NOTE: This Policy/Procedure applies to those who work for or provide a service to Trading (now part of Supply, Trading & Shipping). More

bp Procedure

ST&S Anti-Money Laundering and Anti-Bribery & Corruption

1 Objective

- To have within ST&S a risk-based, globally consistent framework that seeks to ensure compliance with all applicable external laws and regulations concerning Combating Financial Crime (CFC) risks – including Anti-Money Laundering (AML), Anti-Tax Evasion (ATE), Anti-Bribery and Corruption (ABC), Combating Terrorist Financing (CTF) and related issues, as well as the bp Policy: ABC, AML and ATE.

2 This Applies To

The following Staff (either in ST&S Trading or relevant staff/teams who provide a service to ST&S Trading):

- Staff (employees and contractors) and business units.
- Legal entities owned and controlled by ST&S business units globally except where local legal and regulatory requirements exceed them, in which case the more onerous local requirements take precedence.

3 Key Principles

- ST&S shall have appropriate processes to ensure that it complies with all applicable ABC, ATE, AML laws and Sanctions laws and regulations in jurisdictions in which it operates, as set out this document and in conjunction with the bp Policy: ABC, AML and ATE.
- ST&S shall have adequate processes to proactively protect and mitigate against financial crimes, bribery, corruption, tax evasion, terrorist financing or sanctions whether by ST&S or third parties working for ST&S's benefit, such as agents, brokers, intermediaries, suppliers, distributors, or their sub-contractors.
- Staff shall receive the appropriate training on AML, ABC and related matters, as determined by the GAMLO and E&C, to able to comply with the requirements of the bp Policy: ABC, AML and ATE and this Procedure.
- ST&S shall have an AML methodology, and shall apply due diligence on a risk-based approach consistently within ST&S. See *5.2.2 The AML Risk Assessment Methodology and Tool*.
- ST&S shall only enter into transactions with a Counterparty after the Counterparty Due Diligence (CDD) has been satisfactorily completed and mandatory approvals are obtained. See *5.4 Counterparty Due Diligence (CDD) and Enhanced Due Diligence (EDD)*.
- Staff shall promptly report any suspicion of Money Laundering to the Global Anti-Money Laundering Officer (GAMLO), and shall not knowingly 'tip off' the Counterparty in violation of applicable laws or regulations. See *5.11 Money Laundering Suspicions*.
- Staff shall not make or receive payments to/from third parties or parties, unless it has conducted screening in accordance with the CDD Desk Book. See *5.4.1 Front Office Staff Responsibilities*.
- ST&S shall not trade or deal with prohibited entities unless otherwise approved by the GAMLO. See *5.3 Restrictions on Counterparties*.

4 Introduction

ST&S has corporate, legal and regulatory obligations to adhere to high standards of compliance in relation to the detection and prevention of money laundering.

The ST&S Leadership has responsibilities relating to:

- Transactions that lead to a flow of funds into or out of ST&S; and
- Taking reasonable steps to implement appropriate risk management processes to manage ST&S's exposure to financial crime risks.

ST&S is committed to fully complying with the bp Policy: ABC, AML and ATE and all applicable AML and other financial crime laws in all countries in which ST&S operates.

As part of this commitment, this Procedure indicates ST&S's intention to assist in fulfilling their obligations under the bp Code of Conduct, the bp Policy: ABC, AML and ATE, and applicable AML and financial crime laws.

This Procedure covers all Counterparties engaged directly and indirectly by ST&S in relation to Trading Activities.

Further advice on any aspect of this Procedure can be obtained from the GAMLO.

Note: The bp Group Policies, Procedures and supporting documents on ABC, AML and ATE contain the requirements and processes for Staff to follow on ABC, Exchanging Gifts and Entertainment with Third Parties, Hosting of Government Officials and Joint Ventures, Mergers, Acquisitions or Divestments.

5 bp Procedure Requirements

Note: There are requirements in section *3 Key Principles* that shall also be followed.

The following Procedure sections are included in this document:

- *5.1 General Requirements*.
- *5.2 AML Risk Assessments.*
- *5.3 Restrictions on Counterparties.*
- *5.4 Counterparty Due Diligence (CDD) and Enhanced Due Diligence (EDD)*.
- *5.5 Sleeving*.
- *5.6 Counterparty Engagement*.
- *5.7 Terminating/Rejecting a Counterparty*.
- *5.8 Reliance*.
- *5.9 Outsourcing*.
- *5.10 Liaising with External Authorities*.
- *5.11 Money Laundering Suspicions*.
- *5.12 Escalations*.
- *5.13 Record Keeping*.
- *5.14 The GAMLO*.

5.1 General Requirements

Staff shall comply with the bp Policy: ABC, AML and ATE and its derivative procedures.

Staff who are aware of or suspect violations of the bp Policy: ABC, AML and ATE, or bp Code of Conduct shall promptly report that matter to their line manager, Legal, Group Regulatory Compliance Legal, E&C or OpenTalk, in accordance with the bp's Code of Conduct. In addition, Staff who suspect violations of AML Law or this Procedure shall also notify their concerns to the GAMLO.

5.2 AML Risk Assessments, Methodology and Process Reviews

5.2.1 Risk Assessment

The GAMLO shall conduct risk assessment for ST&S on regular basis. These risk assessments shall take into account the relevant factors including jurisdiction risk, Counterparty risk, transaction or activity risk, and current and emerging trends.

ST&S AML risk assessment and management framework, including the AML risk methodology, shall rank risks as Low, Medium or High.

The GAMLO shall direct that ST&S or ST&S business unit(s) implement appropriate mitigating actions to account for risks identified through the risk assessments.

5.2.2 The AML Risk Methodology and Tool

The CDD team shall apply an approved AML Risk Methodology which establishes risk-based due diligence requirements based on indicators of AML risks relevant to the business. The methodology shall indicate the level of potential Money Laundering risk in the form of a risk rating which shall take into account both quantitative and qualitative factors, and may include (but is not limited to) the following:

- Counterparty type (e.g. private company, listed company, fund, subsidiary of listed company, state owned or controlled, sole trader).
- Counterparty business and history (e.g. energy related, length of business history).
- Transaction type (e.g. physical or paper, speculative trading or compliance requirements, projects, agents or service provider).
- Counterparty or other third-party ownership structure (e.g. overly complicated ownership structures, use of offshore or shell entities).
- Settlement type (e.g. OTC or Exchange, physical delivery or cash settled).
- Involvement of Politically Exposed Persons (PEP).
- The Counterparty's or beneficial owner's reputation, including any negative media.
- Any unresolved sanctions list matches.
- Any other related concerns.

The GAMLO shall approve changes to the AML Risk Methodology, and shall review the AML Risk Methodology on a regular basis, at least every three years. The GAMLO shall document and date each review including any changes made to the methodology as a result of the review. The GAMLO shall preserve historical versions of this Procedure.

ST&S shall maintain a tool that allows for consistent application of the AML Risk Methodology and the assignment of risk rankings to Counterparties in accordance with this Procedure.

The risk rankings for Counterparty type, country, industry type, product & services are set out in *Appendix A: Risk Rankings*.

The ST&S AML risk tool shall be calibrated as needed to ensure that any changes in the risk factors are reflected appropriately. Modifications or changes to the AML Risk Methodology Tool shall not be made without the prior formal approval of the GAMLO.

5.2.3 AML Process Review

The GAMLO shall decide when a review is required to gain assurance over the CDD processes, and shall direct and coordinate the required review. The CDD Coordinator shall take prompt and effective action(s) to address any CDD matters raised from the AML review.

5.3 Restrictions on Counterparties

Staff shall comply with the bp Policy: ABC, AML and ATE and the bp Procedure: ITR – Restricted Countries and Parties (ITR List).

ST&S and Staff shall not trade or deal with the following prohibited entity types unless otherwise approved by the GAMLO:

- Special name accounts – any Counterparty or account using a pseudonym or reference number which is intended to hide or obscure the Counterparty's true name or identity.
- "Brass plate" or "Shell" entities, including banks which are Counterparties that do not maintain a physical place of operation in any country and/or are not affiliated with any legal entity with a traceable physical place of operation.
- Anonymous ownership entity – an entity whose ownership cannot be determined at all times because the entity's shares or certificates are issued in bearer form and the bearer or holder of the instrument is indeterminable and are not controlled or otherwise because the entity has a form or structure that prevents an accurate determination of beneficial ownership.

Where normal market mechanisms prevent the Identification of a prospective Counterparty before the execution of a Transaction, the GAMLO, in conjunction with the CDD team, shall assess the circumstances and consider the AML risk of participating in such markets.

If the GAMLO approves Staff to deal or transact with any of the entity types listed above, the GAMLO shall fully document the reasons for providing approval and retain the details in accordance with this Procedure.

5.4 Counterparty Due Diligence (CDD) and Enhanced Due Diligence (EDD)

5.4.1 Front Office Staff Responsibilities

Staff in the Front Office shall not engage in a Trading Activity with a Counterparty, or make a payment to, or receive a payment from a third party, unless it has conducted screening in accordance with the CDD Desk Book.

Staff in the Front Office shall have roles and responsibilities that include ensuring that material changes to a Counterparty's circumstances, relationship with ST&S or transactions of which they become aware are promptly communicated to the CDD team or the GAMLO.

5.4.2 Application of CDD and EDD

Each ST&S regional business unit shall have the ultimate responsibility for ensuring all Counterparty relationships are subject to appropriate levels of CDD in accordance with the requirements set out in this Procedure and that all relevant approvals are obtained.

The CDD team shall assign every prospective Counterparty a risk rating using the approved AML Risk Methodology Tool described in *5.2.2 The AML Risk Assessment Methodology and Tool*. The level of CDD and monitoring required for a Counterparty shall be aligned to its assigned AML risk rating. Where appropriate, EDD shall be conducted. The due diligence standard and review period for each risk rating is set out in *Appendix B: Due Diligence Standards and Review Periods*.

The CDD team shall obtain any relevant approvals.

The CDD team shall notify the CDD Coordinator or their delegate when a Counterparty activity, product or service is assessed as High Risk. The CDD Coordinator or their delegate shall further assess the risks and decide whether to approve the Counterparty relationship or whether to escalate the matter in accordance with *5.12 Escalations*.

If an existing Counterparty has completed a lower level of regional due diligence than is required for global approval, the CDD team shall apply the required additional due diligence before global approval can be provided. The CDD and EDD processes applied for each Counterparty shall include, at a minimum, Identifying, Verifying and screening the Counterparty (and its UBOs and/or KCPs, as needed). The CDD or EDD processes to be applied for each risk rating are set out in the CDD Desk Book and comply with all requirements in this Procedure.

The CDD team shall apply CDD and/or EDD processes aligned with the risk rating assigned to a Counterparty in accordance with the AML Risk Methodology, this Procedure and the CDD Desk Book.

The ST&S Leadership and the GAMLO shall conduct a review of new Counterparties assessed as High Risk on a regular basis for UK incorporated Regulated Entities and as appropriate for other entities. The GAMLO shall implement any additional CDD and/or monitoring as required by the ST&S Leadership.

5.4.3 CDD Desk Book

The CDD Coordinator shall maintain and implement a written CDD Desk Book that contains mandatory due diligence requirements required by an organization engaged in Trading Activities including (but not limited to):

- CDD team roles and responsibilities.
- Due diligence processes.
- Risk-based standards of Identification, Verification and vetting.
- Required 'Know Your Business' (KYB) information.
- EDD measures.
- Sanctions, PEP and adverse media screening.
- CDD monitoring, enhanced monitoring, reporting KPIs and MI.
- Management of Counterparty's Personal Data.
- Requirements for Global Approvals.
- Data integrity of the CDD systems/databases.
- Quality Assurance processes.
- CDD training.

The CDD Coordinator shall review the CDD Desk Book on a regular basis, at least every three years. The CDD Coordinator shall document and date each review including any changes made to the CDD Desk Book as a result of the review. The CDD Coordinator shall preserve historical versions of the CDD Desk Book.

Any material changes to the CDD Desk Book shall be reviewed and agreed with the GAMLO.

5.4.4 Refreshing the CDD for Counterparties

CDD for Counterparties shall be refreshed at a frequency aligned with their AML risk rating (unless additional reviews are required in particular cases). The refresh periods for each risk rating are set out in *Appendix B: Due Diligence Standards and Review Periods*.

CDD on a Counterparty shall also be refreshed in between the review frequency cycle where there are appropriate risk-based reasons to do so. Examples of such reasons include (but are not limited to):

- Significant adverse media, including investigations, prosecutions, or investigative journalism.
- Significant changes in Counterparty activities or operations, such as reincorporation, new involvement of third-party payees, or moves to higher risk jurisdictions.
- Suspicious activities by the Counterparty, such as significant unexplained changes in trading behaviour, unusual or inappropriate statements by a Counterparty's representatives.

The scope of the CDD refresh shall be consistent with the AML Risk Methodology applicable to the business/region and the Counterparty. CDD refreshes shall be tailored to the circumstances of the individual Counterparty, though generally include:

- Risk-based screening of Counterparty information against reputable databases.
- Updating KYB information.
- Updating CDD documentation and the AML risk rating (as required).

5.4.5 Monitoring

The GAMLO shall be responsible for ensuring that there is a process in place whereby Counterparties are monitored on a risk-basis to identify suspicious transactions or activities, adverse sanctions hits, or other AML concerns.

Staff are individually and collectively responsible for considering the financial crime risk of dealing with any Counterparty with which they are doing or considering doing business.

Where a Counterparty is a High Risk Agent or Medium Risk Agent, a Relationship Manager shall be appointed, as described in the Agents - ST&S Procedure.

The GAMLO may require Staff to implement additional monitoring or the CDD team to undertake a CDD refresh based on emerging events or upon becoming aware of information of concern in relation to a Counterparty.

5.4.6 CDD System & Database

The CDD team shall ensure that the Database or System used to capture the KYC details of a Counterparty contains the following minimum information in addition to the items required in the CDD Desk Book: the full legal name of the Counterparty, its KCPs, and any other relevant parties. Due diligence documentation and approvals shall be dated and stored in this Database or System.

AML information gathered and/or produced that is of a sensitive nature, particularly those that are of a personal nature, shall be stored appropriately and in accordance with applicable data protection requirements, including the bp Policy: Data Privacy. The CDD systems for storage of sensitive information (e.g. Personal Data) shall be endorsed by the GAMLO, with advice from the VP E&C ST&S and Legal, as appropriate.

5.5 Sleeving

Staff shall take appropriate steps to prevent Counterparties from using Sleeving to overcome or circumvent ST&S's Counterparty vetting processes.

Staff shall not use sleeving, other than when all of the following conditions are met:

- It is used to mitigate credit risks or credit concerns arising from a Counterparty.
- Counterparties and Sleeving parties are vetted and approved by CDD.
- The prior approval of the GAMLO for the Counterparty has been given.

Sleeving shall not be used to prevent a third party from completing ST&S's CDD processes.

5.6 Counterparty Engagement

Staff shall ensure that appropriate AML clauses are included in contracts entered into with Counterparties or other third parties where required by the bp Policy: ABC, AML and ATE.

Staff shall, where possible, communicate AML obligations and expectations to Counterparties and third parties prior to entering into any engagement.

5.7 Terminating/Rejecting a Counterparty

If the CDD team considers it necessary to terminate/reject a Counterparty based on the outcome of CDD, other than in respect of AML issues, the CDD team shall document its assessment and justification for the rejection, and submit it to the CDD Coordinator for approval. The CDD Coordinator shall escalate the matter to the GAMLO where they deem appropriate.

If the CDD team considers it necessary to terminate or reject a Counterparty based on AML issues, the CDD team shall document its assessment and justification and submit it to the GAMLO. The GAMLO shall assess the risk posed by the Counterparty relationship, and decide based on this risk assessment whether to terminate or reject the Counterparty.

Termination for AML/ABC purposes other than for routine Counterparty portfolio management shall not be investigated without the consent of, and specific termination instructions from, the GAMLO in consultation with Legal.

If a decision is made to terminate a Counterparty's relationship with ST&S, the GAMLO, working in conjunction with Legal as required, shall provide direction that complete the following actions:

- Notify affected regions, across ST&S.
- Provide direction to the CDD Coordinator and/or CDD Managers on appropriate actions to be taken.
- Provide guidance to ST&S and relevant Staff on appropriate communications with the relevant Counterparty (including any tipping off considerations).
- In line with bp Group requirements, ST&S through the GAMLO shall provide Counterparty Watch List (CWL) inputs on rejected or declined third parties as deemed appropriate by the GAMLO to the designated Group (CWL) coordinator or team.
- Record the details of the Counterparty in any other CDD database or system as appropriate.

The CDD team shall notify without delay the relevant Staff, including E&C, of any change in approval status of a Counterparty. Staff shall promptly update relevant front and back office systems.

5.8 Reliance

ST&S may rely on the CDD information for a Counterparty that is provided by another part or bp Group as long as that the requirements set out in this Procedure and the CDD Desk Book have been complied with.

Regardless of whether CDD information in whole or in part is provided by another part of bp Group, the CDD team and Staff shall continue to be accountable and responsible for ensuring that the requirements of this Procedure are complied with, that the Counterparty meets the CDD requirements, and that ongoing monitoring by ST&S of its Counterparty relationship is effective.

5.9 Outsourcing

If ST&S engages in outsourcing (intra-Group and extra-Group), ST&S shall remain accountable and responsible for ensuring compliance with its AML obligations set out in the bp Policy: ABC, AML and ATE and this Procedure.

The GAMLO shall be accountable for the oversight of the effectiveness of any part of the AML systems and controls activities which are outsourced. The GAMLO may delegate oversight for outsourced CDD activities to the CDD Coordinator.

AML systems and controls activities shall not be outsourced without the prior written approval of the GAMLO. If any part of AML and sanctions control activities are outsourced, ST&S shall put in place an appropriate service level agreement (SLA). The SLA shall provide for the following minimum requirements:

- Specification of the precise activities outsourced.
- Acceptable quality level and time frames.
- How sensitive and confidential information and data (including Personal Data) are to be handled, including how applicable data privacy laws and regulations will be complied with.
- The detailed AML and Sanctions processes to be applied/operated.
- Reporting framework of incidents to designated Staff and the GAMLO including an appropriate escalation procedure.
- Provision of regular management information and KPIs to designated Staff and the GAMLO.
- Provisions reflecting legal, regulatory and ST&S business requirements (including allowing for amendments to reflect changes in them).
- Permissions for regular and ad hoc onsite reviews and inspections by Staff and/or the GAMLO to assess whether AML obligations are being met.

If ST&S performs outsourcing activities for other parts of bp Group an SLA containing appropriate minimum requirements shall also be put in place.

5.10 Liaising with External Authorities

The GAMLO shall decide when to submit a Suspicious Activity Report to appropriate law enforcement agencies.

In consultation with the GAMLO and other Senior Managers, E&C shall consider whether AML matters give rise to obligations for a ST&S regulated entity to make relevant disclosures to the Financial Conduct Authority. This does not supersede any individual obligations that the GAMLO or Senior Managers may have.

Certain Staff, including Senior Managers, may be required to communicate with law enforcement agencies or regulators in order to comply with legal or regulatory obligations.

Legal shall support and advise the GAMLO, E&C and relevant Staff as to the legal obligations that apply in order that those individuals may discharge their regulatory duties, and appropriately liaise with external authorities, and shall also consider what further steps may be legally necessary or desirable more generally, such as the issuing of legal holds.

With the exception of the instances listed above, Staff shall not communicate with law enforcement agencies or regulators on AML matters without prior consultation with ST&S Legal, GAMLO or E&C.

5.11 Money Laundering Suspicions

The GAMLO, in conjunction with Legal, shall agree a process for handling, in a timely and confidential manner, reports of suspicion of Money Laundering, which shall include at a minimum:

- Review of the incident.
- Provide instruction to the business, including on whether the Counterparty relationship is to be terminated or rejected.
- Retention of audit trail.

Staff shall be vigilant of potential Money Laundering risks. Staff shall promptly report to the GAMLO, and to Legal or E&C as appropriate:

- Any major changes in activity of a Counterparty.
- Any unusual circumstances in respect of a Counterparty, transaction or activity.
- Any suspicion of potential Money Laundering.

If Staff have a suspicion of potential Money Laundering, they shall:

- Not execute any payment, transaction, delivery of goods/services or Counterparty instruction without obtaining the prior written approval of the GAMLO.
- Avoid discussions with (or otherwise "tip off") the Counterparty.

Once a suspicion of Money Laundering has been reported, any further communication with the Counterparty shall only be as directed by the GAMLO.

Following a report of suspicion of potential Money Laundering, the GAMLO shall determine whether a suspicion of Money Laundering does exist. After the GAMLO's assessment, appropriate feedback shall be provided to the reporter and the assessment and the decision shall be documented.

If the GAMLO concludes that a suspicion of Money Laundering does exist, the GAMLO shall comply with relevant bp Policies (including Management of Concerns and Investigations, where applicable, and *5.14 The GAMLO*) and applicable legal requirements.

5.12 Escalations

Unless otherwise provided in this Procedure, Staff or the CDD team shall escalate any other concerns through the normal supervisory chain to the CDD Coordinator or a CDD Manager.

Following application of the AML risk assessment, the CDD Coordinator or CDD Manager may escalate the following matters to the GAMLO where required in the circumstances:

- Counterparties with material negative media impacting financial crimes such as money laundering, bribery & corruption, fraud, and other offences for money laundering.
- Counterparties involved in allegations of corruption and financial crimes.
- Counterparties involving high risk PEPs or sanctioned entities.

- Counterparties risk rated as "high risk" for other reason(s) than the jurisdiction they are in.

The GAMLO shall review and decide whether to provide risk-based approval for prospective Counterparties.

The GAMLO shall escalate any concerns about the effectiveness of ST&S's AML systems and controls to the ST&S Leadership or the VP E&C ST&S (as appropriate).

5.13 Record Keeping

The CDD team shall keep and maintain records of any documents or information obtained in carrying out CDD (including EDD) or otherwise related to AML activities for all Counterparties (including information in respect of UBOs and KCPs).

Business units shall keep and maintain supporting records of transactions for five years after the business relationship with the Counterparty ends (or five years after an occasional transaction where there is no ongoing business relationship).

All due diligence documentation and approvals, including certified true copies of original Identification documentation and/or records of electronic Non-Documentary Verification checks undertaken in accordance with the CDD Desk Book, shall be dated and stored on the CDD database or system.

The GAMLO shall keep and maintain records of all reported suspicions of money laundering including assessments and decisions made in respect of whether to report such suspicions.

All information shall be maintained in accordance with the bp Policy: Records Management, the bp Global Records Retention and Disposition Procedure, the bp Policy: Data Privacy and the Record Management - ST&S Procedure.

5.14 The GAMLO

The GAMLO shall:

- Act as MLRO for ST&S. As MLRO the GAMLO shall be responsible for oversight of ST&S's compliance with its AML obligations, including the requirements set out in this Procedure, and shall act as a focal point for ST&S's AML activity.
- Develop an annual plan for independent, risk-based testing of the ST&S AML systems and controls, as set out in this Procedure.
- Review and report annually on the effectiveness of AML systems and controls to the ST&S Leadership and make recommendations for necessary improvements.
- Notify the CDD Coordinator of any matters raised from the review and take prompt and effective action(s) to address such matters.
- As appropriate, consult with Legal, E&C and Group Regulatory Compliance Legal on AML and financial crime matters.

5.15 Governance

The following main roles and accountabilities have been clearly defined for staff for achieving the objectives set out in this document, and these shall be communicated accordingly:

Stakeholder/SPA	Roles and Responsibilities
ST&S Leadership	• Has overall responsibility for the establishment and maintenance of effective anti-money laundering systems and controls. • Review and assess the annual report by GAMLO on AML systems and make recommendations where required.
SVP Finance, ST&S	• SMCR prescribed responsibility for the regulated firms' (BPO/BTL/BET) policies and procedures for countering the risk that the firms might be used to further financial crime. • In conjunction with the VP E&C ST&S, review and approve exemptions and deviations from this Procedure. See *6 Exemptions and Failure to Comply*. • Appoint the GAMLO. • Ensure timely business response to management information provided.
VP E&C ST&S	• In conjunction with SVP Finance, ST&S, review and approve exemptions and deviations from this Procedure. See *6 Exemptions and Failure to Comply*. • Provide advice on CDD systems for storage of Personal Data. • Ensure all Staff receive AML training.
VPs F&R ; SVPs T&S / VPs Regions	• Ensure this Procedure is implemented in their teams.
GAMLO	• Business owner of this document. • Fulfil the role of MLRO for ST&S. See *5.14 The GAMLO*. • Provide global oversight for compliance with rules and regulations on AML systems and controls for ST&S. • Provide guidance on issues arising from the application of this Procedure to business as required. • Provide guidance to Staff and the CDD Team on Counterparties assessed as involving a High Risk of Money Laundering, including providing approval for the Counterparty relationship where required. • Determine when Counterparties are to be rejected or terminated for Money Laundering risk, and the appropriate communications when they are. See *5.7 Terminating/Rejecting a Counterparty*. • Assess and as appropriate provide AML approval for new activities, products or services. • Develop and execute an annual plan for risk-based testing of ST&S AML controls and processes. See *5.14 The GAMLO*. • Approve changes to the AML risk methodology. See *5.2.2 The AML Risk Methodology and Tool*. • Communicate and ensure implementation of changes to the ST&S AML risk management framework. • Ensure that there is a process in place for Counterparties to be monitored on a risk-basis. See *5.4.5 Monitoring*. • Report annually to ST&S Leadership on effectiveness of ST&S AML systems and controls. See *5.14 The GAMLO*. • Decide upon, direct and coordinate AML process reviews. See *5.2.3 AML Process Review*.

Stakeholder/SPA	Roles and Responsibilities
	• Where appropriate, provide risk-based approval for prospective Counterparties and AML risk matters. See *5.12 Escalations*. • Endorse CDD systems for storage of sensitive information (e.g. Personal Data). See *5.4.6 CDD System & Database*. • Approve transactions or dealing with restricted Counterparties listed in section *5.3 Restrictions on Counterparties*. • Approve material changes to the CDD Desk Book and systems. See *5.4.3 CDD Desk Book*. • Approve appropriate use of sleeving. See *5.5 Sleeving*. • Provide oversight of ST&S outsourcing of AML systems and controls. See *5.9 Outsourcing*. • Determine a process for handling suspicions of Money Laundering, and assess reports of suspicions of Money Laundering and determine necessary further actions. See *5.11 Money Laundering Suspicions*. • Submit Suspicious Activity Reports to law enforcement agencies. See *5.10 Liaising with External Authorities*. • As appropriate maintain records of decision-making processes in AML matters. See *5.13 Record Keeping*. • Escalate, as appropriate, relevant matters to the VP E&C ST&S and the ST&S Leadership. See *5.12 Escalations*. • Liaise with relevant AML regulatory bodies and external industry forums, and consult with Legal, as appropriate. • Be alert to Financial Conduct Authority (FCA) statements and final notices to ensure that the FCA Regulated Entities stay up to date with, and act on, national and international findings on deficiencies in the AML regime, as well as monitoring.
CDD Coordinator(s)	• In conjunction with the CDD Managers, develop and implement the CDD Desk Book. See *5.4.3 CDD Desk Book*. • Review the CDD Desk Book on a regular basis and at least every three years. • Ensure alignment between the CDD Desk Book and this Procedure. • Monitor the CDD Quality Assurance Programme. • Implement changes arising from the CDD Quality Assurance Program or the ST&S Leadership's review of processes. • Provide oversight of execution and operation of the CDD processes by the CDD team. • Provide approval for establishing or continuing relationships with Counterparties assessed as High Risk. • Promptly escalate AML concerns to the GAMLO or other functions as appropriate. • Provide the KPIs and MI supporting the effective operations of the CDD team. • Provide oversight to outsourced CDD activities, including those managed by ST&S for and on behalf of other bp Group entities. • Oversee risk-based reviews of CDD to maintain up to date risk profiles.
CDD Managers	• In conjunction with the CDD Coordinator, develop and implement the CDD Desk Book. See *5.4.3 CDD Desk Book*. • Following a Counterparty's AML risk assessment, under appropriate circumstances, escalate the Counterparty and details to the GAMLO. • Create and maintain appropriate KPIs/KRIs.

Stakeholder/SPA	Roles and Responsibilities
CDD teams	• Ensure compliance with local laws and regulations. • Conduct an appropriate level of due diligence for all Counterparties and their UBOs and KCPs in accordance with the AML Risk Methodology and the requirements of this Procedure, and obtain relevant approvals. See *5.2.2 The AML Risk Methodology and Tool*. • Notify relevant Staff of changes to Counterparty information. • Escalate Counterparty activities, products or services that are assessed as High Risk to the CDD Coordinator and/or the GAMLO. • Keep and maintain required records of CDD and AML activities. Escalate Counterparty activities, products or services that are assessed as High Risk to the CDD Coordinator or the GAMLO. • Decide when to terminate/reject a Counterparty based on the outcome of CDD, and submit its justification to the CDD Coordinator for approval. See *5.7 Terminating/Rejecting a Counterparty*.
E&C	• Support the business in implementing this document. • Assist, when required, with implementing an AML risk assessment methodology. See *5.2.2 The AML Risk Methodology and Tool*. • Consider whether AML matters give rise to obligations for a ST&S regulated entity to make relevant disclosures to the Financial Conduct Authority, in consultation with the GAMLO and Senior Managers. See *5.10 Liaising with External Authorities*. • Assist in AML training requirements. See *7 Training*.
Legal	• Support and advise the GAMLO, E&C and relevant Staff as to the legal obligations that apply so they may discharge their regulatory duties and appropriately liaise with external authorities. See *5.10 Liaising with External Authorities*. • Provide advice concerning legal issues regarding Money Laundering, or other issues which may arise in relation to this Procedure. • Provide guidance to the GAMLO and CDD teams in respect of to regulatory requirements.
Staff	• Promptly report any suspicion of Money Laundering to the Global Anti-Money Laundering Officer (GAMLO). • Not enter into any Transaction or pay any Counterparty that has been rejected by the CDD team due diligence process. See *5.4 Counterparty Due Diligence (CDD) and Enhanced Due Diligence (EDD)*. • As first line of defence, know the Counterparties they deal with and assist in updating Counterparty information as required. • Comply with the bp Policy: ABC, AML and ATE and associated Procedures. • Ensure that sleeving is not used to overcome or circumvent ST&S's AML or CDD requirements. See *5.5 Sleeving*. • Not communicate with law enforcement agencies or regulators on AML matters without prior consultation with Legal, GAMLO or E&C, with limited exceptions. See *5.10 Liaising with External Authorities*. • Complete assigned AML and ABC training. See *7 Training*.

6 Exemptions and Failure to Comply

Requests to waive/exempt parts or all of this document shall be put in writing, submitted to and approved by the SVP Finance, ST&S and the VP E&C ST&S. This document overrides any existing waivers granted.

Waivers/exemptions are maintained by the ST&S Policies & Procedures team. Existing waivers/exemptions to this document shall be reapplied for whenever the document undergoes a full review or as required by the ST&S Policies & Procedures Manager.

Failure to comply with external laws and/or regulations may render bp and its employees liable to civil and/or criminal proceedings. In addition, outside of any legal liabilities, a violation of a requirement in this document may constitute an event under the Event Reporting - ST&S Policy & Procedure and may lead to disciplinary action being taken, up to and including dismissal, especially those governing Counterparty Onboarding, KYC and AML. In some jurisdictions such breaches may also render you liable to prosecution by a Law Enforcement or Regulatory Body.

7 Training

Staff shall take and successfully complete mandatory AML, ABC and related training as determined by the GAMLO and E&C ST&S.

8 Glossary

Terms, Definitions, Symbols and Abbreviations are provided below:

Term	Explanation
ATE	Anti-Tax Evasion means reasonable measures to prevent the facilitation of tax evasion by ensuring that all ST&S business dealings and conduct of third parties engaged to act on its behalf or represent it are carried out in an honest and ethical manner consistent with bp values and behaviour. For ST&S this includes ensuring business purpose fit and alignment when engaging with third parties.
BDD	Basic Due Diligence. Means conducting more than a light touch due diligence and also having to verify the Counterparty's identity, that of a beneficial owner (15% or more), and those Key Control Persons. Also, it's still necessary to conduct ongoing monitoring of the business relationship.
CDD	The process of a risk-based 'Counterparty Due Diligence' applied by the CDD team to each prospective Counterparty and any other third party involved in the Transactions/payment. CDD includes undertaking Identification, Verification, and screening of Counterparty information (as described in the CDD Desk Book). CDD supporting iData with clearing of settlement banks. CDD grants approvals commensurate to the risk profile of the counterparty and the business proposal. CDD encompasses a range of knowledge, understanding, and information obtained on a Counterparty throughout the lifecycle of the relationship with ST&S. The CDD Desk Book and this Procedure contains details on the risk-based application of CDD.
CDD Desk Book	A set of Counterparty Due Diligence team processes that set out requirements of risk-based CDD and ongoing monitoring processes, including guidance notes.
CDD team	The teams carrying out Counterparty Due Diligence work for ST&S – which may be in head/regional offices or part of Global Business Services (GBS).

Term	Explanation
Counterparty	For the purpose of AML, any third party with whom bp undertakes Transactions (i.e. as agents, brokers, trade counterparties intermediaries, suppliers, distributors, or their sub-contractors), including bp minority owned Joint Ventures. A Counterparty subsidiary shall be treated as a separate entity for the purposes of CDD and approval, when that subsidiary is party to a Transaction or payment.
EDD	Enhanced Due Diligence – means applying a more intensive level of review to Counterparties that represent a potential high AML risk. Also having to verify the Counterparty's identity, that of a beneficial owner (10% or more), and those Key Control Persons. Also, it's still necessary to conduct ongoing monitoring of the business relationship.
GAMLO	Global Anti-Money Laundering Officer, whose role is to provide oversight for the adequacy and effectiveness of financial crime prevention including the KYC/AML programme and is the in-business contact person for financial crime matters such as KYC/AML related activities and issues. In ST&S this individual also fulfils the role of the Money Laundering Reporting Officer (MLRO). In the GAMLO's absence, the DoA is held by the GAMLO's formally appointed Deputy.
Identification	Establishing the identity of the prospective Counterparty, the Corporate entity and ultimate legal business entity.
ST&S Leadership	The ST&S Executive Leadership.
Joint Venture	A business relationship undertaken for a specific business purpose by bp and one or more unaffiliated parties who contribute tangible and/or intangible assets to the relationship. Joint Ventures include both operated and Non-Operated Joint Ventures.
KCP	Key Control Persons. The Counterparty's Principal Owners and Controllers. Principal Owners and Controllers are legal or natural persons who have legal or beneficial ownership (sometimes referred to as Ultimate Beneficial Owner), or de facto control (directly or indirectly) either: (i) 25% and greater of a company (10% and greater for "High Risk" clients) of the Counterparty or otherwise owning or controlling the Counterparty. This includes any shareholders, directors, executive management and/or other legal or natural persons who are in a position to control funds and/or direct the activities of the Counterparty. Where a Principal Owner or Controller is another corporate entity, risk-based measures shall be taken to establish the identity of the individual(s) who ultimately owns or controls the entity. Verifying the identity of the beneficial owner(s) or Controller(s) is carried out on a risk-based approach.
KPIs/KRIs	Key Performance/Risk Indicators.
KYC	Know Your Counterparty.
May	A permissive statement – an option that is neither mandatory nor specifically recommended.
MLRO	Money Laundering Reporting Officer. The MLRO is the nominated person under the UK Money Laundering Regulation and the Proceeds of Crime Act, and also the approved person (SMCR17, previously CF11) by the UK Financial Conduct Authority (FCA), responsible for the oversight of systems and control regarding financial crimes prevention. In ST&S this role is fulfilled by the GAMLO.
Money Laundering	The term 'Money Laundering' refers to the process by which criminals attempt to conceal the true origin and ownership of the proceeds of their criminal activity and get to use the ultimate proceeds safely and without detection. It can also encompass individuals or entities which become involved in arrangements they either know or suspect facilitate the concealing or legitimizing of illicit funds (i.e. handling the proceeds of crime).

Term	Explanation
	This is a very broad definition which goes beyond concealing money. It can cover the proceeds of any crime, regardless of the amount or value, including property bought with criminal funds. It also includes merely holding any such property. All crimes are covered by this legislation and can include, but are not limited to, the following: (a) trafficking of drugs or people; (b) bribery, blackmail or extortion; (c) fraud; (d) forgery and/or counterfeit money; (e) robbery; (f) terrorist financing; (g) stock manipulation. In AML, therefore, the term 'Money Laundering' is used to refer collectively to Money Laundering, terrorist financing and handling the proceeds of crime. In addition, ST&S's CDD team's screening for sanctions is included in the AML due diligence.
NDV	Non-Documentary Verification method, which typically means Verification through an electronic method usually through interface with databases/sources that are accessible online and provide positive information (relating to full name, current address, date of birth) that provides proof that an individual exists, and offers a higher degree of confidence. Such information should include data from more robust sources - where an individual has to prove their identity, or address, in some way in order to be included, as opposed to others, where no such proof is required. In some instances, non-electronic method may also be approved by the GAMLO as an NDV method.
PEP	Politically Exposed Person. An individual who is or has, at any time, been entrusted with prominent public functions, high political profile, or holds, or has held, public office; and an immediate family member, or a known close associate, of such a person. Examples of PEPs include: Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials, and current or ex-public officials who are in a position to use their position to influence the success of a transaction or contract as well as those with an influential political position who hold an economic interest in the transaction. The definition is not intended to cover middle ranking or more junior officials.
Personal Data	Information relating to natural persons who (i) can be identified or who are identifiable, directly from the information in question, or (ii) who can be indirectly identified from that information in combination with other information.
Regulated Entities	These are BET, BTL, BPEC, BPOI and any other ST&S entity subject to similar financial or prudential regulation.
SDD	Simplified Due Diligence. Means conducting light touch due diligence and not having to verify the Counterparty's identity, or that of a beneficial owner, nor those of Key Control Persons. It is, however, still necessary to conduct ongoing monitoring of the business relationship.
Shall	A bp Requirement, and is used in bp Requirement Documents only when it is designating a bp Requirement. See the bp Requirements site.
Should	A specific recommendation where conformance is not mandatory.
Sleeving	A mechanism to accomplish a sale between parties where one or more parties that have not established a credit relationship, by involving in the transaction chain a third party that has an adequate credit relationship with the other two or more parties. In all cases, the parties involved shall be CDD cleared.

Term	Explanation
ST&S	Supply, Trading & Shipping.
Staff	In this document, this refers to individuals employed or contracted to do work for or provide a service to Trading (now part of Trading & Shipping), whether on a temporary or permanent basis. This includes staff within ST&S, in other parts of bp providing services to Trading (e.g. Finance, Technology, GBS) and individuals external to bp (e.g. contractors).
Suspicious Activity Report	Report made by the GAMLO to external Authorities where the GAMLO considers there to be reportable grounds for suspicion. In the UK, such reports are made to the National Crime Agency.
SVPs ST&S	Trading's face to market SVPs: SVP GPTA, SVP GPTI, SVP RPT.
Tipping off	In some jurisdictions, it is a criminal offence to release information which is likely to prejudice an investigation or potential investigation to do or say anything that might 'tip off' the subject of a suspicion of Money Laundering or financial crime.
Trading Activity	Actions that include: i) the making of any firm bid or offer to purchase, sell and/or exchange (including part exchange, barter and other similar arrangements) any energy product, other commodity, or financial instrument; and/or ii) acceptance of any such offer; and/or iii) any variations to any pre-existing transaction; with the intent to create legally binding relations between the parties (including where applicable with bp legal entities) and whether performance of the relevant transaction is by way of physical delivery and/or financial settlement.
Transaction	For the purposes of AML, in the context of supply and Trading Activities, this term covers: (a) the making of any offer to purchase, sell and/or exchange (including part exchange, barter and other similar arrangements) any energy product, other commodity, or financial instrument (including, for the avoidance of doubt, a derivative of any type); and/or (b) acceptance of any such offer; and/or (c) any variations to any pre-existing transaction; and/or (d) making or accepting, or varying any arrangements for, the provision of goods and/or services (such as advice on any investments) including the services of agents and/or brokers acting for bp, in support of, relating or ancillary to (a), (b) and (c) above; and (e) making, accepting or varying any netting or other credit-related arrangements; with intent to create legally binding relations between the parties (including, where applicable, with ST&S legal entities) and whether performance of the relevant transaction is by way of physical delivery and/or financial settlement.
UBO	These are the Ultimate Beneficial Owners, Legal Representatives and other closely associated persons. A UBO is defined as a natural person, who ultimately owns or controls (directly or indirectly) the Counterparty.
Verification	Using appropriate documents and/or tools, authenticate the identities of the UBOs and key control persons, and the KCPs acting for and on behalf of the legal entity if different from the UBOs.
VPs Regions	One of these roles: • VP Regions, RPTA; • VP Regions, RPTAP; • VP Regions, RPTE.

9 Document Version

Version	Effective Date	Approver	Business Owner	Update Requirement
v1.0	24/04/2007	VP, IST-Compliance		New Standard.
v2.0	27/07/2009	VP, Head of IST Compliance		Version approved in Commitments Committee – updated for business requirements.
v3.0	29/11/2011	Associate General Counsel, Global IST Legal / Global Head E&C - IST		Updated structure and appearance, highlighting Control Processes.
v4.0	01/12/2014	Associate General Counsel, Global IST Legal & Global Head E&C - IST	Head of Trading Business Services	Converted to BP Policy & Procedure.
v5.0	02/09/2015	Associate General Counsel, Global IST Legal & Global Head E&C - IST	Head of Trading Business Services	Normal two-three yearly update, alignment with Group Policy and conversion to Procedure.
v5.0a		Global Head E&C - IST		Reallocated Associate General Counsel, Global IST Legal & Global Head E&C - IST accountabilities.
v6.0	17/02/2017	Global Head of E&C - IST	GAMLO	Update of AML processes and accountabilities and targeted changes to improve alignment with FCA rules and clarify when CDD is required for new Counterparties.
v6.0a				Updated supporting forms.
v6.0b				Minor governance table edits for consistency.
v7.0	30/11/2020	Global Head of E&C - IST	GAMLO	Normal three-yearly update.
v8.0	04/01/2021	VP E&C T&S	GAMLO	Reinvent bp changes.
v8.0a				Hyperlink updates.
v8.0b				Incident reporting now Event reporting.
v8.0c				Hyperlinks updated to new P&P site.
v8.0d				TS to ST&S.
v8.0e				Hyperlink changes

Recent updates to this document are identified with a vertical grey line | to their right-hand side.

10 Further Information

Required References

- bp Policy: Anti-Bribery & Corruption (ABC), Anti-Money Laundering (AML) and Anti-Tax Evasion (ATE).
- bp Policy: International Trade Regulations.
- bp ITR - Restricted Countries and Parties Procedure (ITR List).
- bp Code of Conduct.
- Global Trading Guidelines & Requirements - ST&S Policy.
- Record Management - ST&S Procedure.
- bp Policy: Records Management.
- bp Policy: Data Privacy.

Supporting References

- CDD Desk Book.
- Event Reporting - ST&S Policy & Procedure.
- Agents - ST&S Procedure.
- bp Anti-Bribery and Corruption Toolkit.

Appendix A: Risk Rankings

The following risk rankings form part of the ST&S AML Risk Methodology:

The diagram below gives an indication of "potential risk indicators" whether on a primary or secondary red flag category and further shows what risk levels the risk indicators would normally be classed as. Use these risk rankings to assess the risk associated with Counterparties engaged by ST&S. Refer exceptional circumstances to the CDD Coordinator, who may escalate matters to the GAMLO.

Risk Indicator	Low Risk	Medium Risk	High Risk
Legal Entity (Counterparty Type)	• Listed on a recognized regulated market • Public local authorities within low risk jurisdictions	• Newly registered private companies • Partnerships	• Unregulated Hedge Funds • Special Purpose Vehicles (SPVs) • Trusts • Agents & Associated Persons • Entities with less than transparent or unclear ownership within entities classed as medium & high • Entities with less than transparent or unclear Operations within entities classed as medium & high
Counterparty Business Activity	• End users of products; including fuel oil, gas, power & emissions • Service Providers (except if in high risk regions) • Agents incorporated and operating in low risk jurisdictions • Emissions/Carbon Credits for compliance purposes • Tenders	• Brokerage • Services • Agents incorporated and operating in medium risk jurisdictions • Emissions/Carbon Credit Projects • Indicative Bids • Guarantors unless mitigated to low	• Any business background that is not ideal for ST&S product/services • Vulnerable sectors highlighted by E&C • Agents/Representatives • Gas, Power & Emissions trading (EU only) • Third Party Payments • SPV set up • Equity Investments, Hedge funds
Products & Services	• *Service Providers* – deemed to be lower risk in isolation due to the fact the entity is providing a tangible service. If within a high-risk region, the risk ranking needs to be re-assessed	• *Third Party Payee* – Medium risk if the third-party payee is one with whom we have no contractual relationship. If the third party is unrelated to the Counterparty then the risk MUST be flagged as high.	• *Agents/Commercial Developers/Representatives* - Due to nature of services provided, representative capacity and implications of the Bribery and FCPA Acts currently in force

Risk Indicator	Low Risk	Medium Risk	High Risk
	• *Brokerage* – deemed to be lower risk in isolation since the entity is providing a tangible service. If within a high-risk region, the risk ranking needs to be re-assessed. • *Physical Supply/Trading* – deemed to be lower risk because of the physical nature of the transaction. This may make it less risky from a money laundering perspective but can have its risk rating increased due to potential risk of corruption/sanctions/ risky end-user etc. Another exception is that of products and services relating to Gas/Power/Emissions which are considered high risk as a result of VAT & Carousel fraud and applies only to EU and EEA based Counterparties	• *Derivative/Paper Trading* - Deemed to be higher risk than physical business although not necessarily a high-risk product, if the Counterparty is engaging in financial trading in order to hedge commodity price risk, rather than for speculative trading	
Duration (Counterparty's Existence since Incorporation)	• *Five (5) Years & Above* - Counterparties that have been established for more than 5 years have more operational history and information in the public domain than a newly established Counterparty	• *Between Two and Five (>2<5) Years* - Counterparties that have been in operation for more than 2 years but less than 5 years have some track records but these may not be sufficiently robust to provide a high degree of comfort	• *Less than Two (2) Years* - Counterparties established within 2 years have less operational history, less exposure in the public domain and therefore may have added risk i.e. liquidity, credit, legal and reputational risks irrespective of jurisdiction
PEP Exposure (Politically Exposed Persons)	• Local PEPs in low risk jurisdictions with no evidence of adverse comments	• Local & Foreign PEPs with no evidence of adverse comments but from medium risk regions • PEP exposures that have been adequately made less severe Senior Management	• High risk PEPs with notorious evidence of negative/adverse comments • High risk PEPs in high risk jurisdictions • Local & Foreign • PEPs with influence in high risk regions

Risk Indicator	Low Risk	Medium Risk	High Risk
Sanctions Issues	• No hits detected against the Counterparty, UBOs or any of its KCPs	• Hits found but do not have a "material impact" against bp/ST&S engaging with them • No hits found but the entity is in a region or sector that is prone to legal & economic embargoes and sanctions Note: "material impact" includes (but is not limited to): (i) engagement with a Counterparty that could result in sanctions or other punitive measures; (ii) engagement with a Counterparty that is subject to restrictive measures (such as sanctions or sectoral sanctions)	• The Counterparty, its UBOs or KCPs are based in, or registered in, or provide goods or services to ST&S, in a country which is a Blocked Country or Exception Country on the ITR List, or is included on a Specially Designated Nationals List or is a Designated National • The Counterparty (i) imports raw materials from a country included as a Blocked Country or Exception Country on the ITR List, which could be connected to the product purchased by ST&S or (2) it is believed to export products which it has purchased from ST&S to a Blocked Country or Exception Country on the ITR List, and the business has not been approved in accordance with the ITR List
Country/ Jurisdiction Risk Rankings (detailed list by country to be communicated by GAMLO regularly)	• Advanced economies with well-defined structures for conducting activities • Rule of law is well established with sufficient level of financial crime prevention, detection, and prosecution, including disgorgement of proceeds of crime	• Economies not as fully developed as those of North America /Western Europe. Structures for conducting commercial activities though defined are considered not as fully transparent • Rule of law though defined is less well established and financial crime prevention, detection, and prosecution structures are less than sufficiently embedded	• Largely emerging economies and not as fully developed as those of North America. • Structures for conducting commercial activities though defined for many locations are considered not as fully transparent or embedded. Transparency Corruption Perspective Index is <50 with very few exceptions. • Rule of law though defined but less than fully embedded when it comes to financial crime prevention, detection, and prosecution. The structures are less than sufficiently embedded

Appendix B: Due Diligence Standards and Review Periods

Risk Rating	Risk Assessment	Due Diligence Standard	CDD Review Period
LOW	Minimal risk to the business	**SDD** – Simplified Due Diligence	Three (3) Years
MEDIUM	Moderate risk to the business with potential to be high or low	**BDD** – Basic/Normal Due Diligence	Two (2) Years
HIGH	Greater than normal risk and increased attention needed	**EDD** – Enhanced Due Diligence	One (1) Year or less