CHAPTER 4

RISK-BASED APPROACH

➢ **Relevant law/regulation** ▪ Regulations 18, 19(1), 27 (8), 28(13), 33, 35 and 36 ▪ SYSC 3.1.2 G, 6.1.1 R, 6.3.1-3, 6.3.6 ➢ **Other authoritative pronouncements which endorse a risk-based approach** ▪ FATF Recommendations 1 and 10 ▪ Basel Paper – *Sound management of risks related to money laundering and financing of terrorism (updated February 2016)* ▪ IAIS Guidance Paper 5 ▪ IOSCO Principles paper ▪ ESA Risk Factor Guidelines
➢ **Core obligations** ▪ Identify and assess the risks of money laundering and terrorist financing to which its business is subject ▪ Appropriate systems and controls must reflect the degree of risk associated with the business and its customers ▪ Determine appropriate CDD measures on a risk-sensitive basis, depending on the type of customer, business relationship, product or transaction ▪ Take into account situations and products which by their nature can present a higher risk of money laundering or terrorist financing; these specifically include correspondent banking relationships; and business relationships and occasional transactions with PEPs
➢ **Actions required, to be kept under regular review** ▪ Carry out a formal, and regular, money laundering/terrorist financing risk assessment, including market changes, and changes in products, customers and the wider environment ▪ Ensure internal policies, controls and procedures, including staff awareness, adequately reflect the risk assessment ▪ Ensure customer identification and acceptance procedures reflect the risk characteristics of customers ▪ Ensure arrangements for monitoring systems and controls are robust, and reflect the risk characteristics of customers

Introduction and legal obligations

General

4.1 There are a number of discrete steps in assessing the most cost effective and proportionate way to manage and mitigate the money laundering and terrorist financing risks faced by the firm. These steps are to:

- identify the money laundering and terrorist financing risks that are relevant to the firm;
- assess the risks presented by the firm's particular
  - customers and any underlying beneficial owners*;
  - products or services;
  - transactions;

- delivery channels;
- geographical areas of operation;

- design and implement controls to manage and mitigate these assessed risks, in the context of the firm's risk appetite;
- monitor and improve the effective operation of these controls; and
- record appropriately what has been done, and why.

* *In this Chapter, references to 'customer' should be taken to include beneficial owner, where appropriate.*

4.2 Whatever approach is considered most appropriate to the firm's money laundering/terrorist financing risk, the broad objective is that the firm should know at the outset of the relationship who its customers (and, where relevant, beneficial owners) are, where they operate, what they do, their expected level of activity with the firm. The firm then should consider how the profile of the customer's financial behaviour builds up over time, thus allowing the firm to identify transactions or activity that may be suspicious.

Risk Assessment

Regulation 18(1),(2),(3)

4.3 The ML Regulations require firms to take appropriate steps to identify and assess the risks of money laundering and terrorist financing to which its business is subject, taking into account:

- information on money laundering and terrorist financing made available to them by the FCA;
- risk factors, including factors relating to their customers, countries or geographic areas in which they operate, products, services, transactions and delivery channels.

In considering what steps are appropriate, firms must take into account the size and nature of its business. Firms that do not offer complex products or services and that have limited or no international exposure may not need an overly complex or sophisticated business risk assessment.

Regulation 18(4),(5),(6)

4.4 The risk assessments carried out must be documented, kept up to date and made available to the FCA on request. The FCA may decide that a documented risk assessment in the case of a particular firm is not required where the specific risks inherent in the sector in which the firm operates are clear and understood.

Regulation 16(2)

4.5 The UK government has published a national risk assessment of money laundering and terrorist financing[1] which provides a backdrop to a firm's assessment of the UK risks inherent in its business. Firms should be aware of this publication, and should take account of relevant findings that affect their individual business risk assessment.

[1] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/468210/UK_NRA_October_2015_final_web.pdf

Obligation to adopt a risk-based approach

4.6 Senior management of most firms, whatever business they are in, manage the firm's affairs with regard to the risks inherent in the business environment and jurisdictions the firm operates in, those risks inherent in its business and the effectiveness of the controls it has put in place to manage these risks.

4.7 To assist the overall objective to prevent money laundering and terrorist financing, a risk-based approach:

- recognises that the money laundering/terrorist financing threat to firms varies across customers, jurisdictions, products and delivery channels;
- allows management to differentiate between their customers in a way that matches the risk in their particular business;
- allows senior management to apply its own approach to the firm's procedures, systems and controls, and arrangements in particular circumstances; and
- helps to produce a more cost effective system.

Regulation 33(7),(8) Regulation 37(4),(7)

4.8 A firm therefore uses its assessment of the risks inherent in its business to inform its risk-based approach to the identification and verification of individual customers, which will in turn drive the level and extent of due diligence appropriate to that customer. The firm's decisions on the CDD measures to be applied must take account of Risk Factor Guidelines issued jointly by the European Supervisory Authorities.

4.9 No system of checks will detect and prevent all money laundering or terrorist financing. A risk-based approach will, however, serve to balance the cost burden placed on individual firms and their customers with a realistic assessment of the threat of the firm being used in connection with money laundering or terrorist financing. It focuses the effort where it is needed and will have most impact.

4.10 The appropriate approach in any given case is ultimately a question of judgement by senior management, in the context of the risks they determine the firm faces.

Risk assessment – identification and assessment of business risks

Regulation 18(2)(b)

4.11 A firm is required to assess the risks inherent in its business, taking into account risk factors including those relating to its customers, countries or geographical areas in which it operates, products, services, its transactions and delivery channels.

4.12 Examples of the risks in particular industry sectors are set out in the sectoral guidance in Part II. FATF also publishes papers on the ML/TF risks in various industry sectors, see www.fatf-gafi.org. The UK government has published its first national risk assessment of money

laundering and terrorist financing[2] which provides a backdrop to a firm's assessment of the UK risks inherent in its business. Firms should be aware of this publication, and should take account of relevant findings that affect their individual business risk assessment.

4.13 The risk environment faced by the firm includes the wider context within which the firm operates – whether in terms of the risks posed by the jurisdictions in which it and its customers operate, the relative attractiveness of the firm's products or the nature of the transactions undertaken. Risks are posed not only in relation to the extent to which the firm has, or has not, been able to carry out the appropriate level of CDD in relation to the customer or beneficial owner(s), nor by who the customer or its beneficial owner(s) is (are), but also in relation to the activities undertaken by the customer – whether in the normal course of its business, or through the products used and transactions undertaken.

4.14 The business of many firms, their product and customer base, can be relatively simple, involving few products, with most customers falling into similar categories. In such circumstances, a simple approach, building on the risk the firm's products are assessed to present, may be appropriate for most customers, with the focus being on those customers who fall outside the 'norm'. Other firms may have a greater level of business, but large numbers of their customers may be predominantly retail, served through delivery channels that offer the possibility of adopting a standardised approach to many AML/CTF procedures. Here, too, the approach for most customers may be relatively straightforward, building on the product risk.

4.15 For firms which operate internationally, or which have customers based or operating abroad, there are additional risk considerations relating to the position of the jurisdictions involved, and their reputation and standing as regards the inherent ML/TF risk, and the effectiveness of their AML/CTF enforcement regime.

4.16 Many governments and authorities carry out ML/TF risk assessments for their jurisdictions, and firms should have regard to these, insofar as they are published and available.

4.17 The European Commission is empowered to identify high risk third countries with strategic deficiencies in the area of anti-money laundering or countering terrorist financing. The Commission adopted Delegated Regulation 2016/1675 in July 2016. See http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.254.01.0001.01.ENG.

4.18 Countries may also be assessed using publicly available indices from HM Treasury Sanctions[3], FATF high-risk and non-cooperative jurisdictions[4], Moneyval evaluations[5], Transparency International

[2] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/468210/UK_NRA_October_2015_final_web.pdf
[3] http://hmt-sanctions.s3.amazonaws.com/sanctionsconlist.pdf
[4] http://www.fatf-gafi.org/topics/high-riskandnon-cooperativejurisdictions/
[5] http://www.coe.int/t/dghl/monitoring/moneyval/

Corruption Perceptions Index[6], FCO Human Rights Report[7], UK Trade and Investment overseas country risk pages[8] and quality of regulation[9].

SYSC 6.3.6 G

4.19 In identifying its money laundering risk an FCA-regulated firm should consider a range of factors, including

- its customer, product and activity profiles;
- its distribution channels;
- the complexity and volume of its transactions;
- its processes and systems; and
- its operating environment.

4.20 The firm should therefore assess its risks in the context of how it might most likely be involved in money laundering or terrorist financing. In this respect, senior management should ask themselves a number of questions; for example:

- What risk is posed by the firm's customers?
- What risk is posed by a customer's behaviour?
- How does the way the customer comes to the firm affect the risk?
- What risk is posed by the products/services the customer is using?

4.21 Annex 4-I contains further guidance on considerations firms might take account of in assessing the level of ML/TF risk in different jurisdictions. The concept of an 'equivalent jurisdiction' no longer exists under the ML Regulations.

4.22 When the FCA issues a relevant thematic review report, or updates its *Financial Crime Guide*, as part of its ongoing assessment of ML/TF risks, a firm should consider whether there are any areas of risk or issues of concern which are relevant to the firm's business highlighted within the report. Firms should be aware of the FCA's published enforcement findings in relation to individual firms, and its actions in response to these; this information is available on the FCA website at http://www.fca.org.uk/firms/being-regulated/enforcement/outcomes-notices'.

New technologies

Regulation 19(4)(c), 33(6)(b)(v)

4.23 In identifying and assessing the money laundering or terrorist financing risks, firms must take account of whether new products and new business practices are involved, including new delivery mechanisms, and the use of new or developing technologies for both new and pre-existing products. As well as being specifically required in assessing whether there is a high risk of ML/TF in a particular situation, such a risk assessment should take place prior to the launch of the new products, business practices or the use of new or developing technologies. Appropriate measures should be taken to manage and mitigate those risks, including where relevant in particular cases the application of enhanced due diligence measures.

---

[6] http://cpi.transparency.org/cpi2013/results/
[7] http://www.hrdreport.fco.gov.uk/
[8] http://www.ukti.gov.uk/export/howwehelp/oberseasbusinessrisk/countries.html
[9] http://www.state.gov/eb/rls/othr/ics/2013/index.htm

A risk-based approach – Design and implement controls to manage and mitigate the risks

Regulation 19(1)

4.24 Once the firm has identified and assessed the risks it faces in respect of money laundering or terrorist financing – at EU level, UK level and in relation to the firm itself - senior management must establish and maintain policies, controls and procedures to mitigate and manage effectively the risks of money laundering and terrorist financing identified in its risk assessment. These policies, controls and procedures must take account of the size and nature of the firm's business.

4.25 The policies, controls and procedures designed to mitigate assessed ML/TF risks should be appropriate and proportionate to these risks, and should be designed to provide an effective level of mitigation.

Regulation 19(2)(b)

4.26 Firms must obtain approval from their senior management for the policies, controls and procedures that they put in place and for monitoring and enhancing the measures taken, where appropriate.

4.27 A risk-based approach requires the full commitment and support of senior management, and the active co-operation of business units. The risk-based approach needs to be part of the firm's philosophy, and as such reflected in its procedures and controls. There needs to be a clear communication of policies, controls and procedures across the firm, along with robust mechanisms to ensure that they are carried out effectively, weaknesses are identified, and improvements are made wherever necessary.

Regulation 19, 21

4.28 The policies, controls and procedures referred to in paragraph 4.24 must include:

- risk management practices, customer due diligence, reporting, record-keeping, internal controls, compliance management and employee screening;
- where appropriate with regard to the size and nature of the business, an independent audit function to examine and evaluate the firm's policies, controls and procedures.

4.29 The nature and extent of AML/CTF controls will depend on a number of factors, including:

- The nature, scale and complexity of the firm's business
- The diversity of the firm's operations, including geographical diversity
- The firm's customer, product and activity profile
- The distribution channels used
- The volume and size of transactions
- The extent to which the firm is dealing directly with the customer or is dealing through intermediaries, third parties, correspondents or non face to face access
- The degree to which the firm outsources the operation of any procedures to other (Group) entities.

4.30 The application of CDD measures is intended to enable a firm to form a reasonable belief that it knows the true identity of each customer and beneficial owner, and, with an appropriate degree of confidence, knows the types of business and transactions the customer is likely to undertake. The firm's procedures should include procedures to:

- Identify and verify the identity of each customer on a timely basis
- Identify and take reasonable measures to verify the identity of any ultimate beneficial owner
- Obtain appropriate additional information to understand the customer's circumstances and business, including the expected nature and level of transactions

4.31 How a risk-based approach is implemented will depend on the firm's operational structure. For example, a firm that operates through multiple business units will need a different approach from one that operates as a single business. Equally, it will also be relevant whether the firm operates through branches or subsidiary undertakings; whether their business is principally face to face or online; whether the firm has a high staff/customer ratio and/or a changing customer base, or a small group of relationship managers and a relatively stable customer base; or whether their customer base is international (especially involving high net worth individuals) or largely domestic.

4.32 Senior management should decide on the appropriate approach in the light of the firm's structure. The firm may adopt an approach that starts at the business area level, or one that starts from business streams. Taking account of any geographical considerations relating to the customer, or the transaction, the firm may start with its customer assessments, and overlay these assessments with the product and delivery channel risks; or it may choose an approach that starts with the product risk, with the overlay being the customer and delivery channel risks.

A risk-based approach – customer risk assessments

General

Regulation 28(12)

4.33 Based on the risk assessment carried out, a firm will determine the level of CDD that should be applied in respect of each customer and beneficial owner. It is likely that there will be a standard level of CDD that will apply to the generality of customer, based on the firm's risk appetite.

4.34 As regards money laundering and terrorist financing, managing and mitigating the risks will involve measures to verify the customer's identity; collecting additional information about the customer; and monitoring his transactions and activity, to determine whether there are reasonable grounds for knowing or suspecting that money laundering or terrorist financing may be taking place. Part of the control framework will involve decisions as to whether verification should take place electronically, and the extent to which the firm can use customer

verification procedures carried out by other firms. Firms must determine the extent of their CDD measures on a risk-sensitive basis depending on the type of customer, business relationship, product or transaction.

4.35 To decide on the most appropriate and relevant controls for the firm, senior management should ask themselves what measures the firm can adopt, and to what extent, to manage and mitigate these threats/risks most cost effectively, and in line with the firm's risk appetite. Examples of control procedures include:

- Introducing a customer identification programme that varies the procedures in respect of customers appropriate to their assessed money laundering/terrorist financing risk;
- Requiring the quality of evidence – whether documentary, electronic or by way of third party assurance - to be of a certain standard;
- Obtaining additional customer information, where this is appropriate to their assessed money laundering/terrorist financing risk; and
- Monitoring customer transactions/activities.

It is possible to try to assess the extent to which each customer should be subject to each of these checks, but it is the balance of these procedures as appropriate to the risk assessed in the individual customer, or category of customer, to which he belongs that is relevant.

4.36 A customer identification programme that is graduated to reflect risk could involve:

- a standard information dataset to be held in respect of all customers;
- a standard verification requirement for all customers;
- more extensive due diligence (more identification checks and/or requiring additional information) on customer acceptance for higher risk customers;
- where appropriate, more limited identity verification measures for specific lower risk customer/product combinations; and
- an approach to monitoring customer activities and transactions that reflects the risk assessed to be presented by the customer, which will identify those transactions or activities that may be unusual or suspicious.

Customer risk assessments

Regulation 18

4.37 Although the ML/TF risks facing the firm fundamentally arise through its customers, the nature of their businesses and their activities, a firm must consider its customer risks in the context of the wider ML/TF environment inherent in the business and jurisdictions in which the firm and its customers operate. Firms should bear in mind that some jurisdictions have close links with other, perhaps higher risk, jurisdictions, and where appropriate and relevant regard should be had to this.

4.38 The risk posed by an individual customer may be assessed differently depending on whether the customer operates, or is based, in a

jurisdiction with a reputation for ML/TF, or in one which has a reputation for strong AML/CTF enforcement. Whether, and to what extent, the customer has contact or business relationships with other parts of the firm, its business or wider group can also be relevant.

4.39 In reaching an appropriate level of satisfaction as to whether the ML/TF risk posed by the customer is acceptable and able to be managed, requesting more and more identification is not always the right answer – it is sometimes better to reach a full and documented understanding of what the customer does, and the transactions it is likely to undertake. Some business lines carry an inherently higher risk of being used for ML/TF purposes than others.

Regulation 31(1)

4.40 However, as stated in paragraph 5.2.6, if a firm cannot satisfy itself as to the identity of a customer or the beneficial owner who is not the customer; verify that identity; or obtain sufficient information on the nature and intended purpose of the business relationship, it must not enter into a new business relationship and must terminate an existing one.

4.41 While a risk assessment should always be performed at the inception of the customer relationship (although see paragraph 4.48 below), for some customers a comprehensive risk profile may only become evident once the customer has begun transacting through an account, making the monitoring of transactions and on-going reviews a fundamental component of a reasonably designed RBA. A firm may also have to adjust its risk assessment of a particular customer based on information received from a competent authority.

4.42 Some other firms, however, often (but not exclusively) those dealing in wholesale markets, may offer a more 'bespoke' service to customers, many of whom are already subject to extensive due diligence by lawyers and accountants for reasons other than AML/CTF. In such cases, the business of identifying the customer will be more complex, but will take account of the considerable additional information that already exists in relation to the prospective customer.

General principles – use of risk categories and factors

SYSC 6.3.6 G

4.43 In order to be able to implement a reasonable RBA, firms should identify criteria to assess potential money laundering risks. Identification of the money laundering or terrorist financing risks, to the extent that such terrorist financing risk can be identified, of customers or categories of customers, and transactions will allow firms to design and implement proportionate measures and controls to mitigate these risks.

4.44 Money laundering and terrorist financing risks may be measured using a number of factors. Application of risk categories to customers/situations can then provide a strategy for managing potential risks by enabling firms to subject customers to proportionate controls and oversight. The key risk criteria are: country or geographic risk; customer risk; and product/services risk. The weight given to these criteria (individually or in combination) in assessing the overall risk of

potential money laundering may vary from one institution to another, depending on their respective circumstances. Consequently, firms have to make their own determination as to the risk weights. Parameters set by law or regulation may limit a firm's discretion.

Regulation 33(7)(8), 37(4)(7)

4.45 Annex 4-II contains a fuller list of illustrative risk factors a firm may address when considering the ML/TF risk posed by customer situations, consistent with Risk Factor Guidelines issued jointly by the European Supervisory Authorities, to which firms must have regard.

Regulation 28(13)

4.46 When assessing the ML/TF risks relating to types of customers, countries or geographic areas, and particular products, services, transactions or delivery channel risks, a firm should take into account risk variables relating to those risk categories. These variables, either singly or in combination, may increase or decrease the potential risk posed, thus impacting the appropriate level of CDD measures. Examples of such variables include:

- The purpose of an account or relationship
- The level of assets to be deposited by a customer or the size of transactions undertaken
- The regularity or duration of the business relationship

4.47 When assessing risk, firms should consider all relevant risk factors before determining what is the overall risk category and the appropriate level of mitigation to be applied.

4.48 A risk assessment will often result in a stylised categorisation of risk: e.g., high/medium/low. Criteria will be attached to each category to assist in allocating customers and products to risk categories, in order to determine the different treatments of identification, verification, additional customer information and monitoring for each category, in a way that minimises complexity.

Weighting of risk factors

4.49 When weighting risk factors, firms should make an informed judgement about the relevance of different risk factors in the context of a particular customer relationship or occasional transaction. This often results in firms allocating different 'scores' to different factors – for example, firms may decide that a customer's personal links to a jurisdiction associated with higher ML/TF risk is less relevant in light of the features of the product they seek.

4.50 Ultimately, the weight given to each of these factors is likely to vary from product to product and customer to customer (or category of customer) and from one firm to another. When weighting factors, firms should ensure that:

- Weighting is not unduly influenced by just one factor;
- Economic or profit considerations do not influence the risk rating;
- Weighting does not lead to a situation where it is impossible for any business to be classified as high risk;

- Situations identified by national legislation or risk assessments as always presenting a high money laundering risk cannot be over-ruled by the firm's weighting; and
- Firms are able to override any automatically generated risk scores where necessary. The rationale for the decision to override such scores should be documented appropriately.

4.51 Where a firm uses automated systems, purchased from an external provider, to allocate overall risk scores to categorise business relationships or occasional transactions, it should understand how such systems work and how it combines risk factors to achieve an overall risk score. A firm must always be able to satisfy itself that the scores allocated reflect the firm's understanding of ML/TF risk, and it should be able to demonstrate this to the FCA if necessary.

4.52 When the FCA issues a relevant thematic review report, or updates its *Financial Crime Guide*, as part of its ongoing assessment of ML/TF risks, a firm should consider whether there are any areas of risk or issues of concern which are relevant to the firm's business highlighted within the report. Firms should be aware of the FCA's published enforcement findings in relation to individual firms, and its actions in response to these; this information is available on the FCA website at http://www.fca.org.uk/firms/being-regulated/enforcement/outcomes-notices'.

Lower risk/simplified due diligence

4.53 Many customers, by their nature or through what is already known about them by the firm, carry a lower money laundering or terrorist financing risk. ~~These might include:~~

~~➢ Customers who are employment-based or with a regular source of income from a known source which supports the activity being undertaken; (this applies equally to pensioners or benefit recipients, or to those whose income originates from their partners' employment);~~
~~➢ Customers with a long-term and active business relationship with the firm; and~~
~~➢ Customers represented by those whose appointment is subject to court approval or ratification (such as executors).~~
➢

Regulation 37(1) 4.54 ~~There are other circumstances where the risk of money laundering or terrorist financing may be lower. In such circumstances, and~~ p<u>P</u>rovided there has been an adequate analysis of the risk by the country or by the firm, the firm may (if permitted by local law or regulation) apply reduced CDD measures. [See Part I, paragraphs 5.4.1ff for additional guidance on simplified due diligence.] ~~When assessing the ML/TF risks relating to types of customers, countries or geographic areas, and particular products, services, transactions or delivery channels, potentially lower risk situations may be influenced by:~~

~~➢ Customer risk factors~~
~~➢ Country or geographic risk factors~~
~~➢ Product, service, transaction or delivery channel risk factors~~
➢

Regulation 33(7)(8), 37(4)(7)

4.55 Annex 4-II contains a fuller list of illustrative risk factors a firm may address when considering the ML/TF risk posed by customer situations, consistent with Risk Factor Guidelines issued jointly by the European Supervisory Authorities, to which firms must have regard.

4.56 Having a lower money laundering or terrorist financing risk for identification and verification purposes does not automatically mean that the same customer is lower risk for all types of CDD measures, in particular for ongoing monitoring of transactions.

4.57 Firms should not, however, judge the level of risk solely on the nature of the customer or the product. Where, in a particular customer/product combination, *either or both* the customer and the product are considered to carry a higher risk of money laundering or terrorist financing, the overall risk of the customer should be considered carefully. Firms need to be aware that allowing a higher risk customer to acquire a lower risk product or service on the basis of a verification standard that is appropriate to that lower risk product or service, can lead to a requirement for further verification requirements, particularly if the customer wishes subsequently to acquire a higher risk product or service.

4.58 Further considerations to be borne in mind in carrying out a risk assessment are set out in the sectoral guidance in Part II.

Higher risk/enhanced due diligence

4.59 When assessing the ML/TF risks relating to types of customers, countries or geographic areas, and particular products, services, transactions or delivery channels, potentially higher risk situations may be influenced by

- Customer risk factors
- Country or geographic risk factors
- Product, service, transaction or delivery channel risk factors

Regulation 33(1)

4.60 Where higher risks are identified, firms are required take enhanced measures to manage and mitigate the risks. Politically Exposed Persons and Correspondent relationships have been specifically identified by the authorities as higher risk. Specific guidance on enhanced due diligence in these cases is given in section 5.5.

4.61 Where a customer is assessed as carrying a higher risk, then depending on the product sought, it will be necessary to seek additional information in respect of the customer, to be better able to judge whether or not the higher risk that the customer is perceived to present is likely to materialise. Such additional information may include an understanding of where the customer's funds and wealth have come from. Guidance on the types of additional information that may be sought is set out in section 5.5.

4.62 Where the risks of ML/TF are higher, firms must conduct enhanced due diligence measures consistent with the risks identified.

Regulation33(4)

(a) In particular, they must:

- as far as reasonably possible, examine the background and purpose of the transaction; and
- increase the degree and nature of monitoring of the business relationship, in order to determine whether these transactions or activities appear unusual or suspicious.

Regulation 33(5)

(b) Examples of other EDD measures that, depending on the requirements of the case, could be applied for higher risk business relationships include:

- Obtaining, and where appropriate verifying, additional information on the customer and updating more regularly the identification of the customer and any beneficial owner
- Obtaining additional information on the intended nature of the business relationship
- Obtaining information on the source of funds or source of wealth of the customer
- Obtaining information on the reasons for intended or performed transactions
- Obtaining the approval of senior management to commence or continue the business relationship
- Conducting enhanced monitoring of the business relationship, by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination
- Requiring the first payment to be carried out through an account in the customer's name with a bank subject to similar CDD standards

Regulation 33(7)(8) 37(4)(7)

4.63 Annex 4-II contains a fuller list of illustrative risk factors a firm may address when considering the ML/TF risk posed by customer situations, consistent with Risk Factor Guidelines issued jointly by the European Supervisory Authorities, to which firms must have regard.

Regulation 33(1)(f),(4)

4.64 Where EDD measures are applied, firms must as far as reasonably possible examine the background and purpose of all complex ~~and~~ or unusually large transactions, unusual patterns of transactions and transactions which have no apparent economic or legal purpose. They must also increase the degree and nature of monitoring of the business relationship in which such transactions are made to determine whether those transactions or that relationship appear to be suspicious.

4.65 In the case of some situations assessed as high risk, or which are outside the firm's risk appetite, the firm may wish not to take on the customer, or may wish to exit from the relationship. This may be the case in relation to particular types of customer, or in relation to customers from, or transactions to or through, particular high risk countries or geographic areas, or in relation to a combination of other risk factors.

4.66 Although jurisdictions may be subject to economic sanctions, there may be some situations where for humanitarian or other reasons a firm may, under licence, take on or continue with the customer or the business or transaction in, to, or through such high risk jurisdictions.

4.67 The firm must decide, on the basis of its assessment of the risks posed by different customer/product combinations, on the level of verification

that should be applied at each level of risk presented by the customer. Consideration should be given to all the information a firm gathers about a customer, as part of the normal business and vetting processes. Consideration of the overall information held may alter the risk profile of the customer.

4.68 Identifying a customer as carrying a higher risk of money laundering or terrorist financing does not automatically mean that he is a money launderer, or a financier of terrorism. Similarly, identifying a customer as carrying a low risk of money laundering or terrorist financing does not mean that the customer is not. Staff therefore need to be vigilant in using their experience and common sense in applying the firm's risk-based criteria and rules (see Chapter 7 – Staff awareness, training and alertness).

4.69 When the FCA issues a relevant thematic review report, or updates its *Financial Crime Guide*, as part of its ongoing review of its controls to manage and mitigate its ML/TF risks, a firm should consider how its systems, controls and procedures appear in relation to the self-assessment questions set out in the report. Firms should be aware of the FCA's published enforcement findings in relation to individual firms, and its actions in response to these; this information is available at http://www.fca.org.uk/firms/being-regulated/enforcement/outcomes-notices'

A risk-based approach – Monitor and improve the effective operation of the firm's controls

Regulation 19(2)(b)
SYSC 6.3.8 R

4.70 The policies, controls and procedures should be approved by senior management, and the measures taken to manage and mitigate the risks (whether higher or lower) should be consistent with national requirements and with guidance from competent authorities.

4.71 Independent testing of, and reporting on, the development and effective operation of the firm's RBA should be conducted by, for example, an internal audit function (where one is established), external auditors, specialist consultants or other qualified parties who are not involved in the implementation or operation of the firm's AML/CTF compliance programme.

SYSC 6.3.3 R

4.72 The firm will need to have some means of assessing that its risk mitigation procedures and controls are working effectively, or, if they are not, where they need to be improved. Its policies, controls and procedures will need to be kept under regular review. Aspects the firm will need to consider include:

- appropriate procedures to identify changes in customer characteristics, which come to light in the normal course of business;
- reviewing ways in which different products and services may be used for money laundering/terrorist financing purposes, and how these ways may change, supported by typologies/law enforcement feedback, etc;

- adequacy of staff training and awareness;
- monitoring compliance arrangements (such as internal audit/quality assurance processes or external review);
- where appropriate, the establishment of an internal audit function;
- The balance between technology-based and people-based systems;
- Capturing appropriate management information;
- Upward reporting and accountability;
- Effectiveness of liaison with other parts of the firm; and
- Effectiveness of the liaison with regulatory and law enforcement agencies.

4.73 When the FCA issues a relevant thematic review report, or updates its *Financial Crime Guide*, as part of its monitoring of the performance of its ML/TF controls, a firm should consider whether any of the examples of poor practice have any resonance within the firm. Firms should be aware of the FCA's published enforcement findings in relation to individual firms, and its actions in response to these; this information is available on the FCA website at http://www.fca.org.uk/firms/being-regulated/enforcement/outcomes-notices.

A risk-based approach – Record appropriately what has been done and why

SYSC 6.3.3 R
Regulation 18(4)

4.74 Firms must document their risk assessments in order to be able to demonstrate their basis, keep these assessments up to date, and have appropriate mechanisms to provide appropriate risk assessment information to competent authorities.

4.75 Annex 4-III contains illustrative examples of systems and controls a firm might have in place in order to keep its risk assessments up to date.

4.76 The responses to consideration of the issues set out above, or to similar issues, will enable the firm to tailor its policies and procedures on the prevention of money laundering and terrorist financing. Documentation of those responses should enable the firm to demonstrate to its regulator and/or to a court:

- how it assesses the threats/risks of being used in connection with money laundering or terrorist financing;
- how it agrees and implements the appropriate systems and procedures, including due diligence requirements, in the light of its risk assessment;
- how it monitors and, as necessary, improves the effectiveness of its systems and procedures; and
- the arrangements for reporting to senior management on the operation of its control processes.

4.77 In addition, on a case-by-case basis, firms should document the rationale for any additional due diligence measures it has undertaken (or any it has waived) compared to its standard approach, in view of its risk assessment of a particular customer.

Risk management is dynamic

SYSC 6.3.3 R

4.78 Risk management generally is a continuous process, carried out on a dynamic basis. A money laundering/terrorist financing risk assessment is not a one-time exercise. Firms must therefore ensure that their risk management processes for managing money laundering and terrorist financing risks are kept under regular review.

4.79 There is a need to monitor the environment within which the firm operates. Success in preventing money laundering and terrorist financing in one area of operation or business will tend to drive criminals to migrate to another area, business, or product stream. Periodic assessment should therefore be made of activity in the firm's market place. If evidence suggests that displacement is happening, or if customer behaviour is changing, the firm should be considering what it should be doing differently to take account of these changes.

4.80 In a stable business change may occur slowly: most businesses are evolutionary. Customers' activities change (without always notifying the firm) and the firm's products and services – and the way these are offered or sold to customers – change. The products/transactions attacked by prospective money launderers or terrorist financiers will also vary as perceptions of their relative vulnerability change.

4.81 There is, however, a balance to be achieved between responding promptly to environmental changes, and maintaining stable systems and procedures.

4.82 A firm should therefore keep its risk assessment(s) up to date. An annual, formal reassessment might be too often in most cases, but still appropriate for a dynamic, growing business. It is recommended that a firm revisit its assessment at least annually, even if it decides that there is no case for revision. Firms should include details of the assessment, and any resulting changes, in the MLRO's annual report (see paragraphs 3.37 to 3.45).

Annex 4-I

CONSIDERATIONS IN ASSESSING THE LEVEL OF ML/TF RISK IN DIFFERENT JURISDICTIONS

1. This Annex is designed to assist firms by setting out how they might approach their assessment of other jurisdictions, to determine their level of ML/TF risk. The Annex discusses jurisdictions where there may be a presumption of low risk, and those where such a presumption may not be appropriate without further investigation. It then discusses issues that a firm should consider in all cases when coming to a judgement on the level of ML/TF risk implicit in any particular jurisdiction.

Implications of an assessment as low risk

2. Assessment of a jurisdiction as low risk only allows for some easement of the level of due diligence carried out – it is not a complete exemption from the application of CDD measures in respect of customer identification. It does not exempt the firm from carrying out ongoing monitoring of the business relationship with the customer, nor from the need for such other procedures (such as monitoring) as may be necessary to enable a firm to fulfil its responsibilities under the Proceeds of Crime Act 2002.
3. Although the judgement on the risk level is one to be made by each firm in the light of the particular circumstances, senior management is accountable for this judgement – either to its regulator, or, if necessary, to a court. It is therefore important that the reasons for concluding that a particular jurisdiction is low risk (other than those in respect of which a presumption of low risk may be made) are documented at the time the decision is made, and that it is made on relevant and up to date data or information.

Categories of country

(a) *EU/EEA member states*

4. When identifying lower risk jurisdictions, FATF encourages firms to take into consideration country risk factors:

   - Countries identified by credible sources, such as mutual evaluation or detailed assessment reports, as having effective AML/CFT systems.
   - Countries identified by credible sources as having a low level of corruption or other criminal activity.

   In making a risk assessment, countries or financial institutions could, when appropriate, also take into account possible variations in money laundering and terrorist financing risk between different regions or areas within a country.

5. All Member States of the EU (which, for this purpose, includes Gibraltar as part of the UK, and Aruba as part of the Kingdom of the Netherlands) are required to enact legislation and financial sector procedures in accordance with the EU Fourth Money Laundering Directive. The directive implements the revised 2012 FATF standards.

All EEA countries have undertaken to implement the fourth money laundering directive and all are members of FATF or the relevant FATF style regional body (for Europe, this is MONEYVAL).

6. **Gibraltar** is also directly subject to the requirements of the money laundering directive, which it has implemented. It is therefore considered to be low risk for these purposes.
7. Given the commitment to implement the Fourth Money Laundering Directive, firms may initially presume EEA member states to be low risk; significant variations may however exist in the precise measures that have been taken to transpose the money laundering directive (and its predecessors) into national laws and regulations. Moreover, the effective implementation of the standards will also vary. Where firms have substantive information which indicates that a presumption of low risk cannot be sustained, either in general or for particular products, they will need to consider whether their procedures should be enhanced to take account of this information.
8. The status of implementation of the fourth money laundering directive across the EU is available at http://ec.europa.eu/internal_market/company/docs/official/080522web_en.pdf.

(b) *FATF and FATF style regional body members*

9. All FATF members, including members of FATF style regional bodies, undertake to implement the FATF anti-money laundering and counter-terrorism Recommendations as part of their membership obligations.

10. However, unlike the transposition of the money laundering directive by EU Member States, implementation cannot be mandatory, and all members will approach their obligations in different ways, and under different timetables.

11. Information on the effectiveness of implementation in these jurisdictions may be obtained through scrutiny of Mutual Evaluation reports, which are published on the FATF website, as well as through the FATF public statement, compliance statement and advisory notices issued by HM Treasury.

(c) Other jurisdictions

12. A majority of countries and territories do not fall within the lists of countries that can be presumed to be low risk This does not necessarily mean that the AML/CTF legislation, and standards of due diligence, in those countries are lower than those in other jurisdictions assessed as low risk. However, standards vary significantly, and firms will need to carry out their own assessment of particular countries. In addition to a firm's own knowledge and experience of the country concerned, particular attention should be paid to any FATF-style or IMF/World Bank evaluations that have been undertaken.

13. As a result of due diligence carried out, therefore, for the purposes of determining those jurisdictions which, in the firm's judgement, are low risk, firms may rely, for the purposes of carrying out CDD measures, on other regulated firms situated in such a jurisdiction.

Factors to be taken into account when assessing other jurisdictions

14. Factors include:

- Geographical risk factors
- Membership of groups that only admit those meeting a certain benchmark
- Contextual factors – political stability; level of (endemic) corruption etc
- Evidence of relevant (public) criticism of a jurisdiction, including HMT/FATF advisory notices
- Independent and public assessment of the jurisdiction's overall AML regime
- Need for any assessment to be recent
- Implementation standards (inc quality and effectiveness of supervision)
- Incidence of trade with the jurisdiction – need to be proportionate especially where very small

Geographical risk factors

15. Geographical risk factors include:

    - countries identified by credible sources, such as mutual evaluations, detailed assessment reports or published follow-up reports, as not having effective systems to counter money laundering or terrorist financing;
    - countries identified by credible sources as having significant levels of corruption or other criminal activity, such as terrorism, money laundering, and the production and supply of illicit drugs;
    - countries subject to sanctions, embargos or similar measures issued by, for example, the European Union or the United Nations;
    - countries providing funding or support for terrorism;
    - countries that have organisations operating within their territory which have been designated—
        - by the government of the United Kingdom as proscribed organisations under Schedule 2 to the Terrorism Act 2000, or
        - by other countries, international organisations or the European Union as terrorist organisations;

    Firms should bear in mind that the presence of one or more risk factors may not always indicate that there is a high risk of money laundering or terrorist financing in a particular situation.

Membership of an international or regional 'group'

16. There are a number of international and regional 'groups' of jurisdictions that admit to membership only those jurisdictions that have demonstrated a commitment to the fight against money laundering and terrorist financing, and which have an appropriate legal and regulatory regime to back up this commitment.

Contextual factors

17. Such factors as the political stability of a jurisdiction, and where it stands in tables of corruption are relevant to whether it is likely that a jurisdiction will be low risk. It will, however, seldom be easy for firms to make their own assessments of such matters, and it is likely that they will have to rely on external agencies for such evidence – whether prepared for general consumption, or specifically for the firm. Where the firm looks to publicly available evidence, it will be important that it has some knowledge of the criteria that were used in making the assessment; the firm cannot rely solely on the fact that such a list has been independently prepared, even if by a respected third party agency.

    Evidence of relevant (public) criticism

18. The FATF from time to time issues statements on its concerns about the lack of comprehensive AML/CTF systems in a number of jurisdictions (see section 2.4 below). When constructing their internal procedures, therefore, financial sector firms should have regard to the need for additional monitoring procedures for transactions from any country that is listed on these statements of concern. Additional monitoring procedures will also be required in respect of correspondent relationships with financial institutions from such countries.

19. Other, commercial agencies also produce reports and lists of jurisdictions, entities and individuals that are involved, or that are alleged to be involved, in activities that cast doubt on their integrity in the AML/CTF area. Such reports lists can provide some useful and relevant evidence – which may or may not be conclusive – on whether or not a particular jurisdiction is likely to be low risk.

Mutual evaluation reports

20. Particular attention should be paid to assessments that have been undertaken by standard setting bodies such as FATF, and by international financial institutions such as the IMF.

FATF

21. FATF member countries monitor their own progress in the fight against money laundering and terrorist financing through regular mutual evaluation by their peers. In 1998, FATF extended the concept of mutual evaluation beyond its own membership through its endorsement of FATF-style mutual evaluation programmes of a number of regional groups which contain non-FATF members. The groups undertaking FATF-style mutual evaluations are

    - the Offshore Group of Banking Supervisors (OGBS) see www.ogbs.net
    - the Caribbean Financial Action Task Force (CFATF) see www.cfatf.org
    - the Asia/Pacific Group on Money Laundering (APG) see www.apgml.org
    - MONEYVAL, covering the Council of Europe countries which are not members of FATF see www.coe.int/Moneyval
    - the Financial Action Task Force on Money Laundering in South America (GAFISUD) see www.gafisud.org
    - the Middle East and North Africa Financial Action Task Force (MENAFATF) see www.menafatf.org
    - the Eurasian Group (EAG) see www.eurasiangroup.org,
    - the Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG) see www.esaamlg.org
    - the Intergovernmental Action Group against Money-Laundering in Africa (GIABA) see www.giabasn.org

22. Firms should bear in mind that mutual evaluation reports are at a 'point in time', and should be interpreted as such. Although follow up actions are usually reviewed after two years, there can be quite long intervals between evaluation reports in respect of a particular jurisdiction. Even at the point an evaluation is carried out there can be changes in train to the jurisdiction's AML/CTF regime, but these will not be reflected in the evaluation report. There can also be subsequent changes to the regime (whether to respond to criticisms by the evaluators or otherwise) which firms should seek to understand and to factor into their assessment of whether the jurisdiction is low risk.

23. In assessing the conclusions of a mutual evaluation report, firms may find it difficult to give appropriate weighting to findings and conclusions in respect of the jurisdiction's compliance

with particular Recommendations. For the purposes of assessing level of risk, compliance (or otherwise) with certain Recommendations may have more relevance than others. The extent to which a jurisdiction complies with the following Recommendations may be particularly relevant:

Legal framework:
Recommendations 1, 3, 4 and 5
Measures to be taken by firms:
Recommendations 9, 10, 11, 17 and 20,
Supervisory regime:
Recommendations 26, 27 and 35
International co-operation:
Recommendations 2 and 40

24. Summaries of FATF and FATF-style evaluations are published in FATF Annual Reports and can be accessed at www.fatf-gafi.org. However, mutual evaluation reports prepared by some FATF-style regional bodies may not be carried out fully to FATF standards, and firms should bear this in mind if a decision on whether a jurisdiction is low risk is based on such reports.

IMF/World bank

25. As part of their financial stability assessments of countries and territories, the IMF and the World Bank have agreed with FATF a detailed methodology for assessing compliance with AML/CTF standards, using the FATF Recommendations as the base. A number of countries have already undergone IMF/World Bank assessments in addition to those carried out by FATF, and some of the results can be accessed at www.imf.org. Where IMF/World Bank assessments relate to FATF members, the assessments are formally adopted by the FATF and appear on the FATF website.

Implementation standards (including effectiveness of supervision)

26. Information on the extent and quality of supervision of AML/CTF standards may be obtained from the extent to which a jurisdiction complies with Recommendations 17, 23, 29 and 30.

Incidence of trade with the jurisdiction

27. In respect of any particular jurisdiction, the level and extent of due diligence that needs to be carried out in making a judgement on the level of risk will be influenced by the volume and size of the firm's business with that jurisdiction in relation to the firm's overall business.

UK prohibition notices and advisory notices

Prohibition notices

28. Under certain circumstances, HM Treasury may, pursuant to the Counter-terrorism Act 2008, Schedule 7, issue directions to a firm in relation to customer due diligence; ongoing monitoring; systematic reporting; and limiting or ceasing business. Details of any such HM Treasury directions will be found at www.hm-treasury.gov.uk.

Advisory notices

HM Treasury

29. HM Treasury issues advisory notices in which it expresses the UK's full support of the work of the FATF on jurisdictions of concern. The HM Treasury advisory notice is available at https://www.gov.uk/government/publications/money-laundering-and-terrorist-financing-controls-in-overseas-jurisdictions-advisory-notice

30. The FATF issues periodic announcements about its concerns regarding the lack of comprehensive AML/CTF systems in various jurisdictions.

31. The FATF maintains a *Public Statement* which lists jurisdictions of concern in three categories:

    1. Jurisdictions subject to a FATF call on its members and other jurisdictions to apply countermeasures to protect the international financial system from the ongoing and substantial money laundering and terrorist financing (ML/TF) risks emanating from the jurisdiction.

    2. Jurisdictions with strategic AML/CTF deficiencies that have not committed to an action plan developed with the FATF to address key deficiencies. The FATF calls on its members to consider the risks arising from the deficiencies associated with each jurisdiction, as described below.

    3. Jurisdictions previously publicly identified by the FATF as having strategic AML/CTF deficiencies, which remain to be addressed.

32. The FATF also maintains a statement *Improving Global AML/CTF Compliance: On-going Process*, which lists jurisdictions identified as having strategic AML/CTF deficiencies for which they have developed an action plan with the FATF. While the situations differ among jurisdictions, each has provided a written high-level political commitment to address the identified deficiencies. The FATF will closely monitor the implementation of these action plans and encourages its members to consider the information set out in the statement.

33. The latest versions of these FATF Statements are available at http://www.fatf-gafi.org**.**

FCA

34. The FCA expect firms they supervise for money laundering purposes to consider the impact of these statements on their policies and procedures.

ANNEX 4-II

ILLUSTRATIVE RISK FACTORS RELATING TO CUSTOMER SITUATIONS

I. CUSTOMER RISK FACTORS

A. Business or professional activity

Risk factors that may be relevant when considering the risk associated with a customer's or their beneficial owners' business or professional activity include:

• Does the customer or beneficial owner have links to sectors that are associated with higher corruption risk, such as construction, pharmaceuticals and healthcare, arms trade and defence, extractive industries and public procurement?

• Does the customer or beneficial owner have links to sectors that are associated with higher ML or TF risk, for example certain Money Service Businesses, casinos or dealers in precious metals?

• Does the customer or beneficial owner have links to sectors that involve significant amounts of cash?

• Where the customer is a legal person, what is the purpose of their establishment? For example, what is the nature of their business?

• Does the customer have political connections, for example, are they a Politically Exposed Person (PEP), or is their beneficial owner a PEP? Does the customer or beneficial owner have any other relevant links to a PEP, for example, are any of the customer's directors PEPs and if so, do these PEPs exercise significant control over the customer or beneficial owner? In what jurisdiction is the PEP, his business or a business he is connected with, located?

• Does the customer or beneficial owner hold another public position that might enable them to abuse public office for private gain? For example, are they senior or regional public figures with the ability to influence the awarding of contracts, decision-making members of high profile sporting bodies or individuals that are known to influence the government and other senior decision-makers?

• Is the customer a legal person subject to enforceable disclosure requirements that ensure that reliable information about the customer's beneficial owner is publicly available, for example public companies listed on stock exchanges that make such disclosure a condition for listing?

• Is the customer a credit or financial institution from a jurisdiction with an effective AML/CTF regime and is it supervised for compliance with local AML/CTF obligations? Is there evidence that the customer has been subject to supervisory sanctions or enforcement for failure to comply with AML/CTF obligations or wider conduct requirements in recent years?

• Is the customer a public administration or enterprise from a jurisdiction with low levels of corruption?

• Is the customer's or their beneficial owner's background consistent with what the firm knows about their former, current or planned business activity, their business'

turnover, the source of funds and the customer's or beneficial owner's source of wealth?

• Is the customer a beneficiary of a life insurance policy in situations where there may be an increased risk, for example life settlements, or beneficiaries with no obvious links to the policy holder?

• Is the customer a third country national who is applying for residence rights in or citizenship of an EEA state in exchange for transfers of capital, purchase of property, government bonds, or investment in corporate entities in that EEA state?

B. Reputation

The following risk factors may be relevant when considering the risk associated with a customer's or their beneficial owners' reputation**:**

• Are there any adverse media reports or other relevant information sources about the customer? For example, are there any allegations of criminality or terrorism against the customer or their beneficial owners? If so, are these credible? Firms should determine the credibility of allegations on the basis of the quality and independence of the source data and the persistence of reporting of these allegations, among others. The absence of criminal convictions alone may not be sufficient to dismiss allegations of wrongdoing.

• Is the customer, beneficial owner or anyone publicly known to be closely associated with them had their assets frozen due to administrative or criminal proceedings or allegations of terrorism or terrorist financing? Does the firm have reasonable grounds to suspect that the customer or beneficial owner or anyone publicly known to be associated with them has, at some point in the past, been subject to such an asset freeze?

• Does the firm know if the customer or beneficial owner has been subject to a suspicious activity report in the past?

• Does the firm have any in-house information about the customer's or their beneficial owner's integrity, obtained, for example, in the course of a long-standing business relationship?

C. Nature and behaviour

The following risk factors may be relevant when considering the risk associated with a customer's or their beneficial owners' nature and behaviour (not all of these risk factors will be apparent at the outset, but may emerge only once a business relationship has been established):

• Does the customer have legitimate reasons for being unable to provide robust evidence of their identity, perhaps because they are an asylum seeker?

• Does the firm have any doubts about the veracity or accuracy of the customer's or beneficial owner's identity?

• Are there indications that the customer might seek to avoid the establishment of a business relationship? For example, does the customer look to carry out one or

several one-off transactions where the establishment of a business relationship might make more economic sense?

• Is the customer's ownership and control structure transparent and does it make sense? If the customer's ownership and control structure is complex or opaque, is there an obvious commercial or lawful rationale?

• Does the customer issue bearer shares or have nominee shareholders?

• Is the customer a legal person or arrangement that could be used as an asset holding vehicle?

• Is there a sound reason for changes in the customer's ownership and control structure?

• Does the customer request transactions that are complex, unusually or unexpectedly large or have an unusual or unexpected pattern without apparent economic or lawful purpose or a sound commercial rationale? Are there grounds to suspect that the customer is trying to evade certain thresholds?

• Does the customer request unnecessary or unreasonable levels of secrecy? For example, is the customer reluctant to share CDD information, or do they appear to disguise the true nature of their business?

• Can the customer's or beneficial owner's source of wealth or source of funds be easily explained, for example through their occupation, inheritance or investments?

• Does the customer use their products and services as expected when the business relationship was first established?

• Where the customer is a non-resident, could their needs be better serviced elsewhere? Is there a sound economic or lawful rationale for the customer requesting the type of financial service sought? Note that EU law creates a right for customers who are legally resident in the EU to obtain a basic bank account, but this right applies only to the extent that firms can comply with their AML/CTF obligations.

• Is the customer a non-profit organisation whose activities expose it to particularly high risks of abused for terrorist financing purposes?

II. COUNTRIES AND GEOGRAPHIC AREAS FACTORS

When identifying the risk associated with countries and geographic areas, firms should consider the risk related to:

a) the jurisdiction in which the customer or beneficial owner is based;

b) the jurisdictions which are the customer´s or beneficial owner's main place of business; and

c) the jurisdiction to which the customer or beneficial owner has relevant personal links.

Annex 4-I sets out further guidance on considerations firms might take account of in assessing the level of ML/TF risk in different jurisdictions.

III. PRODUCTS, SERVICES AND TRANSACTIONS RISK FACTORS

When identifying the risk associated with their products, services or transactions, firms should consider the risk related to:

a) the level of transparency, or opaqueness, the product, service or transaction afford;

b) the complexity of the product, service or transaction; and

c) the value or size of the product, service or transaction.

Risk factors that may be relevant when considering the risk associated with a product, service or transaction's transparency include:

• To what extent do products or services facilitate or allow anonymity or opaqueness of customer, ownership or beneficiary structures, for example pooled accounts, bearer shares, fiduciary deposits, offshore and certain trusts, or legal entities like foundations that are structured in a way to take advantage of anonymity and dealings with shell companies or companies with nominee shareholders that could be abused for illicit purposes?

• To what extent is it possible for a third party that is not part of the business relationship to give instructions, *e.g.* certain correspondent banking relationships?

Risk factors that may be relevant when considering the risk associated with a product, service or transaction's complexity include:

• To what extent is the transaction complex and involves multiple parties or multiple jurisdictions, for example certain trade finance transactions? Are transactions straightforward, for example regular payments into a pension fund?

• To what extent do products or services allow payments from third parties or accept overpayments where this is not normally foreseen? Where third party payments are foreseen, does the firm know the third party's identity, for example a state benefit authority or a guarantor? Or are products and services funded exclusively by fund transfers from the customer's own account at another financial institution that is subject to AML/CTF standards and oversight that are comparable to those required under the UK regime?

• Does the firm understand the risks associated with its new or innovative product or service, in particular where this involves the use of new technologies or payment methods?

Risk factors that may be relevant when considering the risk associated with a product, service or transaction's value or size include:

• To what extent are products or services cash intensive, such as many payment services but also certain current accounts?

• To what extent do products or services facilitate or encourage high value transactions? Are there any caps on transaction values of levels of premium that could

limit the use of the product or service for money laundering or terrorist financing purposes?

IV. DELIVERY CHANNEL RISK FACTORS

When identifying the risk associated with the way the customer obtains the products or services they require, firms should consider the risk related to:

a) the extent to which the business relationship is conducted on a non-face to face basis; and

b) any introducers or intermediaries the firm might use and the nature of their relationship to the firm.

When assessing the risk associated with the way the customer obtains the product or services, firms should consider a number of factors including:

• Is the customer physically present for identification purposes? If they are not, has the firm used a reliable form of non-face to face CDD? Has it taken steps to prevent impersonation or identity fraud? Has the firm used an electronic identification process that is secure from fraud and misuse and capable of providing an appropriate level of assurance?

• Has the customer been introduced from other parts of the same financial group and if so, to what extent can the firm rely on this introduction as reassurance that the customer will not expose the firm to excessive ML/TF risk? What has the firm done to satisfy itself that the group entity applies CDD measures to UK standards?

• Has the customer been introduced from a third party, for example a bank that is not part of the same group, and is the third party a financial institution or is their main business activity unrelated to financial service provision? What has the firm done to be satisfied that:

i. the third party applies CDD measures and keeps records to UK standards and that it is supervised for compliance with comparable AML/CTF obligations in line with UK requirements?

ii. the third party will provide, immediately upon request, relevant copies of identification and verification data, among others in line with UK requirements? and

iii. the quality of the third party's CDD measures is such that it can be relied upon?

• Has the customer been introduced through a tied agent, *i.e.* without direct firm contact? To what extent can the firm be satisfied that the agent has obtained enough information so that the firm knows its customer and the level of risk associated with the business relationship?

• If independent or tied agents are used, to what extent are they involved on an ongoing basis in the conduct of business? How does this affect the firm's knowledge of the customer and ongoing risk management?

• Where a firm uses an intermediary, are they:

i. a regulated person subject to AML obligations that are consistent with those of the UK regime?

ii. subject to effective AML supervision? Are there any indications that the intermediary's level of compliance with applicable AML legislation or regulation is inadequate, for example because the intermediary has been sanctioned for breaches of AML/CTF obligations?

iii. based in a jurisdiction associated with higher ML/TF risk? Where a third party is based in a high risk third country that the Commission has identified as having strategic deficiencies, firms must not rely on that intermediary. However, reliance may be possible provided that the intermediary is a branch or majority-owned subsidiary undertaking of another firm established in the EU, and the firm is confident that the intermediary fully complies with group wide policies, controls and procedures in line with UK requirements.

• Is there a transaction related to oil, arms, precious metals, tobacco products, cultural artefacts, ivory and other items related to protected species (*), and other items of archaeological, historical, cultural and religious significance, or of rare scientific value, where the ML/TF risk is raised?

(*) Protected species: illegal wildlife trade can be defined as the illegal hunting, poaching, taking, possession, sales, transport, smuggling, trade or trafficking of CITES designated species and/or other protected wildlife, including their parts and products, according to specific national laws or international treaties.

ANNEX 4-III

CONSIDERATIONS IN KEEPING RISK ASSESSMENTS UP TO DATE

Firms should keep their assessment of ML/TF risk associated with individual business relationships and occasional transactions, as well as the underlying factors, under review to ensure their assessment of ML/TF risk remains up to date and relevant. Firms should assess information obtained as part of their ongoing monitoring of the business relationship and consider whether this affects the risk assessment.

Firms should also ensure that they have systems and controls in place to identify emerging ML/TF risks and that they can assess and, where appropriate, incorporate these in their business-wide and individual risk assessments in a timely manner.

Examples of systems and controls firms should put in place to identify emerging risks include:

- processes to ensure internal information is reviewed regularly to identify trends and emerging issues, both in relation to individual business relationships and the firm's business;

- processes to ensure the firm regularly reviews relevant information sources. This should involve, in particular:

  i. regularly reviewing media reports that are relevant to the sectors or jurisdictions the firm is active in;

  ii. regularly reviewing law enforcement alerts and reports;

  iii ensuring that the firm becomes aware of changes to terror alerts and sanctions regimes as soon as they occur, for example by regularly reviewing terror alerts an looking for sanctions regime updates; and

  iii. regularly reviewing thematic reviews and similar publications issued by competent authorities.

- processes to capture and reviewing information on risks relating to new products;

- engagement with other industry representatives and competent authorities (such as round tables, conferences and training) and processes to feed back any findings to relevant staff; and

- establishing a culture of information sharing within the firm and strong company ethics.

Examples of systems and controls firms should put in place to ensure their individual and business-wide risk assessment remains up to date include:

- setting a date at which the next risk assessment update takes place, *e.g.* on the 1 March every year, to ensure new or emerging risks are included in the risk assessment. Where the firm is aware that a new risk has emerged, or an existing one has increased, this should be reflected in the risk assessment as soon as possible; and

- carefully recording issues throughout the year that could have a bearing on the risk assessment, such as internal suspicious transaction reports, compliance failures and intelligence from front office staff.

Like the original risk assessments, any update of a risk assessment and adjustment of accompanying CDD measures should be proportionate and commensurate with the ML/TF risk.