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 July 2020)*
  - IAIS Guidance Paper 5
  - IOSCO Principles paper
- **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 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/proliferation 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, terrorist financing and proliferation financing risks faced by the firm. These steps are to:

- identify the money laundering, terrorist financing and proliferation 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/proliferation 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, and 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) 18A(1),(2),(3)

4.3 The ML Regulations require firms to take appropriate steps to identify and assess the risks of money laundering, terrorist financing and proliferation financing[1] to which its business is subject, taking into account:

- information on money laundering, terrorist financing and proliferation 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) 18A(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); 16A

4.5 The UK government has published national risk assessments (NRAs) of money laundering, terrorist financing and proliferation financing[2] which provide a backdrop to a firm's assessment of the UK risks inherent in

[1] The Money Laundering and Terrorist Financing (Amendment)(No.2) Regulations 2022 introduced a requirement for proliferation financing risk assessments wef 1 September 2022. A stand-alone PF risk assessment is not required.

[2] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/468210/UK_NRA_October_2015_final_web.pdf; https://www.gov.uk/government/publications/national-risk-assessment-of-money-laundering-and-terrorist-financing-2017; https://www.gov.uk/government/publications/national-risk-assessment-of-money-laundering-and-terrorist-financing-2020; https://www.gov.uk/government/publications/national-risk-assessment-of-proliferation-financing

its business. Firms should be aware of these publications, and should take account of relevant findings that affect their individual business risk assessment.

Regulation 16A(9)

4.5A The meaning of proliferation financing, as it relates to risk assessment, policies, controls and procedures, is specifically limited to the provision of funds or financial services for use in contravention of a relevant financial sanctions obligation.

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, terrorist financing and proliferation financing, a risk-based approach:

- recognises that the money laundering/terrorist financing/proliferation 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)
Regulation 37(4)

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.

4.9 No system of checks will detect and prevent all money laundering, terrorist financing and proliferation 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, terrorist financing and proliferation 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 judgment 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/PF risks in various industry sectors, see www.fatf-gafi.org. The UK government has published national risk assessments of money laundering and terrorist financing which provide a backdrop to a firm's assessment of the UK risks inherent in its business. Firms should be aware of these publications, 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/PF risk, and the effectiveness of their AML/CTF enforcement regime.

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

4.17 The UK's list of high-risk countries is set out in Schedule 3ZA of the ML Regulations (as amended by The Money Laundering and Terrorist Financing (Amendment) (High-Risk Countries) Regulations 2022) which identifies high-risk third countries with strategic deficiencies in the area of anti-money laundering or counter terrorist financing. The list mirrors FATF's jurisdictions under increased monitoring and high-risk jurisdictions subject to a call for action.
See https://www.gov.uk/government/publications/money-laundering-advisory-notice-high-risk-third-countries--2/hm-treasury-advisory-notice-high-risk-third-countries.

4.18 Countries may also be assessed using publicly available indices from, for example, HM Treasury Sanctions, FATF high-risk and non-cooperative jurisdictions, Transparency International Corruption Perceptions Index and the Department of International Trade (see paragraph 3.30).

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, terrorist financing and proliferation 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/PF 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 (https://www.fca.org.uk/about/enforcement).

New technologies

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

4.23 In identifying and assessing the money laundering, terrorist financing and proliferation 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/PF 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.

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

Regulation 19(1); 19A(1)

4.24 Once the firm has identified and assessed the risks it faces in respect of money laundering, terrorist financing and proliferation financing, senior management must establish and maintain policies, controls and procedures to mitigate and manage effectively the risks of money laundering, terrorist financing and proliferation 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/PF risks should be appropriate and proportionate to these risks, and should be designed to provide an effective level of mitigation.

Regulation 19(2)(b), 19A(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, 19A, 21
20(1)(b)

4.28 The policies, controls and procedures referred to in paragraph 4.24 must include, but are not limited to:

- 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.
- for parent firms, policies on the sharing of information about customers, customer accounts and transactions.

4.29 The nature and extent of AML/CTF/PF 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, terrorist financing and proliferation financing, managing and mitigating the risks will involve measures to verify the customer's identity; collecting additional information about the customer; and monitoring their 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/proliferation 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/proliferation 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 they belong 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/PF 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/PF 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/PF, or in one which has a reputation for strong AML/CTF enforcement, or whether a customer is established in a high risk third country (see 5.5.11). 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/PF 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/PF 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/PF. 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), 37(4)

4.45 Annex 4-II contains a fuller list of illustrative risk factors a firm may address when considering the ML/TF/PF risk posed by customer situations.

Regulation 28(13)

4.46 When assessing the ML/TF/PF 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 judgment 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/PF 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/PF 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 (https://www.fca.org.uk/about/enforcement).

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 provided there has been an adequate analysis of the risk by the country or by the firm, including taking into account risk factors in Regulation 37(3), 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.)]

4.55 Annex 4-II contains a fuller list of illustrative risk factors a firm may address when considering the ML/TF/PF risk posed by customer situations.

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/PF 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 to 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, as well as business relationships with customers established in a high risk third country or relevant transactions where either of the parties is established in a high risk third country. 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/PF are higher, firms must conduct enhanced due diligence measures consistent with the risks identified.

Regulation 33(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

4.63 Annex 4-II contains a fuller list of illustrative risk factors a firm may address when considering the ML/TF/PF risk posed by customer situations.

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 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 https://www.fca.org.uk/about/enforcement.

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/PF 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 at https://www.fca.org.uk/about/enforcement.

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, terrorist financing and proliferation 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/proliferation financing risk assessment is not a one-time exercise. Firms must therefore ensure that their risk management processes for managing money laundering, terrorist financing and proliferation 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 ML/TF/PF 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, terrorist financiers and proliferation 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).