the risk of fraud.

In the case of a "Standby LC", the issuing bank guarantees to pay the seller, even if the buyer fails to pay. Standby LCs are treated in accordance with the requirements for guarantors and security providers as set out in section 21.

20.4. Due diligence requirements

The role that T&S plays in the trade finance transaction determines the due diligence requirements. Therefore, T&S must first identify, document and understand all of the parties to the trade finance transaction.

a) T&S is the applicant/buyer

Where T&S is acting as the applicant (i.e. the buyer), due diligence must be conducted as follows:

Scenario	Description	KYC requirement	Rationale
1	Beneficiary (seller)	SDD, CDD or EDD in line with CRS risk rating	Seller is the trading counterparty
2	Issuing bank of an LC on behalf of T&S in favour of a counterparty (approved and unapproved regulator)	BDD in line with G&A Vendor requirements	Vendor relationship. Flow of funds is from T&S to a bank; no receipt of funds

b) T&S is the beneficiary/seller

Where T&S is acting as the beneficiary (i.e. seller) in the transaction, KYC measures must be conducted as follows:

Scenario	Description	KYC requirement	Rationale
1	Applicant (buyer)	SDD, CDD or EDD in line with CRS risk rating	Applicant is the trading counterparty
2	Issuing/Confirming/Advising Bank where T&S is beneficiary (seller): where the bank is in a non-EDD country[50]	BDD. If material, unmitigated red flags found, reduced EDD to be applied in line with guidance at section 10.11	Flow of funds is between T&S and non-EDD country issuing or confirming bank
3	Issuing/Confirming/Advising Bank where T&S is beneficiary (seller): EDD country	Reduced EDD in line with CRS risk rating and guidance at section 10.11	Flow of funds is between T&S and a higher risk bank. Misuse of trade finance and LCs is a known money laundering typology.

In addition to the KYC requirements above, Business Lines must have appropriate controls in place to ensure they:

[50] Including subsidiaries or branches in EDD countries where >50% owned, controlled and consolidated by a parent company regulated by an Approved Regulator and counterparty/ parent confirms it applies parent company's ethics and compliance policies.

- identify the countries and trading routes utilised in the trade finance transaction and escalate any sanctions connections to the TC Team;

- identify the goods being traded and conduct dual-use goods screening, where relevant; and

- identify the role and location of agents and other third parties used by the applicant in relation to the transaction and escalate to the FC Team where they are deemed to represent an increased bribery and corruption risk.

One of the key risks around trade finance is that transactions and the associated documents can appear legitimate, even though they may have been created simply to justify the movement of funds between parties, or to show a paper trail for non-existent or fraudulent goods. Where T&S is the seller in a trade finance transaction, the level and type of documentation received by T&S will be principally dictated by the buyer, i.e. the counterparty.

Due to the diversity of documentation and the nuances of sanctions and other legal obligations, the Business Lines and relevant functions e.g. Credit, Finance, must ensure they have appropriate controls in place to identify any red flags in relation to the types of the documents received. Where this is the case, the Business Line must consult with the Compliance Team.

21. GUARANTORS AND SECURITY PROVIDERS

21.1. Definition

As part of a T&S agreement that requires security for credit purposes, the counterparty may be required to provide payment default undertakings or guarantees e.g. parent company or third party guarantees or standby LCs from banks (hereafter referred to as "guarantors"). Guarantors will guarantee payments to T&S should the counterparty not be able to pay.

The requirements of this section may also be applied to direct guarantors, or security trustees appointed for commodity based lending relationships, where collateral/security is placed in trust with a third party to retain and allocate to the lenders, in the event of default by the borrower/producer.

21.2. Overview of risk

Where a counterparty defaults on a payment or contract, the guarantor or security provider will be called upon to settle the liability in line with the security/guarantee arrangement. This introduces a third party payment risk which exposes T&S to increased Financial Crime risk, including money laundering and/or the circumvention of sanctions.

21.3. Timing of due diligence

Where counterparty relationships or transactions are subject to a guarantor, the guarantor or security provider is only considered to be a counterparty at the point the guarantee/security is called i.e. if the counterparty defaults on a contract or payment.

As a minimum, T&S must treat all guarantors as a related party of the counterparty at the point at which they become a guarantor and undertake sanctions screening. If the guarantee is called, T&S must treat any payment from a guarantor in line with the Third Party Payments requirements (see section 18 above) and must consult with the FC Team regarding any additional KYC measures that might be required.

21.4. Due diligence requirements

As guarantees or security may never be called and therefore T&S may never transact with the provider, the nature and extent of KYC measures depend on the type of guarantor used.

- Where a guarantee is provided by a beneficial owner of a counterparty i.e. parent company, or UBO, there is no requirement to perform separate KYC measures on the guarantor, as it will already have been covered by the KYC measures undertaken on the counterparty, including screening for sanctions.

- Where a bank or FI provides a standby LC, the bank should be added as a related party to the counterparty KYC file prior to the LC being issued and should be subject to the requirements for Trade Finance LC Issuing banks as set out in section 20.4. i.e. BDD or reduced CDD/EDD, depending on the jurisdiction of the bank.

Where any of the scenarios below apply, the guarantor must be subject to full KYC measures in line with its entity type and CRS risk rating, at the same time as the counterparty, and prior to any guarantee being accepted:

- the guarantor is a third party to the counterparty (i.e. not part of the same corporate group as the counterparty, or a bank/FI); or

- there is a reasonable likelihood that the guarantor will be called upon to fulfil their obligation or if advised by T&S Legal or Credit.

All KYC documentation obtained with regards to a guarantor must be maintained together with the KYC information of the counterparty.

22. COMMODITY BASED LENDING

22.1 Definition

This section sets out the minimum due diligence requirements to be applied for commodity based lending relationships within T&S.

Due to the complex and bespoke nature of commodity financing transactions, Business Lines must ensure that they consult with the Compliance Advisory Team or FC Team for any specific KYC requirements or Financial Crime risks that may need to be mitigated.

Commodity financing, sometimes referred to as structured commodity based lending or structured trade finance ("STF"), is a bespoke financing solution provided to facilitate the underlying sale and/or purchase of commodities. Participants in commodity financing include producers, trading houses and financial institutions. The principal types of commodity financing are:

- Pre-shipment financing;
- Pre-export financing;
- Prepayment financing;
- Warehouse and Inventory Financing;
- Repurchase (Repos);
- Borrowing Base Facilities/Reserve-Based Facilities; and
- Lease Financing.

Commodity financing solutions can be applied across part or all of the commodity trade value chain: from producer to processor/refiner to distributor, and by the physical traders who buy and deliver commodities in the international and domestic markets. Commodity financing of producers may in some cases be structured to mitigate credit and price risks to leave the performance risk and as such it is particularly well suited for companies doing business in what are considered higher risk (typically emerging) markets and sectors.

At present, the commodity financing structures most frequently utilised by T&S are pre-export financing, prepayment financing and borrowing base/reserve-based facilities.

22.2 Why undertake commodity financing?

A wide range of parties may benefit from participation in commodity financings, including:

- Producers: Financing supported by cash flows from the sale of commodities can provide producers with capital for the purchase of raw materials, acquisition of assets, funding of capital expenditure, provision of working capital, and acquisition of equipment. Local

producers in emerging markets, which may otherwise struggle to secure capital, can benefit particularly from these arrangements.

- Trading companies: The provision of commodity financing by a trader may provide a competitive advantage to differentiate the trader from the competition, helping to secure the offtake[51]. The trader may be able to provide competitive financing even to higher credit risk counterparties located in higher risk industries or countries, due to its ability to view financing risks and trading risks and returns in totality. Traders may also provide risk management solutions, such as hedging, to address some of the operational and price risks associated with the transaction.

- Financial institutions: For financial institutions, commodity financing presents an opportunity to work alongside traders to access new clients and gain exposure to markets that may not otherwise be accessible. Commodity financing transactions involving a highly credit rated offshore offtaker (such as T&S) are particularly attractive to lenders as they mitigate against payment risk. Traders may also help to provide price hedging solutions. This leaves financiers exposed to production risk, which is typically mitigated by taking security over the commodity reserves or production licence.

22.3 Risk overview

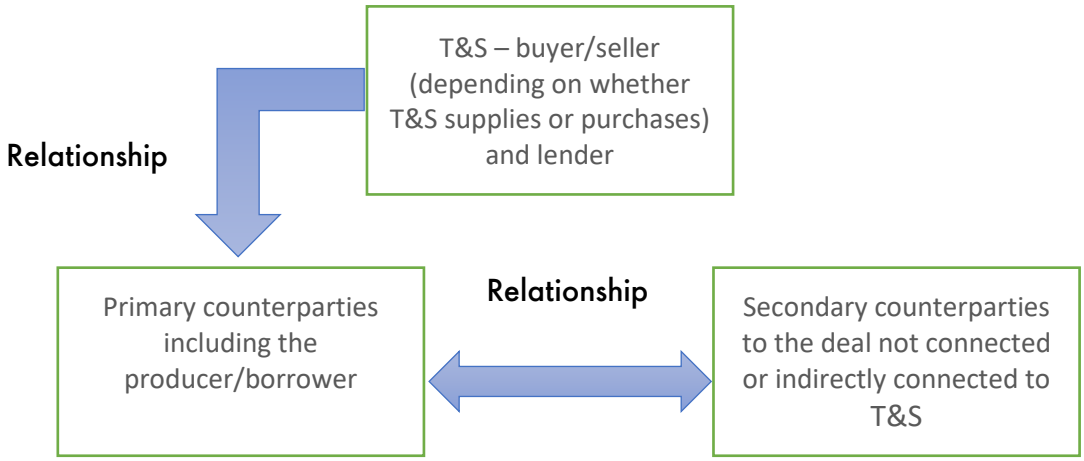
Commodity financing may result in increased Financial Crime and reputational risk to T&S. While money laundering risk exposure may be lower due to the fact that T&S will typically receive re-payment of the loan (directly or indirectly) through the crude offtake from the producing counterparty, there is typically increased bribery and corruption and sanctions risk due to factors including the large values of the underlying contracts, the countries involved, and the origin of assets used as collateral.

For each commodity based lending deal, additional due diligence measures must be undertaken by the T&S Business Line to identify, analyse, understand and document the level of Financial Crime risk associated with a commodity financing relationship. These additional measures must be applied in line with the requirements set out below.

[51] Provision of trader financing is particularly important in securing long-term crude offtakes in markets such as West Africa and South America.

22.4 Who is the counterparty?

As illustrated in the diagram below, there may be multiple parties to a commodity financing deal, including both primary and secondary counterparties.



- The following are considered primary counterparties to a commodity based lending deal subject to full KYC measures in line with these Standards:

Primary counterparty	Due diligence required
Producer/offtake counterparty[52]	Full KYC measures i.e. SDD, CDD or EDD and additional requirements set out in section 22.6
Borrower (which is typically the same entity as the producer/offtake counterparty, or an affiliate)	Full KYC measures i.e. SDD, CDD, EDD and additional requirements set out in section 22.6
Providers of credit risk insurance to T&S (deal-specific)	Full KYC measures i.e. SDD, CDD, EDD as applicable
Any joint venture partner(s) of T&S	Full KYC measures i.e. SDD, CDD or EDD as applicable
Any consultant or introducer providing advice directly to T&S on the transaction[53]	Full KYC measures i.e. SDD, CDD or EDD as applicable

[52] Depending on the whether the deal involves the purchase of commodities by T&S or supply, Shell may be either the buyer or seller under the offtake.

[53] Note, Business Lines should ensure that fees paid to brokers/consultants/intermediaries in High ABC risk countries, either directly or indirectly by T&S, are reviewed in consultation with T&S Legal or Compliance to ensure there are no Bribery and Corruption red flags.

- Secondary counterparties: other parties to a commodity financing deal, being:

Secondary counterparty	Due diligence required
Co-lenders i.e. banks/FIs and other lenders who provide finance to the counterparty under the same or connected loan facility	BDD, SDD, CDD or EDD or no KYC requirement depending on regulated status and role as per section 22.6
Facility Agent i.e. the main bank that receives and makes payments between the lenders/borrowers	BDD, CDD or EDD depending on regulated status as per section 22.6
Lead Arranger	BDD, CDD or EDD depending on regulated status as per section 22.6
Security Agent/Trustee	BDD, CDD or EDD depending on regulated status as per section 22.6
Guarantors and security providers	Treat as related parties or undertake BDD, SDD, CDD or EDD depending on jurisdiction, per section 21
Account or payment bank or other administrative parties to T&S	BDD in line with G&A Vendor requirements
Account or payment bank or other administrative parties to the borrower/other lenders	No requirement to perform KYC
Consultants, advisors and introducers for parties other than T&S[54]	No requirement to perform KYC measures
Providers of hedging to the counterparty	No requirement to perform KYC measures
Seller of an asset being acquired with the proceeds of the loan	No requirement to perform KYC measures
Any other material participants or beneficiaries to the deal e.g. a core provider of technical services to the counterparty	No requirement to perform KYC measures

22.5 Due diligence requirements

Commodity financing transactions are diverse in nature. T&S must understand and document the level of risk associated with their counterparties in a commodity financing relationship.

The due diligence requirements to be applied by the Business Line will vary depending on the role of the counterparty. The table below sets out the different due diligence requirements for primary counterparties that are the producers/borrowers, other primary counterparties and secondary counterparties other than banks.

[54] Including third party providers of due diligence reports where T&S places reliance on the report.

The due diligence measures set out in the table below are in addition to the related party and screening requirements set out in sections 6 and 8 of these Standards.

	Counterparty type		
Requirement	Producer/ offtake/ borrower	Other primary counter-parties	Secondary counter-parties
Identify the expected level of annual transactions and/or money flows to/from the producer	✓	N/A	N/A
Identify and understand the underlying activity of the producer/counterparty and the relationship between the parties	✓	✓	N/A
Identify ownership, control and origin of any assets used as collateral including origin for all underlying commodities	✓	N/A	N/A
Understand where any investment proceeds are to be transferred to	✓	N/A	N/A
Identify the source of any settlement funds	✓	N/A	N/A
Evidence the underlying activity that the commodity based lending is going to be used to support and consider in relation to the operating jurisdiction of the producer	✓	N/A	N/A
Review and confirm that documents in relation to the deal e.g. loan agreements, are legitimate to ensure that commodity based lending is not obtained through fraudulent means which may result in T&S losing significant amount of money	✓	✓	N/A

In addition to the requirements above, the Business Line must establish, where relevant, the origin of the commodities. This could include obtaining the certificate of origin or other equivalent documentation. This must be carried out prior to establishing any relationships with relevant parties to the commodity based lending deal.

22.6 FIs and other co-lenders involved in commodity based lending

The following KYC requirements apply to FIs, including banks, investment funds, including multilateral/supranational banks and development banks/agencies, and government backed credit export agencies, involved in commodity based lending deals.

	Type	Relationship with T&S	KYC Standard	Rationale	Exclusions/conditions
1	FI *(Approved Regulator[55])* who is Facility Agent/Lead Arranger/Security Trustee/Agent for T&S	Direct	BDD	Direct counterparty but limited role; flow of funds between lower risk FI and T&S only in capacity as facility coordinator or security holder	• Usual BDD exclusions apply
2	FI *(Unapproved Regulator)* who is Facility Agent/Lead Arranger/ Security Trustee/Agent for T&S	Direct	Reduced CDD/ EDD as applicable, in line with risk assessment	Direct counterparty but limited role; flow of funds between higher risk FI and T&S	
3	FI (*Approved Regulator[57]):* • With whom T&S enters into a sub-participation arrangement (funded or risk participation); or • To whom T&S sells its loan participation on a secondary market	Direct	SDD	Direct counterparty with relationship initiated/controlled by T&S; flow of funds between lower risk FI and T&S	• Usual SDD exclusions apply

[55] As set out in section 5.4.1, a FI may be classified as regulated by an Approved Regulator if it is directly regulated, or it is a consolidated subsidiary or branch in any country, where the parent company directly or indirectly owns >50% of the subsidiary. This also applies to subsidiaries and branches in EDD countries, as long as the entity/parent also confirms it applies its regulated parent company's ethics and compliance policies. Multilateral banks and development banks/agencies may be treated as regulated by an Approved Regulator if they are headquartered in a country that is not High Risk for Financial Crime purposes.

	Type	Relationship with T&S	KYC Standard	Rationale	Exclusions/conditions
4	FI (*Unapproved Regulator*): • With whom T&S enters into a sub-participation arrangement (funded or risk participation); or • To whom T&S sells its STF participation on a secondary market	Direct	Reduced CDD EDD as applicable	Direct counterparty with relationship initiated/controlled by T&S; flow of funds between higher risk FI and T&S	
5	FI (*Approved and Unapproved Regulator)* who: • Is co-lender with T&S in the same tranche/facility; or • Joins a tranche/facility with T&S due to another lender selling its commitment in a loan	Indirect	BDD (non-EDD countries[56]) Reduced EDD (EDD countries)	Indirect relationship; no flow of funds between T&S and FI (other than via security agent); limited KYC due to source of funds provided to producer/offtake counterparty	• Usual BDD exclusions apply • May also be applied to non-FIs in syndicate, subject to consultation with FC Team and overall risk assessment of deal
6	FI who is: • a co-lender in a different tranche to T&S (same facility); • a co-lender in a different facility; • a facility agent for other facilities; • a security agent or other administrative party for other lenders/ facilities	No relationship	No KYC requirement, unless T&S is asked to directly transact with the party, in which case follow 3 or 4 above	No relationship; T&S may sign intercreditor agreement as part of overall arrangement but no commercial or transactional relationship	

[56] Including subsidiaries or branches in EDD countries where >50% owned, controlled and consolidated by a parent company regulated by an Approved Regulator and counterparty/ parent confirms it applies parent company's ethics and compliance policies.

KYC information and documentation may be provided to T&S and certified as applicable, by an authorised representative of the Facility Agent/Lead Arranger where they are regulated by an Approved Regulator.

22.7 Risk assessment

As part of the KYC process, the Business Line must undertake and document a risk assessment of the commodity based lending transaction and parties, to enable the Financial Crime risks including money laundering.

The risk assessment must consider the following, at a minimum:

- Use of the funds to be provided: identify and understand the intended use of the borrowed funds to ensure that T&S does not become complicit in directly or indirectly funding illegal or unethical activities;

- Sanctions Nexus (Direct and Indirect): in conjunction with the screening undertaken by the FC Team, identify and assess the sanctions risk of all parties and commodities involved in the transaction to ensure that no relationship breaches relevant sanctions regulations or is outside of T&S sanctions risk appetite;

- Business activities and source of funds of borrower and its UBO(s): assess the underlying business activities of the offtake counterparty/borrower including establishing the location of their operations and the legitimacy of the source of funds behind the borrowing entity's business and its UBO(s);

- Parties to the deal: review and assess the parties involved in the deal, including the composition of the lending syndicate, the regulated status of the Facility Agent and other parties and their respective jurisdictions. The jurisdictions they operate in need to be established to ensure that potential bribery and corruption risks have been adequately mitigated.

- Deal fees: What fees have been paid to third parties to identify, negotiate and execute this deal and are they in line with expectations and market practices? Has the Business consulted with the SECO ABC SME regarding the fee profile, where relevant, to look for red flags that might indicate bribery and corruption, or other Financial Crime concerns?

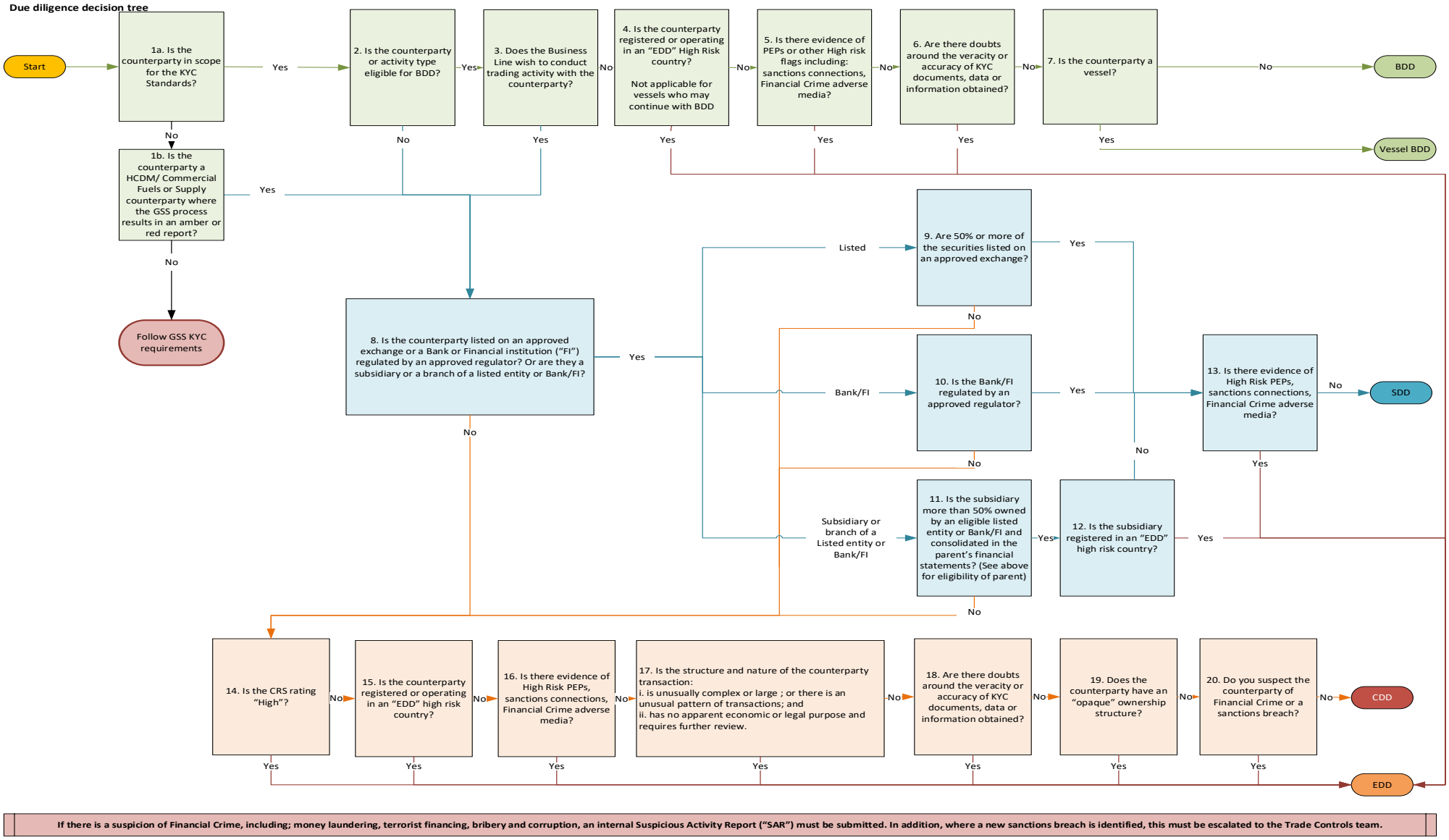
- Contractual protections: Are we protected contractually, for early termination, due to concerns with Financial Crime or Sanctions compliance of parties? How much control do we have in other parties joining the syndicate or wider deal and what KYC rights do we have prior to acceptance?

The rationale for the commodity financing deal must be fully documented based on the risk assessment performed and T&S Business Lines must implement controls to adequately mitigate the risks identified. It is not acceptable for this rationale to be based solely on the commercial advantages that the counterparty relationship presents to T&S.

22.8 Approvals

All commodity financing deals are subject to pre-approval in accordance with the T&S MoA which delegates organisational authority for approving commodity financing deals. In addition, where a deal involves High Risk counterparties, additional approvals may be required as set out in section 13.

APPENDIX 1: DUE DILIGENCE DECISION TREE



APPENDIX 2: ULTIMATE BENEFICIAL OWNER – SPECIFIC ENTITY GUIDANCE

For partnerships and trusts, and similar entity types, the individuals considered to either be a UBO or hold control varies. The list sets out an overview of control per entity type.

1. Trusts: In relation to a trust, the UBOs are:

    - the settlor;
    - the trustees;
    - the beneficiaries, or where the individuals benefiting from the trust have not been determined, the class of persons in whose main interest the trust is set up, or operates; or
    - any individual who has control over the trust.

2. Foundations or other similar arrangement: The beneficial owners are those who hold equivalent or similar positions to those set out above.

3. Legal entity or legal arrangement (e.g. a "Production Sharing Contract" or similar, which is not a body corporate, partnership, trust or foundation (see Appendix 7 for further detail): The UBOs are:

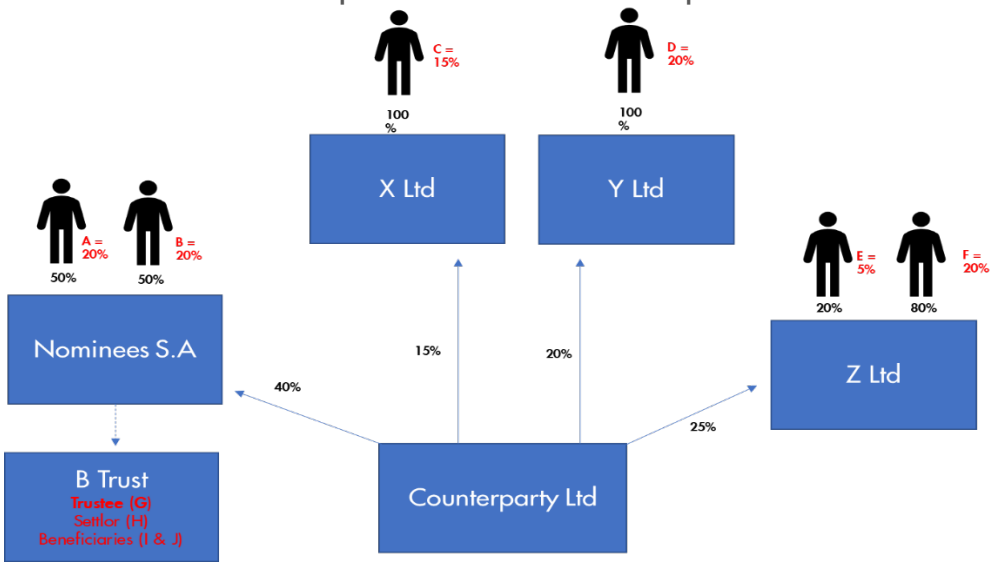
    - any individual who benefits from the property of the entity or arrangement (owns more than 25% for SDD and CDD or owns more than 10% for EDD);
    - where the individuals who benefit from the entity or arrangement have yet to be identified, the class of persons in whose main interest the entity or arrangement is set up or operates; or
    - any individual who exercises control over the property of the entity or arrangement.

Where an individual is the beneficial owner of a body corporate which benefits from or exercises control over the property of the entity or arrangement, the individual is to be regarded as benefiting from or exercising control over the property of the entity or arrangement.

APPENDIX 3: EXAMPLE OF BENEFICIAL OWNERSHIP AND CONTROL

Example of ownership

Set out below is an example on beneficial ownership:



Additional information

1. Nominees S.A. holds shares on behalf of the B Trust, which has 1 x Trustee (G), 1 x settlor (H) and 2 x unrelated beneficiaries each entitled to 50% of the trust assets (I and J).
2. Nominees S.A. votes in accordance with the instructions of the Trustee (G).
3. The shareholder of Y Ltd (D) is the wife of the Trustee of B Trust (G).
4. All other shareholders have full voting rights in accordance with their shareholdings

Based on the diagram above, the following are considered as:

1. Beneficial owners of the counterparty: Nominees S.A, X Ltd, Y Ltd (EDD only), Z Ltd and B Trust
2. UBOs:
    1. CDD: Individuals D + G + H (all own more than 25%)
    2. EDD: Individuals C + D + F + G + H + I + J (all own more than 10%)
3. Who is the Ultimate Controller? Individual G as they direct the decision making of the entity.

Examples of linkages/aggregation of shareholding

Potential linkages between shareholders may include:

- two shareholders who are husband and wife, each with a shareholding of 15%, would constitute UBOs through aggregation as collectively they own 30% of the counterparty; or

- three shareholders, each with a shareholding of 12% but who have a joint agreement to vote together at shareholder meetings, would constitute UBOs, as through aggregation they collectively own 36% of the counterparty.

Examples of control

Set out below are examples of decisions and/or activities which may indicate that an individual has control over an entity. This is neither a prescribed nor exhaustive list. The Business Line should use this information to help identify potential controllers as part of their assessment on the beneficial ownership of a counterparty.

- Directs the activities of a company, trust or firm;

- Has absolute decision rights over decisions related to the running of the business of the company, for example relating to:

    - adopt or amend an entity's business plan;
    - change of an entity's nature of business;
    - request additional borrowing from external lenders outside of previously agreed thresholds;
    - appoint or remove of the CEO or other senior management;
    - establish or amend any profit-sharing, bonus or other incentive scheme of any nature for directors or employees;
    - grant options under a share option or other share-based incentive scheme;

- Hold absolute veto rights over decisions related to the running of the business e.g. appointment of majority of Directors unless this is in relation to certain fundamental matters for the purposes of protecting minority interests in the company which is unlikely, on its own, to constitute "significant influence or control" over the company; or

- A person who is not a member of the board of directors but regularly or consistently directs or influences a significant section of the board, or is regularly consulted on board decisions and whose views influence decisions made by the board;

- A company founder who no longer has a significant shareholding in the company they started, but makes recommendations to the other shareholders on how to vote and those recommendations are always or almost always followed; or

- Authority to wind up the entity.

Share types

Different share types will change the level of control a shareholder has in a company.

1. Ordinary shares

Ordinary shares entitle the shareholder to a vote in matters put before shareholders in proportion to their percentage ownership in the company. Ordinary shareholders are entitled to receive dividends if any are available after dividends on preferred shares are paid.

Ordinary shareholders typically:

- have rights to share in profits, if available;
- have rights to share in surplus assets on winding up; and
- have voting rights.

2. Preferred Shares

Preferred shares (sometimes known as "preference shares") represent partial ownership in a company. These types of shares pay the shareholder a fixed dividend that does not fluctuate, although the company does not need to pay this dividend if it lacks the financial ability to do so.

The main benefit to holding preferred shares is that the shareholder has a greater claim on the company's assets than other shareholders. However, preferred shareholders do not tend to have voting rights.

3. Other

Other share classes include:

- non-voting shares which carry no voting rights;
- restricted voting shares: give only limited rights;
- redeemable shares (buy back): carry the same rights as ordinary shares;
- deferred dividend shares: have full rights as to voting and rank with the ordinary shares on liquidation, but their entitlement to a dividend is deferred until a specific date; and
- deferred shares or founder shares: these shares do not have any rights to dividends either for a set period, or until certain conditions are met.

4. Bearer shares

Bearer shares provide the physical share certificate holder with voting rights and dividends within an entity. No name is recorded on the share certificate. However, unlike ordinary shares or other share classes above, there is no written record kept of the ownership of bearer shares nor the transfer of ownership.

APPENDIX 4: SCREENING GUIDANCE MATERIALITY EXAMPLES

Set out below are examples of material and immaterial Financial Crime adverse media. This is not an exhaustive list as this is a subjective area, and individuals assessing the materiality of any reports, should consult with the FC Team advisors or managers for guidance where required.

a) Material adverse media:

- recent (i.e. within the past 5 years for entities and 10 years for individuals), confirmed involvement in deliberate acts of and/or facilitation of Financial Crime e.g. convictions for money laundering, involvement in terrorist financing, undertaking sanctioned transactions, widescale market abuse, or committing acts of bribery or corruption;

- regulatory enforcement actions due to violation of Financial Crime compliance controls mandated by regulations e.g. significant Financial Crime controls failures or weaknesses, where there is a pattern of repeated behaviour or other indication that the counterparty has taken remedial action, so as to indicate elevated Financial Crime risk exposure;

- recent (i.e. within the past 5 years), ongoing investigations, allegations or probes by external bodies such as regulators or law enforcement agencies indicating significant or repeated illegal conduct by the counterparty or Director or UBO in relation to Financial Crime; or

- reported or identified associations to sanctioned jurisdictions (GECs), entities and/or individuals;

- credible reports alleging that a related party who is a PEP has misappropriated assets from their public office or has been involved or implicated in corruption or acceptance of bribes; or

- reports of illegal activity conducted or facilitated by the counterparty that raises significant concern regarding the ethical conduct or compliance of the counterparty, even where it might not have directly resulted in Financial Crime e.g. involvement in modern slavery or human rights issues.

b) Immaterial adverse media:

- Financial Crime convictions more than five years old for entities and more than ten years old for individuals, but this should be considered in light of whether judicial processes are still ongoing;

- negative financial news such as falls in share price or profit warnings which are not related to Financial Crime;

- probes by external bodies such as regulators or law enforcement agencies where there has been no update over the prior five years, unless systemic/multiple instances of probes;

- allegations which are more than five years old for entities or individuals which did not result in a formal charge or indictment;

- dismissal of allegations or court cases by a judge or law enforcement;

- prosecutions of specific employees for Financial Crime matters who acted independently and/or outside of their area of authority, where the relevant individuals have been disciplined/removed and where the counterparty itself was not directly involved;

- information on litigation cases not directly connected to Financial Crime; or

- regulatory enforcement actions due to violation of Financial Crime compliance controls mandated by regulations, that have been settled and where there is no indication that the counterparty has not taken remedial action.

APPENDIX 5: TRANSLATION REQUIREMENTS

As set out in section 15.3, all counterparty KYC information must be entered into T&S systems (including GoldTier) in English. This section sets out the information to be obtained for all translations.

Translation by an employee

Where translation is provided by a T&S employee, the following employee details must be noted on the relevant document/file:

- name of the employee;
- job title of the employee;
- signature of the employee; and
- date of translation.

Translation by professional firm

Counterparties may choose to have their documents translated by a third party professional firm. Where this occurs, the following details must be noted on the relevant document/file

- name of the translator, where provided;
- legal name and business address of the entity;
- title of the document(s) translated; and
- date of translation.

The Business Lines are responsible for utilising the above information to verify the credentials of the third party translation firm employed by the counterparty.

APPENDIX 6: APPROVED EXCHANGES, REGULATORS AND SOURCES

Click here for approved exchanges, regulators and sources

APPENDIX 7: ADDITIONAL GUIDANCE FOR PARTNERSHIPS

This appendix sets out an overview of common partnership arrangements along with guidance of which individuals may be considered as either a UBO or Director.

a) LLPs ("Limited Liability Partnership")

LLP is a legal entity which is considered to be a corporate body in line with a limited company rather than a partnership. An LLP allows its members to be managers ("managing members") but limits their liability. Scottish partnerships and LLPs must be treated as corporate bodies.

UBOs and directors within this partnership structure are often defined as follows:

UBO	Director
▪ Partners who hold a specified percentage of equity or voting rights (more than 25% for SDD and CDD, more than 10% for EDD) will be considered to be UBOs and must be identified and verified; or ▪ Where no partner holds a number of units or voting rights above the specified percentage, an assessment must be undertaken to identify if any partner can exercise effective control of the LLP; if they can, they must be treated as a UBO.	▪ Partners with responsibility for the day to day operations of the LLP, as per the operating agreement of the LLP, must be treated as directors; ▪ Other individuals who are not partners but have management or administration responsibility for the LLP must be treated as directors; ▪ If the LLP has a separate management or executive board, the partners on the board must be treated as directors.

b) LLCs ("US Limited Liability Company")

A US LLC is a US corporate form which is hybrid of a corporate body, partnership and sole trader. An LLC is owned and operated by members who hold units which are equivalent to shares within corporate bodies.

UBOs and directors within this partnership structure are often defined as follows:

UBO	Director
▪ Members who hold a specified percentage of units or voting rights (more than 25% for SDD and CDD, more than 10% for EDD);	▪ Non-members with senior management or administration responsibility for the LLC must be treated as directors.

▪ Where no member holds a number of units or voting rights above the specified percentage, an assessment must be made to identify if any other member can exercise effective control of the LLC and is so, they must be treated as a UBO; or ▪ Members with responsibility for the day to day operations of the LLC, as per the bylaws or operating agreement of the LLC.	

c) LPs (Limited Partnership)

An LP is a form of partnership where there is a separation between the management responsibility and ownership of the partnership. Owners with management responsibility are referred to as General Partners (as defined below) and all other partners are referred to as Limited Partners.

A General Partner is defined as any partner who has the below attributes:
- Are liable for any debts the business can't pay;
- Control and manage the business; and
- Can make irreversible ('binding') decisions for the business.

UBOs and directors within this partnership structure are often defined as follows:

UBO	Director
▪ General Partners.	▪ If the LP has a separate management board, the members must be treated as directors.

d) Unincorporated associations

An unincorporated association is a business that has no distinct legal form and is principally operated by individuals or groups of individuals.

UBOs and directors within this partnership structure are defined as follows:

UBO	Director
▪ Members owning or controlling more than a specified percentage (more than 25% for SDD or CDD and more than 10% for EDD) of the partnership's capital, profit or voting rights.	▪ Members who otherwise exercise control over the management of the partnership.

APPENDIX 8: GLOSSARY

Term	Explanation
ABC	Anti-Bribery and Corruption
Adverse Media	Adverse media is any kind of unfavourable or negative information found across a wide variety of news sources.
Affiliate	Whilst the strict definition varies between jurisdictions, entities are affiliated, or "affiliates" if they are related to each other via common ownership (full or partial, majority or minority) or if controlled by a common third party.
AML	Anti-Money Laundering
Annual turnover	Total sales generated in a specific period
Approved Exchange	An approved exchange is one that T&S has assessed as having appropriate public disclosure requirements in relation to ownership and business activities, or satisfactory regulatory oversight for AML purposes. See Appendix 6 for a list of approved exchanges.
Authorised Representative	Any individual who is authorised to sign contractual documentation between T&S and the counterparty; or any individual who is authorised by the counterparty to instruct T&S to make a payment or trade on the counterparty's behalf.
Basic due diligence ("BDD")	Basic Due Diligence: The lowest level of due diligence permitted by T&S and can only be applied in restricted circumstances for defined low-risk counterparty types involved in business activities that are not regulated for AML or CTF purposes, and where the proposed relationship is considered to present limited Financial Crime risk.
Bearer Shares	Shareholding is owned by the person(s) who holds the physical share or stock certificate(s) that are not registered on the company's share register. Ownership may be changed easily and frequently with no record of changes in ownership recorded.
Beneficial owner	T&S defines a beneficial owner as any immediate or intermediate shareholders that sit between the counterparty and the UBOs.
Board of Directors	A Board of Directors is a group of people who jointly supervise the activities of an organisation.
Bribery and Corruption	This occurs when a payment, gift, favour or advantage is offered, made, sought or accepted to influence a business outcome. Serious penalties, including prison sentences, may be imposed upon those guilty of bribery. Bribery and corruption may involve Government Officials (GO), companies or private individuals, and may occur directly or

Term	Explanation
	indirectly through third parties (including joint ventures or their participants). Shell prohibits the payment of all bribes and facilitation payments. Further information can be found in the Shell Ethics and Compliance Manual.
Business Relationship	A business, professional or commercial relationship between T&S and a counterparty, which (a) is connected to the business of T&S and (b) is expected by T&S, at the time when contact is established, to have an element of duration.
C&I	Commercial and Industrial
CCO	Chief Compliance Officer
CCP	Central Clearing counterparty
Counterparty due diligence ("CDD")	Counterparty Due Diligence: Standard level of due diligence applied to low and medium risk counterparty relationships.
COFs	Counterparty Onboarding Focal point in LOD1 – responsible for the IDD performed on counterparties and all counterparty outreach.
Counterparty	The entity or individual with whom T&S has a business relationship.
CRS	Counterparty risk scoring. A scoring model designed to measure the financial crime risk presented by a single counterparty relationship.
Direct GI	Direct Government Intermediaries: Any GI where its dealings with a Government Official (GO) are primary or essential to the main purpose, role, or activity for which Shell has engaged that GI.
DMLRO	Deputy Money Laundering Reporting Officer
DNDB	"Do not do business" list – this is a list of counterparties who have been rejected or exited due to sanctions or financial crime risk outside of T&S appetite.
ECM	Ethics and Compliance Manager within SECO: in T&S, the Head of Financial Crime and the Financial Crime Managers are ECMs
Enhanced due diligence ("EDD")	Enhanced Due Diligence: Applying in higher risk scenarios, the obligation to obtain and verify additional information/documentation requirements over and above those required for CDD. EDD measures help to provide greater insight into a company allowing for a more in-depth understanding of the organisation and activities prior to accepting a business relationship and mitigate increased risks.

Term	Explanation
EDD country	The countries agreed by the T&S MLRO and HRCC as requiring automatic application of EDD measures, due to their increased FC risk. This includes those countries mandated by EU AML regulations as "high risk third countries", GECs and HRCs for sanctions, and others as determined by the TSLT under the T&S risk appetite. The current list of EDD countries can be found here.
EVP T&S	Executive Vice President of Trading & Supply
FC Team	Financial Crime Team within T&S Compliance, reporting to the Head of Financial Crime
Financial Crime	Any kind of criminal conduct relating to money or to financial services or markets, including any offence involving: (1) money laundering, including handling the proceeds of crime; or (2) the financing of terrorism; or (3) trade and economic sanctions violations; or (4) bribery and corruption; or (5) tax evasion; or (6) modern slavery; or (7) fraud or dishonesty; or (8) misconduct in, or misuse of information relating to, a financial market.
Financial Crime Risk Appetite	The amount and type of Financial Crime risk that T&S is willing to tolerate.
Financial Crime Risk Management Framework	Measures put in place by T&S to prevent and manage the inherent Financial Crime risks, emerging from the environment in which T&S operates. These measures include the implementation of systems, controls and processes to prevent criminals from using T&S to perpetrate or facilitate Financial Crime.
Fraud	This occurs when a person through false representation, failing to disclose information, or abuse of their position intends to make a gain for themselves or another or to cause loss or expose another to risk of loss. On conviction of fraud a person can face imprisonment or a fine (or both). Examples of fraud include: ▪ Dishonestly making a false representation, e.g. lying about your qualifications to get a job or making a false expense claim ▪ Dishonestly failing to disclose information, e.g. failing to disclose a salary overpayment from payroll ▪ Dishonestly abusing a position of trust, e.g. using your position to divert company payments to a personal account or circumventing sanctions controls Asset misappropriation is any dishonest act, or attempted act to steal or misuse any tangible or intangible assets. Examples include: ▪ Misusing a company car for a personal trip without approval

Term	Explanation
	▪ Theft of cash ▪ Stealing or misusing intellectual property such as trade secrets, registered designs and patents
Foundation	A foundation is a non-profit organisation that is usually created through a single primary donation from an individual or a business and whose funds and programs are managed by its own trustees or directors.
Fund	A fund (or investment fund), is a way of investing in assets alongside other investors to benefit from the inherent advantages of working as part of a group. A fund may be held by the public, such as a mutual fund, exchange-traded fund, or closed-end fund, or it may be sold only to private investors, such as a hedge fund or private equity fund. Funds are often managed by a Fund Manager or a Fund Advisor who will make investments in portfolios of securities on behalf of the investors.
G&A vendors	General and Administrative vendors are parties from whom T&S purchases general products and services to maintain daily operations and administer the business, but where these costs are not directly attributable to a specific counterparty or transaction, or the company's direct supply or trade of commodities.
General Embargoed Countries ("GECs")	Generally Embargoed Countries; countries that are subject to comprehensive sanctions. The link for the current list can be found in the Shell Ethics and Compliance Manual (Trade Compliance Rules).
General Partner	Member of a partnership. The general partner is typically responsible for the management of the partnership and the limited partner is generally an investor only.
GoldTier	GoldTier is a third party KYC workflow tool used to manage T&S counterparty onboarding and risk management processes. GoldTier allows users to capture KYC information and record documentary evidence for the KYC process.
Government Intermediary	Any person, company, firm or joint venture that is engaged by Shell and has any direct or indirect dealings with a government official connected with Shell's business, including an intermediary nominated by a government but paid by Shell. These include processing agents e.g. freight forwarders, customs agents; commercial agents (consultants, business agents); or professional agents (attorneys, accountants) and certain contracts that involve the appointment of a GI e.g. turnkey contracts for the construction of facilities.

Term	Explanation
	See SECO Due Diligence Sharepoint pages for further information
Government Official ("GO")	Under SECO rules, a GO is: an employee of any government agency, ministry or department of a government, including any person acting in official capacity for a government, regardless of rank or position; any official or employee of a company wholly or partially controlled by a government (e.g. a state-owned oil company), a political party or any official of one; any candidate for political office; any officer or employee of a public international organisation, such as the United Nations or World Bank; and immediate family members (spouse, dependent child, parent or household member) of any of the people listed.
GSS	Group Screening Service within Royal Dutch Shell
High FC Risk country	The countries assessed by the Financial Crime Team and MLRO as prone to higher levels of money laundering, terrorist financing, bribery and corruption or other FC risk. The list of country risk ratings is maintained by the FC Team in GoldTier and is subject to change.
Highly Restricted Countries ("HRCs")	Highly Restricted Countries: countries not subject to comprehensive sanctions or embargoes but where certain activities are restricted. The link for the current list can be found in the Shell Ethics and Compliance Manual (Trade Compliance Rules).
High Risk Counterparty Committee ("HRCC")	High Risk Counterparty Committee, comprised of T&S senior management members, who review and approve escalated high-risk counterparties.
HSSE	Health, Safety, Security & Environment: the processes or activities that are carried out to ensure health, safety, security and environmental protection in the working environment.
ID&V	Identification and Verification: ▪ Identification is the process undertaken to obtain and record minimum information in relation to counterparties, and their related parties. ▪ Verification is the process of confirming/evidencing the identified information to independent and reliable sources.
Initial due diligence ("IDD")	Initial Due Diligence is undertaken by the Counterparty Onboarding Focal Points ("COF") within the Business Lines to gather key documentation and data about the proposed counterparty relationship.

Term	Explanation
Indirect GI	Any GI where its dealings with a GO are non-primary or ancillary to the main purpose, role, or activity for which Shell has engaged that GI and where the primary activity to the main purpose could not be done without interacting with a GO.
Indirect Sanctions Nexus	Scenarios whereby a direct counterparty is not subject to sanctions but there is another element in the transaction that is sanctioned. See Sanctions Compliance Policy for examples.
Investment Advisor ("IA")	An IA is a person or organisation that makes investment recommendations or conducts securities analysis in return for a fee. An IA is a separate legal entity to the fund. The IA and IM may be the same person.
Investment Manager ("IM")	An IM is a separate legal entity to the fund which is given authority to act as agent and manage the funds and investments held by the fund vehicle. The IM and IA may be the same person
IMO	International Maritime Organisation
JMLSG	Joint Money Laundering Steering Group – is a UK body which provides guidance on industry best practice for countering the money laundering risk faced by regulated firms
JV	Joint Venture
KYC	Know Your Counterparty
Limited Partner	Member of a partnership. A limited partner is generally an investor only but may also form part of a partnership board.
LOD1	Line of Defence One
LOD2	Line of Defence Two
LOD3	Line of Defence Three
Low FC Risk country	The countries assessed by the Financial Crime Team and MLRO as prone to lower levels of money laundering, terrorist financing, bribery and corruption or other FC risk, or strengthened regulatory oversight and supervision. The list of country risk ratings is maintained by the FC Team in GoldTier and is subject to change.
Medium Risk FC country	The countries assessed by the Financial Crime Team and MLRO as prone to moderate or mitigated levels of money laundering, terrorist financing, bribery and corruption or other FC risk. The list of country risk ratings is maintained by the FC Team in GoldTier and is subject to change.
MI	Management Information

Term	Explanation
MLRO	Money Laundering Reporting Officer
MOA	Manual of Authorities
Money Laundering ("ML")	The process of taking the proceeds of criminal activity and making them appear legal. Preventing money laundering activity is a global concern. Many of the countries where T&S operates now have some form of anti-money laundering legislation. The legislation tends to place criminal liability on both the company and individual employees.
NA	North America
Ongoing due diligence ("ODD")	Ongoing Due Diligence: The process of periodically reviewing KYC and risk profile information held to ensure it is current, accurate and in line with risk appetite. ODD may also be undertaken in response to trigger events indicating a change in KYC or risk information for a counterparty or related party.
OTC	Over the counter
Politically Exposed Person ("PEP")	An individual who is or has, at any time in the preceding three years, been entrusted with a prominent public function. This includes, but is not limited to, heads of state or of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, important political party officials. Immediate family members, or known close associates, are also defined as PEPs.
Publicly Listed company	A publicly listed company is a company that offers its securities (stocks/shares, bonds/loans, etc.) for sale to the public, often through a stock exchange, or through market makers operating in over the counter markets.
RDS Group	Royal Dutch Shell Group
Regulated credit or financial institution	A regulated credit or financial institution is a bank, co-operative or other organisation that provides financial services (including banking, financing, brokerage and investment management) to the public and other institutions. See Appendix 6 for list of approved regulators.
Related Party	A related party is an individual or entity who is considered to exercise control and/or influence over a counterparty through ownership or being otherwise able to influence the actions of a counterparty or make business decisions in respect of the counterparty.
Risk-Based Approach ("RBA")	The adoption of a risk management process for dealing with Financial Crime. This process encompasses recognizing the existence of Financial Crime risks, undertaking an assessment of the risks and implementing

Term	Explanation
	systems, controls and processes to manage and mitigate the identified risks.
Sanctions	Sanctions are used for a number of purposes, including pressurizing a particular country or regime to change their behaviour, or to prevent terrorist financing. There are many different types of sanctions including travel bans, asset freezes, trade embargoes and other restrictions. All companies and individuals within the RDS group must comply with financial sanctions requirements issued by the European Union, United States of America, United Kingdom and United Nations irrespective of their base country. Further information can be found in the SECO Ethics and Compliance Manual.
Sanctions Nexus	Where a transaction has a connection, directly or indirectly, to a: ▪ sanctioned party; ▪ GEC; or ▪ HRC
SARs	Suspicious Activity Reports or Suspicious Activity Reporting
Simplified due diligence ("SDD")	Simplified Due Diligence: Allows for the extent, timing and type of KYC measures to be adjusted for counterparties deemed to present a low degree of financial crime risk.
SEAU	Shell Energy Australia
SECO	Shell Ethics and Compliance Office
SEEL	Shell Energy Europe Limited
Shell	The collective name for all the legal entities and organisations that make up the Royal Dutch Shell PLC group, including T&S.
SIA	Shell Internal Audit
SIETCO	Shell International Eastern Trading Company
Source of Funds ("SOF")	The activity which generates the funds which enable the counterparty to conduct business, for example investment, revenue from products.
Source of Wealth ("SOW")	The activities which have generated the total net worth of an individual, for example inheritance, income, private investment
SPV	Special Purpose Vehicle
STASCO	Shell International Trading and Shipping Company Limited, the UK trading company of T&S, regulated by the FCA for AML purposes
STF	Structured Trade Finance: a type of transaction where parties extend financing to support the trade of commodities, typically in emerging markets.

Term	Explanation
STIL	Shell Trading International Limited
STORs	Suspicious Transaction and Order Reports
STUSCO	Shell Trading US Company
T&S	T&S is a reference to the Shell Trading and Supply Organisation, as a business unit within the Royal Dutch Shell plc ("RDS") Group, or to each separate legal entity within the Shell Trading and Supply Organisation, as the context requires.
T&S Leadership Team ("TSLT")	The T&S Senior Management Team formed of the T&S EVP and other Business Line VPs
Tax Evasion	An unlawful attempt to minimise tax liability through fraudulent techniques to circumvent or frustrate tax laws, such as deliberate understatement of taxable income or wilful non-payment of due taxes.
TC Team	The Trade Compliance team within T&S Compliance, reporting to the Head of Regulation
Terrorist Financing ("TF")	▪ Money or other property which is likely to be used for the purposes of terrorism (including any resources of a proscribed organisation); or ▪ Proceeds of the commission of acts of terrorism; or ▪ Proceeds of acts carried out for the purposes of terrorism "Proceeds of an act" includes a reference to any property which wholly or partly, and directly or indirectly, represents the proceeds of the act (including payments or other rewards in connection with its commission). "Resources" includes any money or other property which is applied or made available, or is to be applied or made available, for use by the organisation.
Trading Activity	This constitutes regulated activity for the purposes of AML and CTF under relevant AML legislation e.g. STASCO business
Trust	A trust is a legal arrangement where one or more trustees are made legally responsible for holding assets, which are placed in trust for the benefit of one or more beneficiaries. The trustees are responsible for managing the trust and carrying out the wishes of the person who has put the assets into trust (the 'settlor').
Ultimate Beneficial Owner ("UBO")	The Ultimate Beneficial owner refers to the natural person(s) who ultimately owns or controls a legal entity and/or the natural person on whose behalf a transaction is being conducted. It also includes those persons who exercise ultimate effective control over a legal entity.

Term	Explanation
Ultimate Controller	The individual who exercises the most significant control over a legal entity whether by virtue of ownership or the ability to execute key operational decisions (such as appoint and remove board members) from the counterparty
Well-known person	A well-known person is defined as an individual who has a substantial, well-known and widely reported public profile e.g. celebrities, members of royalty or prominent entrepreneurs.

APPENDIX 9: CHANGE CONTROL LOG

Version	Section	Change made
1.0 to 2.0	4.7 Financial trading: who is the counterparty?	Clarified that KYC must be applied to exchange-traded counterparties where there is physical delivery of products.
1.0 to 2.0	4.12.1. BDD eligibility	Added clarification that BDD can be applied to Transmission and Distribution system operators, including government-owned transmission/distribution or "grid" operators, and national or regional commodity regulators/bodies, where T&S is paying for the use of a service.
		Clarified that eligibility of BDD for a Shell-owned joint ventures and entities does not include those based in EDD countries.
		Added a footnote to confirm that the definition of small scale for crude leaseholders will be set out in the IDD and CDD operating procedures.
		Expanded the royalty payees reference to capture similar parties and provide clarity that these are in scope for the KYC Standards as T&S transacts with them on behalf of our counterparties.
		Confirmed that BDD may still be applied to Financial Institutions involved in credit or finance activities where these are registered in Low and Medium AML risk countries, even where there are PEPs identified.
1.0 to 2.0	4.12.3 BDD – Shell owned entities	Added a new section to re-confirm the approach for a Shell-owned entity.
1.0 to 2.0	4.12.4.BDD – Vessels Requirements	Added the requirement to screen the vessel name along with the IMO number for vessels
1.0 to 2.0	4.14.1 CDD Requirements	Removed the requirement to verify Source of Wealth for UBO
1.0 to 2.0	4.15.2 High Risk counterparty approvals	Added the requirement that all counterparties registered or with a substantial presence in an EDD country will require HRCC approval, as agreed recently by the HRCC.
1.0 to 2.0	5.3 Information required on related parties	Clarified that residential address does not need to be verified for a UBO or other Related Party. The only requirement for verification is to obtain a government issued photographic ID document.

Version	Section	Change made
		Added a note to confirm the KYC requirement for a corporate trustee of a trust, which must be subject to full KYC.
1.0 to 2.0	6.4.2 UBOs, Ultimate Controllers and Publicly Listed Companies not on an approved exchange	Removed the requirement to identify and verify an Ultimate Controller for any listed entity on an approved exchange.
1.0 to 2.0	6.6 Complex ownership structures	Provided clarity on what constitutes a complex ownership structure.
1.0 to 2.0	7.4 Screening requirements	Screening section amended with two consolidated tables for all counterparties showing which parties are required to be screened for 1) PEPs and sanctions, and 2) Adverse media.
1.0 to 2.0	8.6 PEP risk assessment	Added a note that where SDD is applied, where there is no identifiable UBO and the Ultimate Controller is identified as either the Chairman or CEO, and the individual is also identified as a PEP, the PEP may be treated as Low Risk in the absence of any other risk factors.
1.0 to 2.0	14.4 Certification overview	Amended the wording for the definition of attestation to provide more clarification.
1.0 to 2.0	14.4.2 Eligibility	Removed the requirement for all pages of a certified document to be signed by the certifier.
1.0 to 2.0	16.3 Legal and trading name	Removed the requirement to screen all trading names and any former names.
1.0 to 2.0	16.4 Known aliases	Removed the requirement to screen all known aliases.
1.0 to 2.0	17.2 Deviations	Expanded the approval of a deviation to include a GM's appointed delegate.
1.0 to 2.0	19.4 Trade Finance due diligence requirements	Removed the need for BDD to be performed on a confirming Bank where T&S is the buyer in a trade finance transaction.
1.0 to 2.0	Approved Sources List	▪ Added sources for identification and verification of Source of Funds for individuals ▪ Clarified that verification of ownership structure may be provided by a counterparty in-house professional i.e. lawyer/accountant, only where their credentials can be verified and only for counterparties in non-EDD countries.

Version	Section	Change made
		▪ Clarification that residential address/country of residence for UBOs/Related Parties does not need to be verified where a government-issued, photographic ID document is obtained to verify name and date of birth.
2.0 to 3.0	Numerous changes for annual refresh	▪ For a full list of changes, see T&S KYC Standards Refresh document on Financial Crime Sharepoint
3.0 to 3.1	Minor changes between soft launch and formal launch of 2020 annual refresh version	▪ Section 1.4 Roles & Responsibilities – added Commercial Operations under T&S Business Lines ▪ Section 4.5 Counterparties subject to SECO Due Diligence Process - added Commercial Operations counterparties as currently subject to the due diligence requirements prescribed by SECO - Clarified that counterparties in EDD countries or those requiring GSS enhanced screening are now required to follow T&S KYC Standards ▪ Section 5.3.1 BDD Eligibility - confirmed that those who purchase wholesale gas not just power from T&S for onward sale or local distribution to the end customer are BDD eligible - updated the wording for individual customers and direct suppliers, removing the reference to 'small-scale' for Crude Lease, in anticipation of change to risk based approach being rolled out in April 2021 ▪ SDD requirements – added SPV and branch manager requirements to the relevant tables in sections 5.4.3, 5.5.1 and 5.6.1 ▪ Section 9.6 PEP risk assessment – wording changes to the PEP decision tree to provide more clarity ▪ Section 10.7 Well Known- Persons (PEPs): added wording to confirm the delegate of the Head of Financial Crime can approve the use of non-approved verification sources ▪ Appendix 7 Additional Guidance for Partnerships: minor wording changes to clarify the examples of UBOs and related parties are examples and are not exhaustive
3.1 to 3.2	Appendix 8 - Glossary	▪ Minor updates to the abbreviations and/or definitions of some of the glossary items, to align with the Financial Crime Policy's glossary.