Chapter 3
Risk-Based Approach

Contents of this Chapter

3.1. Introduction

1. This Chapter is designed to assist the firm in taking a *risk*-based approach to the prevention of its products and services being used for the purposes of *ML* and *FT* and is broken down into three main sections:

   (a) Risk-Based Approach - which provides a high-level overview of the *risk*-based approach;
   (b) Business Risk Assessments - which details the relevant requirements of *Schedule 3*, together with the *Commission Rules* and *guidance*, in respect of the firm undertaking *ML* and *FT business risk assessments* and determining its *risk appetite*; and
   (c) Relationship Risk Assessments - which sets out the relevant obligations of *Schedule 3*, together with the *Commission Rules* and *guidance*, for the conducting of *risk* assessments of new and existing *business relationships* and *occasional transactions*.

Risk-Based Approach

3.2. Definition, Purpose and Benefits

2. A *risk*-based approach towards the prevention and detection of *ML* and *FT* aims to support the development of preventative and mitigating measures that are commensurate with the *ML* and *FT risks* identified by the firm and to deal with those *risks* in the most cost-effective and proportionate way.

3. Paragraph 2 of *Schedule 3* provides a general duty for the firm to understand, assess and mitigate *risks*. In this respect the firm shall:

   (a) understand its *ML* and *FT risks*; and
   (b) have in place effective policies, procedures and controls to:

      (i) identify,
      (ii) assess,
      (iii) mitigate,
      (iv) manage, and
      (v) review and monitor,

   those *risks* in a way that is consistent with the requirements of *Schedule 3*, *the Relevant Enactments*, the requirements of this *Handbook* and the *NRA*.

4. A *risk*-based approach prescribes the following procedural steps to manage the *ML* and *FT risks* faced by the firm:

   (a) identifying the specific threats posed to the firm by *ML* and *FT* and those areas of the firm's business with the greatest vulnerability;
   (b) assessing the likelihood of those threats occurring and the potential impact of them on the firm;
   (c) mitigating the likelihood of occurrence of identified threats and the potential for damage to be caused, primarily through the application of appropriate and effective policies, procedures and controls;
   (d) managing the residual *risks* arising from the threats and vulnerabilities that the firm has been unable to mitigate; and
   (e) reviewing and monitoring those *risks* to identify whether there have been any changes in the threats posed to the firm which necessitate changes to its policies, procedures and controls.

5. In applying a *risk*-based approach and taking the steps detailed above, it is crucial that, regardless of the specific considerations and actions of the firm, clear documentation is prepared and retained to ensure that the *board* and senior management can demonstrate their compliance with the requirements of *Schedule 3* and the *Commission Rules* in this *Handbook*.

6. A *risk*-based approach starts with the identification and assessment of the *risk* that has to be managed. In the context of *Schedule 3* and this *Handbook*, a *risk*-based approach requires the firm to assess the *risks* of how it might be involved in *ML* and *FT*, taking into account its *customers* (and the *beneficial owners* of *customers*), countries and geographic areas, the products, services and transactions it offers or undertakes, and the delivery channels by which it provides those products, services and/or transactions.

7. In determining how the *risk*-based approach should be implemented, the firm should analyse and seek to understand how the identified *ML* and *FT risks* affect its business. This determination should take into account a range of information, including (amongst others) the type and extent of the *risks* that the firm is willing to accept in order to achieve its strategic objectives (its "*risk appetite*"), its AML and CFT experience and *the Bailiwick's NRA*.

8. Through the *business risk assessments* and determination of a *risk appetite*, the firm can establish the basis for a *risk*-sensitive approach to managing and mitigating *ML* and *FT* risks. It should be noted, however, that a *risk*-based approach does not exempt the firm from the requirement to apply *enhanced measures* where it has identified higher *risk* factors as detailed in Chapter 8 of this *Handbook*.

9. *Schedule 3* and this *Handbook* do not prohibit the offering of any products or services or the acceptance of any *customer*, unless it is known, or there are reasonable grounds to suspect, that the *customer*, or the *beneficial owner* thereof, is undertaking or associated with *ML* or *FT*. The *risk*-based approach, as defined in *Schedule 3* and this *Handbook*, instead requires that the *risks* posed by *customers* (and the *beneficial owners* of *customers*), countries and geographic areas, products, services, transactions and delivery channels are identified, assessed, managed and mitigated and that evidence of such is documented and reviewed on an on-going basis.

10. By adopting a *risk*-based approach the firm should ensure that measures to prevent or mitigate *ML* and *FT* are commensurate with the *risks* identified. In this respect, the *business risk assessments* will also serve to enable the firm to make decisions on how to allocate its resources in the most efficient and effective way and to determine its appetite and tolerance for *risk*.

11. No system of checks will detect and prevent all *ML* and *FT*. A *risk*-based approach will, however, serve to balance the cost burden placed upon the firm and its *customers* with a realistic assessment of the threat of the firm being used in connection with *ML* and/or *FT*. It focuses the effort where it is needed and has most impact.

12. The benefits of a *risk*-based approach include:

    (a) recognising that the *ML* and *FT* threats to the firm vary across its *customers*, countries/geographic areas, products/services and delivery channels;
    (b) providing for the *board* to apply its own approach to the policies, procedures and controls of the firm in particular circumstances, enabling the *board* to differentiate between its *customers* in a way that matches the *risk* to its particular business;
    (c) helping to produce a more cost-effective system of *risk* management;
    (d) promoting the prioritisation of effort and activity by reference to the likelihood of *ML* and/or *FT* occurring;
    (e) reflecting experience and proportionality through the tailoring of effort and activity to *risk*;
    (f) enabling the application of the requirements of *Schedule 3* and this *Handbook* sensibly and in consideration of all relevant *risk* factors; and

(g) allowing for the consideration of the accumulation of identified *risks* and the determination of the level of overall *risk*, together with the appropriate level of mitigation to be applied.

13. It is important to acknowledge that various sectors and types of business, whether in terms of products/services, delivery channels or types of *customers*, can differ materially. An approach to preventing *ML* and *FT* that is appropriate in one sector may be inappropriate in another. Appendix D to this *Handbook* provides *guidance* on sector-specific *risk* factors to assist the firm in the development of its *risk* management framework.

3.3. Identification and Mitigation of Risks

14. *Risk* can be seen as a function of three factors and a *risk* assessment involves making judgements about all three of the following elements:

(a) threat – a person or group of persons, an object or an activity with the potential to cause harm;
(b) vulnerability – an opportunity that can be exploited by the threat or that may support or facilitate its activities; and
(c) consequence – the impact or harm that *ML* and *FT* may cause.

15. Having identified where it is vulnerable and the threats that it faces, the firm should take appropriate steps to mitigate the opportunity for those *risks* to materialise. This will involve determining the necessary controls or procedures that need to be in place in order to reduce the *risks* identified. The documented *risk* assessments that are required to be undertaken by *Schedule 3* will assist the firm in developing its *risk*-based approach.

16. In accordance with Paragraph 3(7) of *Schedule 3*, the firm shall have regard to:

(a) any relevant *Commission Rules* and *guidance* in this *Handbook*,
(b) any relevant notice or instruction issued by *the Commission* under *the Law*, and
(c) the *NRA*,

in determining what constitutes high or low *risk*, what its *risk appetite* is, and what constitute appropriate measures to manage and mitigate *risks*.

17. In addition to those noted above, information on *ML* and *FT risk* factors could come from a variety of other sources, whether these are accessed individually or through commercially available tools or databases that pool information from several sources. The sources could include:

(a) national and supranational *risk* assessments, such as those published by the EU, the UK and other countries or territories similar to *the Bailiwick*;
(b) information published by law enforcement agencies (for example, the *FIS*) such as threat reports, alerts and typologies;
(c) information published by *the Commission*, such as thematic reports, warnings and the reasoning set out in enforcement actions taken by it;
(d) information on the purpose and rationale of UK, UN and EU sanctions regimes;
~~(c)~~(e) guidance on *ML*, *FT* and preventing the proliferation of weapons of mass destruction published by the States of Guernsey Policy and Resources Committee;
~~(d)~~(f) information from international standard-setting bodies, including the FATF, such as guidance papers and reports on specific threats or *risks*, as well as mutual evaluation reports when considering the *risks* associated with a particular country or geographic area;
~~(e)~~(g) information provided by industry bodies, such as typologies and emerging *risks*;
~~(f)~~(h) information published by non-governmental organisations (for example, Global Witness or Transparency International); and

~~(g)~~(i) information published by credible and reliable commercial sources, (for example, *risk* and intelligence reports) or open sources (for example, reputable newspapers).

18. Retaining *documentation* on the results of the firm's *risk* assessment framework will assist the firm to demonstrate how it:

(a) identifies and assesses the *risks* of being used for *ML* and *FT*;
(b) agrees and implements appropriate and effective policies, procedures and controls to manage and mitigate *ML* and *FT risk*;
(c) monitors and improves the effectiveness of its policies, procedures and controls; and
(d) ensures accountability of the *board* in respect of the operation of its policies, procedures and controls.

3.4. Accumulation of Risk

19. In addition to the individual consideration of each *risk* factor, the firm must also consider all such factors holistically to establish whether their concurrent or cumulative effect might increase or decrease the firm's overall *risk* exposure and the dynamic that this could have on the controls implemented by the firm to mitigate *risk*.

20. Such an approach is relevant not only to the firm in its consideration of the *risks* posed to its business as a whole as part of undertaking its *business risk assessments*, but also in the consideration of the *risk* that individual *business relationships* or *occasional transactions* pose.

21. There are also other operational factors which may increase the overall level of *risk*. These factors should be considered in conjunction with the firm's *ML* and *FT risks*. Examples of such factors could be the outsourcing of AML and CFT controls or other regulatory requirements to an external third party or another member of the same group as the firm; or the use of on-line or web-based services and cyber-crime risks which may be associated with those service offerings.

3.4.1. Weighting Risk Factors

22. In considering the *risk* of a *business relationship* or *occasional transaction* holistically, the firm may decide to weigh *risk* factors differently depending on their relative importance.

23. When weighing *risk* factors, the firm should make an informed judgement about the relevance of different *risk* factors in the context of a *business relationship* or *occasional transaction*. This will likely result in the firm allocating varying 'scores' to different factors; for example, the firm may decide that a *customer's* personal links to a country, territory or geographic area associated with higher *ML* and/or *FT risk* is less relevant in light of the features of the product they seek.

24. Ultimately, the weight given to each *risk* factor is likely to vary from product to product and *customer* to *customer* (or category of *customer*). When weighting *risk* factors, the firm should ensure that:

(a) the *risk* rating is not unduly influenced by just one *risk* factor;
(b) economic or profit considerations do not influence the *risk* rating;
(c) the weight assigned does not lead to a situation where it is impossible for any *business relationship* or *occasional transaction* to be classified as a *high risk relationship*;
(d) the provisions of Paragraph 5(1) of *Schedule 3* setting out the situations which will always present a high *risk* (for example, the involvement of *foreign PEPs* or *correspondent banking relationships*) cannot be over-ruled; and

(e) it is able to override any automatically generated *risk* scores where necessary. The rationale for the decision to override such scores should be documented appropriately.

25. Where the firm uses automated IT systems to allocate overall *risk* scores to *business relationships* or *occasional transactions* and does not develop these in house but purchases them from an external provider, it should understand how the system works and how it combines *risk* factors to achieve an overall *risk* score. The firm should be able to satisfy itself that the scores allocated reflect the firm's understanding of *ML* and *FT risk* and it should be able to demonstrate this.

3.5. Policies, Procedures and Controls

26. In accordance with Paragraph 3(6) of *Schedule 3*, the firm shall –

(a) have in place policies, procedures and controls approved by its *board* that are appropriate and effective, having regard to the assessed *risk*, to enable it to mitigate and manage:

(i) *risks* identified in the *business risk assessments*, and *relationship risk assessments* undertaken under Paragraph 3(4)(a) of *Schedule 3*; and
(ii) *risks* relevant, or potentially relevant, to the firm identified in the *NRA* (which *risks* shall be incorporated into the *business risk assessments*);

(b) regularly review and monitor the implementation of those policies, controls and procedures and enhance them if such enhancement is necessary or desirable for the mitigation and management of those *risks;* and
(c) take additional measures to manage and mitigate higher *risks* identified in the *business risk assessments* and in *relationship risk assessments* undertaken under Paragraph 3(4)(a) of *Schedule 3*.

27. The firm's policies, procedures and controls must take into account the nature and complexity of the firm's operation, together with the *risks* identified in its *business risk assessments*, and must be sufficiently detailed to allow the firm to demonstrate how the conclusion of each *relationship risk assessment* has been reached.

Business Risk Assessments

3.6. Introduction

28. A key component of a *risk*-based approach involves the firm identifying areas where its products and services could be exposed to the *risks* of *ML* and *FT* and taking appropriate steps to ensure that any identified *risks* are managed and mitigated through the establishment of appropriate and effective policies, procedures and controls.

29. The *business risk assessments* are designed to assist the firm in making such an assessment and provide a method by which the firm can identify the extent to which its business and its products and services are exposed to *ML* and *FT*. Good quality *business risk assessments* are therefore vital for ensuring that the firm's policies, procedures and controls are proportionate and targeted appropriately.

30. The *board* must ensure that the firm's *business risk assessments*, together with details of the firm's *risk appetite*, are communicated to all *relevant employees*.

31. In communicating the firm's *business risk assessments* and *risk appetite*, the firm should ensure that *relevant employees* understand the implications of these on the day-to-day functions of

relevant employees and their effect on the strategic objectives of the firm, in particular those *relevant employees* with *customer*-facing or business development roles.

3.7. Content and Structure

32. In accordance with Paragraph 3(1)(a) of *Schedule 3*, the firm shall carry out and *document* a suitable and sufficient *ML business risk assessment*, and a suitable and sufficient *FT business risk assessment*, which are specific to the firm.

33. In carrying out the *business risk assessments* in accordance with Paragraph 3(1) of *Schedule 3*, the firm must ensure that the assessments of the *risks* of *ML* and *FT* are distinct from one another, clearly addressing the different threats posed by each *risk* and should reflect that appropriate steps have been taken in order to identify and assess the specific *risks* posed to the firm.

34. The format of the *business risk assessments* is a matter to be decided by the firm. However, regardless of the format used, it is important that the *business risk assessments* are *documented* in accordance with Paragraph 3(1)(a) of *Schedule 3* in order to provide clear evidence to demonstrate the basis upon which they have been conducted. Notwithstanding the requirement for the *ML* and *FT business risk assessments* to be distinct, there is nothing to prevent them being contained within one over-arching *document* recording, in its entirety, the firm's assessment of *ML* and *FT risk*.

35. In accordance with Paragraph 3(3) of *Schedule 3*, the *business risk assessments* shall be appropriate to the nature, size and complexity of the firm, and be in respect of:

(a) *customers*, and the *beneficial owners* of *customers*,
(b) countries and geographic areas, and
(c) products, services, transactions and delivery channels (as appropriate), and in particular in respect of the *ML* or *FT risks* that may arise in relation to:

(i) the development of new products and new business practices, before such products are made available and such practices adopted; and
(ii) the use of new or developing technologies for both new and pre-existing products, before such technologies are used and adopted.

36. The *business risk assessments* must also take account of the findings of the *NRA* and reflect the firm's assessment of whether the *risks* identified in the *NRA* are relevant, or potentially relevant, to the firm, and where they are, identify the measures for mitigating those *risks*.

37. The firm should have regard to the *ML* and *FT* threats relevant to its sector as articulated in the *NRA*, assess how those threats are relevant to the products and services it offers, and assess its vulnerability to *ML* and *FT* after taking into account mitigating measures. The sections of the *NRA* which discuss the modalities of *ML* and *FT*, and the case studies contained within, are particularly relevant. Despite there being no *FT* case studies in the *NRA* some of the countries and patterns of behaviour involved in the *ML* case studies will be relevant to possible *FT* activity, especially in relation to secondary *FT* i.e. where the proceeds of crime are used to fund terrorism. Additionally the firm should have regard to *FT* typologies issued by the FATF:

FATF FT Guidance

~~37.~~38. In accordance with Paragraph 3(2) of *Schedule 3*, in carrying out its *business risk assessments*, the firm shall consider all relevant *risk* factors before determining:

(a) the level of overall *risk* to the firm;
(b) the firm's *risk appetite*; and
(c) the appropriate level and type of mitigation to be applied.

~~38.~~39. ~~In addition to identifying any particular areas of vulnerability to the *risks* of *ML* and *FT*, t~~The *business risk assessments* should contain references as to how the firm manages or mitigates the *risks* which it has identified and the policies, procedures and controls which have been established in this regard.

~~39.~~40. Industry sectors will have inherent and/or generic *risk* factors and these should be referenced in the firm's *business risk assessments*. *Business risk assessments* are likely to be deficient if the risks to the firm's sector identified in the *NRA* are not considered or if the irrelevance of those risks to its business is not explained in the assessments. Additionally, the firm will also have *risk* factors particular to its own business which should be analysed in the *business risk assessments*.

~~40.~~41. The firm must not copy the *business risk assessments* prepared by another business, or use 'off-the-shelf' assessments which pre-identify suggested *ML* and *FT risks* without the firm ensuring the assessments have been tailored to its business and the specific *risks* that it faces.

~~41.~~42. Such an approach in adopting an 'off-the-shelf' assessment can lead to the firm failing to accurately identify the *ML* and *FT risks* specific to its business. This in turn can lead to inadequate or inappropriate policies, procedures and controls that are either ill-suited to the firm or fail to appropriately mitigate the firm's *risks*.

~~42.~~43. In addition to the above, the *business risk assessments* should not:

(a) be a 'cut and paste' version of the relevant sections of the *Handbook* and/or the *NRA*. This does not demonstrate that the *board* has given serious consideration to the vulnerabilities specific to the products, services and *customers* of the firm;
(b) be generic assessments which have simply been populated with general information. Again, this does not demonstrate that the *board* has given serious consideration to the vulnerabilities particular to its business;
(c) contain unsubstantiated, highly generalised references to the *risks* faced by the firm, for example, a reference to all business being low *risk* or statements such as 'there is a risk that our products could be used to finance terrorism'. Such statements would not be acceptable unless they are backed-up with specific information evidencing how this assessment had been made; or
~~(c)~~(d) copy statements about a sector's risks from the *NRA* without substantiating why those risks are relevant to the firm; or
~~(d)~~(e) focus upon isolated *risk* factors, for example, concentrating solely upon a geographic location.

~~43.~~44. There may be occasions where threats span a number of *risk* categories, for example, there may be operational risks associated with a piece of *customer*-facing technology in addition to *ML* and *FT* or other financial crime risks. Where the firm wishes to combine its *ML* and *FT business risk assessments* with assessments of other risks, such as conduct risk or credit risk, the firm should ensure that the assessments of *ML* and *FT risk* are clearly identified.

3.8. Risk Appetite

~~44.~~45. In accordance with Paragraph 3(2) of *Schedule 3* the firm shall, having considered all relevant *risk* factors, determine its *risk appetite* as part of carrying out its *business risk assessments*.

~~45.~~46. The determination of the firm's *risk appetite* is an important element in carrying out its *business risk assessments*, setting out the amount of *ML* and *FT risk* it is prepared to accept in pursuing its strategic objectives. Having identified the inherent *ML* and *FT risks* to its business, identifying the amount of such *risk* that it is willing to take on is an integral part of the design and implementation of appropriate and effective policies, procedures and controls to manage and mitigate *risk*.

~~46.~~47. The *board* is responsible for setting the firm's *risk appetite*, together with the overall attitude of the firm to *risk* taking. The primary goal of the *risk appetite* is to define the amount of *risk* that the firm is willing to accept in the pursuit of its objectives, as well as outlining the boundaries of its *risk* taking, beyond which the firm is not prepared to accept *risk*.

~~47.~~48. In this respect the firm's documented *risk appetite* should include a qualitative statement (for example, detailing those categories of *customer* or country/territory that the firm deems to pose too great a *risk*) as well as quantitative measures to support its *risk appetite*, including the firm's tolerance and capacity to take on *risk*, i.e. the maximum level of *risk* that it is possible to accept without exceeding or overstretching its administrative, operational and resourcing constraints.

~~48.~~49. In determining its *risk appetite* the firm should be realistic in the context of its business model. A firm targeting business from high *risk* countries or territories, offering high *risk* products or services or with a large percentage of *high risk relationships* would consequently have a high *risk appetite* and its *business risk assessments* should be drafted accordingly.

~~49.~~50. The following is a non-exhaustive list of example questions that the firm could consider in developing its *risk appetite*:

(a) What are the strategic objectives of the firm? Are they clear?
(b) What specific *risks* could pursuing these objectives expose the firm to?
~~(b)~~(c) How relevant to the firm's objectives are the main risks identified in the *NRA* to the firm's sector?
~~(c)~~(d) What are the significant *risks* the *board* is willing to take?
~~(d)~~(e) What are the significant *risks* the *board* is not willing to take?
~~(e)~~(f) Is the *board* clear about the nature and extent of the significant *risks* it is willing to take in achieving its strategic objectives?
~~(f)~~(g) Have the *board* and senior management reviewed the capabilities of the firm to manage the *risks* that it faces?
~~(g)~~(h) What capacity does the firm have in terms of its ability to manage *risks*?
~~(h)~~(i) Do *employees* of the firm understand their role and responsibility for managing *risk*?
~~(i)~~(j) How much does the firm spend on compliance and *risk* management each year? How much does the firm need to spend to ensure its compliance and *risk* management controls can sufficiently mitigate the identified *risks*?

3.9. Review

~~50.~~51. In accordance with Paragraph 3(1)(b) of *Schedule 3*, the firm shall regularly review its *business risk assessments*, at a minimum annually and more frequently when changes to the business of the firm occur, so as to keep them up to date.

~~51.~~52. The *NRA* process is an iterative one, which will involve the exercise being repeated over time, therefore the firm must take into account the findings of any updated *NRA* and reflect the firm's assessment of whether the *risks* identified in any updated *NRA* are relevant, or potentially relevant, to the firm, and where they are, identify the measures for mitigating those *risks*.

~~52.~~53. Just as the activities of the firm can change, so too can the corresponding *ML* and *FT risks*. Mergers, acquisitions, the purchase or sale of a book of business, the adoption of a piece of technology or technological solution, the introduction of a new product or service, a restructuring or a change of external service provider are just some of the events which can affect both the type and extent of the *risks* to which the firm could be exposed. In light of any such changes the *business risk assessments* should be reviewed to consider whether the *risks* to the firm have changed and to ensure that the controls to mitigate those *risks* remain effective.

~~53.~~54. Other operational changes, for example, a change in *employee* numbers or a change to group policies, can all have an impact upon the resources required to effectively manage *ML* and *FT risks*.

~~54.~~55. Where, as a result of the firm's review, changes to the *business risk assessments* are required, in accordance with Paragraph 3(1)(b) of *Schedule 3* the firm shall make those changes.

~~55.~~56. Where changes to the *business risk assessments* are made, the firm must give consideration to whether the policies, procedures and controls of the firm remain appropriate and effective in light of the revised *business risk assessments* and make any changes it considers appropriate in a timely manner.

3.10. Example Risk Factors

~~56.~~57. Below are example *risk* factors that may be considered by the firm as part of the assessment of its *ML* and *FT risks*. The examples given are not intended to be exhaustive or to be used by the firm as checklists of *risks*.

~~57.~~58. *Customer risk*:

(a) The countries, territories and geographic areas with which *customers* (and the *beneficial owners* of *customers*) have a *relevant connection*;
(b) The complexity of *customer* and beneficial ownership structures;
(c) The complexity of *legal persons* and *legal arrangements*;
(d) The use of introduced business arrangements;
(e) The use or acceptance of *intermediary relationships*;
(f) The number of *business relationships* assessed as high *risk*;
(g) The countries and geographic areas targeted by the firm and from which the firm will accept new *customers* (including the *beneficial owners* of *customers*);
(h) The number of *customers* and *beneficial owners* assessed as *PEPs* and their associated countries or territories; and
(i) The number of *customers* and *beneficial owners* which are charities or non-profit organisations ("NPOs") and their associated countries or geographic areas.

~~58.~~59. Product/service *risk*:

(a) The nature, scale, diversity and complexity of the products and services of the firm;
(b) The target markets, both in terms of geography and class of *customer*;
(c) The distribution channels utilised by the firm;
(d) Whether the value of transactions is expected to be particularly high;
(e) The nature, scale and countries/geographic areas associated with *funds* sent and received on behalf of *customers*;
(f) Whether payments to any unknown or un-associated third parties are allowed; and
(g) Whether the products/services/structure are of particular, or unusual, complexity.

~~59.~~60. Other potential sources of *risk* to consider:

(a) Internal and/or external audit findings; and
(b) Typologies and findings of *ML* and *FT* case studies.

3.11. New Products and Business Practices

~~60.~~61. In accordance with Paragraph 3(3)(c)(i) of *Schedule 3*, the firm shall, before making available or adopting new products or business practices, ensure that its *business risk assessments* have identified and assessed the *ML* and *FT risks* arising from those products or practices.

~~61.~~62. References to new products should be read as referring to products which the firm has not previously offered and which present new or differing *ML* or *FT risks* to the firm.

~~62.~~63. References to new business practices relate to new ways in which the firm's products or services are offered or delivered. For example, a new business practice could include the development of a *customer*-facing portal or other software where *customers* can interact with the firm.

~~63.~~64. If the firm decides to proceed with the offering or adoption of a new product or business practice, the *board* of the firm must approve the *risk* assessment undertaken in accordance with Paragraph 3(3)(c)(i) of *Schedule 3* and that approval must be documented.

3.12. New Technologies

~~64.~~65. In accordance with Paragraph 3(3)(c)(ii) of *Schedule 3*, the firm shall, before adopting and using a new or developing technology for a new or pre-existing product, ensure that its *business risk assessments* have identified and assessed the *risks* arising from the technology's use or adoption.

~~65.~~66. These technologies are likely to fall within the Financial Technology ("FinTech") arena, which includes technology aimed at disrupting the delivery or transaction channels of traditional products and services, as well as the creation of new products or services utilising enhancements in technology. Examples of such technologies include the use of distributed ledger technology in the delivery of traditional securities through to the trading or safekeeping of virtual assets.

~~66.~~67. The *risk* assessment of a new or developing technology must include, as a minimum, an assessment of the *ML* and *FT risks* and vulnerabilities inherent in the use or adoption of the technology in order that appropriate controls can be implemented. This includes evaluating the technology itself, together with the anticipated use of the technology and the threats posed by this use.

~~67.~~68. It is not essential that the *risk* assessment of a technology extends to a highly technical, comprehensive report on the specifications and functionality. The objective of the *risk* assessment is to evaluate the *ML* and *FT risk*s and vulnerabilities inherent in the use of the technology and to identify the controls necessary to mitigate and limit the firm's exposure.

~~68.~~69. If the firm decides to proceed with the adoption or use of a new or developing technology for a new or pre-existing product, the *board* of the firm must approve the *risk* assessment undertaken in accordance with Paragraph 3(3)(c)(ii) of *Schedule 3* and that approval must be documented.

~~69.~~70. Following the initial *risk* assessment of a new or developing technology, the firm should periodically review its assessment in conjunction with its responsibility for the review of its wider *ML* and *FT business risk assessments* as described in Section 3.9. of this *Handbook*.

Relationship Risk Assessment

3.13. Introduction

~~70.~~71. The purpose of this Section is to set out the *Commission Rules* and *guidance* surrounding the assessment of *risk* in a *business relationship* or *occasional transaction* ("*relationship risk assessment*") at the point of take-on, as well as the ongoing requirement to ensure that any *relationship risk assessment* remains appropriate and relevant as the relationship evolves.

~~71.~~72. The firm's *business risk assessments* and its defined *risk appetite* will assist in determining the take-on of any new business. The *relationship risk assessment* is the assessment of a new or existing *business relationship* or *occasional transaction* against the parameters determined within the *risk appetite* and the *ML* and *FT risks* identified in the *business risk assessments*.

~~72.~~73. There may be circumstances where the *risks* of *ML* and *FT* are high and *ECDD* measures are to be applied. Similarly, there may be circumstances within which the firm can apply *SCDD* measures because it has assessed the *risk* of the *business relationship* or *occasional transaction* as being low. Further information on the *relationship risk assessment* process, including examples of high and low *risk* factors, can be found in this Section.

3.14. Management and Mitigation

~~73.~~74. In order to consider the extent of its potential exposure to the *risks* of *ML* and *FT*, in accordance with Paragraph 3(4) of *Schedule 3* the firm shall -

(a) prior to the establishment of a *business relationship* or the carrying out of an *occasional transaction*, undertake a *relationship risk assessment*, and
(b) regularly review any *relationship risk assessment* carried out under (a) so as to keep it up to date and, where changes to that *relationship risk assessment* are required, it shall make those changes.

~~74.~~75. Based on the outcome of its *relationship risk assessment*, the firm must decide whether or not to accept (or continue) each *business relationship* or whether or not to accept any instructions to carry out an *occasional transaction*.

~~75.~~76. When undertaking or reviewing a *relationship risk assessment*, in accordance with Paragraph 3(5)(a) of *Schedule 3* the firm shall take into account its *risk appetite* and *risk* factors relating to:

(a) the type or types of *customer* (and the *beneficial owners* of the *customer*);
(b) the country or geographic area; and
(c) the product, service, transaction and delivery channel that are relevant to the *business relationship* or *occasional transaction*.

77. The *FATF* has identified a number of countries and territories with significant strategic deficiencies in their regimes to counter *ML*, *FT* and financing of proliferation for which it has called for the application of countermeasures. Appendix H to this *Handbook* identifies those countries and territories in relation to which the *FATF* has called for the application of countermeasures. Appendix I to this *Handbook* lists a number of countries and territories that are identified by reliable and independent external sources as presenting a higher risk, this includes those subject to a "call for action" those "under increased monitoring" by the FATF. These sources highlight specific risks associated with the country or territory to help firms devise relevant mitigating measures.

78.	For the purposes of Paragraph 3(5)(a) of *Schedule 3*, when considering country or geographical area risk factors, the firm must take into account the information set out in Appendix H and I to this *Handbook* when undertaking or reviewing a *relationship risk assessment*.

79.	In addition to the *risk* factors set out above, the firm must also give consideration to the following when undertaking or reviewing a *relationship risk assessment*: (a) where the product or service provided by the firm is a life insurance policy, the type or types of beneficiary of that policy; (b) the purpose and intended nature of the *business relationship* or *occasional transaction*, including the possibility of *legal persons* and *legal arrangements* forming part of the relationship; (c) the type, volume, value and regularity of activity expected; and (d) the expected duration (if a *business relationship*).

80. For the purposes of Paragraph 3(5)(a) of *Schedule 3* and *Commission Rule* 3.79~~5~~.(a) above, the firm's consideration of the type or types of the *customer, beneficial owner* or beneficiary should incorporate whether they are a natural person, *legal person* or *legal arrangement*, as well as their identity and background.

81.	In accordance with Paragraph 3(5)(b) of *Schedule 3*, when undertaking or reviewing a *relationship risk assessment*, the firm shall understand that the *risk* factors noted in Paragraph 3(5)(a) of *Schedule 3* as set out above and any other *risk* factors, either singly or in combination, may increase or decrease the potential *risk* posed by the *business relationship* or *occasional transaction*.

82.	In light of the above, when undertaking a *relationship risk assessment* the firm must ensure that all relevant *risk* factors are considered, both singly and in combination, before making a determination as to the level of overall assessed *risk*.

83. Consideration of the purpose and intended nature of a *business relationship* or *occasional transaction* in accordance with *Commission Rule* 3.7~~5~~9.(b) should include an assessment of the economic or other commercial rationale for the *business relationship* or *occasional transaction*.

84.	The firm's procedures may provide for standardised profiles to be used for *relationship risk assessments* where the firm has *satisfied* itself, on reasonable grounds, that such an approach effectively manages the *risk* for each particular *business relationship* or *occasional transaction*. However, where the firm has a diverse *customer* base, or where a wide range of products and services are offered, it must develop a more structured and rigorous system to show that judgement has been exercised on an individual basis rather than on a generic or categorised basis.

85.	Whatever method is used to assess the *risk* of a *business relationship* or *occasional transaction*, the firm must maintain clear documented evidence as to the basis on which the *relationship risk assessment* has been made.

86.	Where, despite there being high *risk* factors identified, the firm does not assess the overall *risk* as high because of strong and compelling mitigating factors, the firm must identify the mitigating factors and, along with the reasons for the decision, *document* them and retain them on the relevant *business relationship* or *occasional transaction* file.

87.	Based upon the results of the *relationship risk assessment*, the firm must determine, on the basis of *risk*:

(a) the extent of the identification information to be obtained on the *key principals* to the *business relationship* or *occasional transaction* in accordance with Paragraphs 4 and 5 of *Schedule 3* and Chapters 4 to 8 of this *Handbook*;

(b) how and to what extent that information will be verified using *identification data*;

(c) whether to apply *SCDD* measures where the *business relationship* or *occasional transaction* has been assessed as being low *risk* and displays one or more of the characteristics in Chapter 9 of this *Handbook*; and

(d) the extent to which the resulting *business relationship* will be monitored on an ongoing basis.

3.15. ~~Business from Sensitive Sources~~ Notices, Instructions or Warnings~~, etc.~~

88. From time to time *the Commission* issues ~~Business from Sensitive Sources Notices, Advisory~~ Notices, Instructions and Warnings which highlight potential *risks*. ~~, including those arising from particular countries, territories and geographic areas.~~ Th~~e~~is information ~~contained within these notices~~, together with sanctions legislation applicable in *the Bailiwick*, must be considered when undertaking or reviewing a *relationship risk assessment*.

89. Further information on *the Bailiwick's* sanctions regime and legislation can be found in Chapter 12 of this *Handbook*.

3.16. Mandatory High Risk Factors

90. In accordance with Paragraph 5(1) of *Schedule 3*, where the firm is required to carry out *CDD* measures, it must also carry out *ECDD* measures in relation to high *risk business relationships* and *occasional transactions*, including, without limitation -

(a) a *business relationship* or *occasional transaction* in which the *customer* or any *beneficial owner* is a *foreign PEP*;

(b) where the firm is an *FSB*, a *business relationship* which is –

(i) a *correspondent banking relationship*, or

(ii) similar to such a relationship in that it involves the provision of services, which themselves amount to financial services business or facilitate the carrying on of such business, by one *FSB* to another;

(c) a *business relationship* or an *occasional transaction* –

(i) where the *customer* or *beneficial owner* has a *relevant connection* with a country or territory that -

(A) provides funding or support for terrorist activities, or does not apply (or insufficiently applies) *the FATF Recommendations*, or

(B) is a country otherwise identified by the FATF as a country for which such measures are appropriate,

(ii) which the firm considers to be a *high risk relationship*, taking into account any notices, instructions or warnings issued from time to time by *the Commission* and having regard to the *NRA*,

(d) a *business relationship* or an *occasional transaction* which has been assessed as a *high risk relationship*, and

(e) a *business relationship* or an *occasional transaction* in which the *customer*, the *beneficial owner* of the *customer*, or any other *legal person* in the ownership or control structure of the *customer*, is a *legal person* that has *bearer shares* or *bearer warrants*.

91. Chapter 8 of this *Handbook* sets out the requirements of *Schedule 3* and the *Commission Rules* in relation to *high risk relationships* and includes details of sources which may assist in the assessment of *risk*.

~~91.~~92. The firm is required to have regard to the *NRA* in determining what constitutes a high or low risk, what its *risk appetite* is, and what constitutes appropriate measures to manage and mitigate *risks*. The sections of the *NRA* report which discuss the modalities of *ML* and *FT*, and the case studies contained within, are particularly relevant to how the firm manages and mitigates customer, product, service, transaction and delivery channel *risk* factors.

3.17. Risk Factors

~~92.~~93. The *risk* factors included within the following sections are purely for guidance and are provided as examples of factors that the firm might consider when undertaking a *relationship risk assessment*. The following factors are not exhaustive and are not prescribed as a checklist. It is for the firm to assess and decide what is appropriate in the circumstances of the *business relationship* or *occasional transaction* and it is not expected that all factors will be considered in all cases.

~~93.~~94. The example indicators do not remove the ability of the firm to apply a *risk*-based approach. In this respect the firm should take a holistic view of the *risk* associated with each *business relationship* or *occasional transaction* as set out in Section 3.4. of this Chapter. The presence of isolated *risk* factors does not necessarily move a *business relationship* or *occasional transaction* into a higher or lower *risk* category; however, in accordance with Section 3.4.1. above, certain *risk* factors could have a bigger contribution to the overall *risk* assessment than others.

~~94.~~95. If it is determined, through a *relationship risk assessment*, that there are types of *customer*, activity, business or profession that are at *risk* of abuse from *ML* and/or *FT*, then the firm should apply higher AML and CFT requirements as dictated by the relevant *risk* factor(s).

3.17.1. Customer Risk Factors

~~95.~~96. When identifying the *risk* associated with its *customers*, including the *beneficial owners* of *customers*, the firm should consider the *risk* related to:

(a) the *customer's* (and *beneficial owner's)* business or professional activity;
(b) the *customer's* (and *beneficial owner's*) reputation; and
(c) the *customer's* (and *beneficial owner's*) nature and behaviour.

~~96.~~97. *Risk* factors that may be relevant when considering the *risk* associated with a *customer's* or *beneficial owner's* business or professional activity include:

(a) Does the *customer* or *beneficial owner* have links to sectors that are commonly associated with higher corruption risk, such as construction, pharmaceuticals and healthcare, the arms trade and defence, the extractive industries or public procurement?
(b) Does the *customer* or *beneficial owner* have links to sectors that are associated with higher *ML* and/or *FT risk*, for example, certain money service providers ("MSPs"), casinos or dealers in precious metals?

(c) Does the *customer* or *beneficial owner* have links to sectors that involve significant amounts of cash?

(d) Where the *customer* is a *legal person* or *legal arrangement*, what is the purpose of their establishment? For example, what is the nature of their business?

(e) Does the *customer* have political connections, for example, are they a *PEP*, or is the *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 line with Paragraph 5(1) of *Schedule 3*, where a *customer* or the *beneficial owner* is a *foreign PEP* the firm shall apply *ECDD* measures.

(f) Does the *customer* or *beneficial owner* hold another prominent position or enjoy a high public profile that might enable them to abuse this position for private gain? For example, are they senior local or regional public officials with the ability to influence the awarding of public contracts, decision-making members of high-profile sporting bodies or individuals who are known to influence the government and other senior decision-makers?

(g) Is the *customer* a *legal person* subject to enforceable disclosure requirements that ensure 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?

(h) Is the *customer* an *FSB* acting on its own *account* from a country or territory listed in Appendix C to this *Handbook*? Is there evidence that the *customer* has been subject to supervisory sanctions or enforcement for failure to comply with AML and CFT obligations or wider conduct requirements in recent years?

(i) Is the *customer* a public administration or enterprise from a country or territory with low levels of corruption?

(j) Is the *customer's* or the *beneficial owner's* background consistent with what the firm knows about their former, current or planned business activity, their business's turnover, the source of funds and the *customer's* or *beneficial owner's* source of wealth?

~~(j)~~(k) Is the *customer* a money remitter in a higher risk jurisdiction for terrorism or terrorist financing whose activities could be abused for *FT* purposes?

(l) Is the customer a Non-Profit Organisation ("NPO") whose activities could be abused for *FT* purposes, in particular those NPOs operating directly or indirectly in higher *risk* jurisdictions for terrorism?

~~97.~~98. The following *risk* factors may be relevant when considering the *risk* associated with a *customer's* or *beneficial owner's* reputation:

(a) Are there adverse media reports or other relevant sources of information about the *customer*, for example, are there any allegations of criminality or terrorism against the *customer* or the *beneficial owner*? If so, are these reliable and credible? The firm should determine the credibility of allegations on the basis of the quality and independence of the source of the data and the persistence of reporting of these allegations, among other considerations. The firm should note that the absence of criminal convictions alone may not be sufficient to dismiss allegations of wrongdoing.

(b) Has 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 *FT*? Does the firm have reasonable grounds to suspect that the *customer* or *beneficial owner* or anyone publicly known to be closely associated with them has, at some point in the past, been subject to such an asset freeze?

~~(b)~~(c) Are there adverse reports or other relevant sources indicating that the *customer*, or *beneficial owner* or anyone publicly known to be closely associated with them support or promote violent extremism or terrorism?

~~(c)~~(d) Does the firm know if the *customer* or *beneficial owner* has been the subject of an internal or external disclosure in the past?

~~(d)~~(e) Does the firm have any in-house information about the *customer's* or the *beneficial owner's* integrity, obtained, for example, in the course of a long-standing *business relationship*?

~~98.~~99. The following *risk* factors may be relevant when considering the *risk* associated with a *customer's* or *beneficial owner's* nature and behaviour The firm should note that not all of these *risk* factors will be apparent at the outset, they may emerge only once a *business relationship* has been established:

(a) Does the *customer* have legitimate reasons for being unable to provide robust evidence of their identity, for example, because they are an asylum seeker?

(b) Does the firm have any doubts about the veracity or accuracy of the *customer's* or *beneficial owner's* identity?

(c) 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 transaction or several one-off transactions where the establishment of a *business relationship* might make more economic sense?

(d) 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?

(e) Does the *customer* issue *bearer shares* or does it have *nominee shareholders*?

(f) Is the *customer* a *legal person* or *legal arrangement* that could be used as a personal asset holding vehicle?

(g) Is there a sound reason for changes in the *customer's* ownership and control structure?

(h) Does the *customer* request transactions that are complex, unusual or unexpectedly large or have an unusual or unexpected pattern without an apparent economic or lawful purpose or a sound commercial rationale? Are there grounds to suspect that the *customer* is trying to evade specific thresholds, such as those subject to mandatory reporting, either in *the Bailiwick* or the *customer's* home country or territory?

(i) Does the *customer* request unnecessary or unreasonable levels of secrecy? For example, is the *customer* reluctant to share *identification data*, or do they appear to want to disguise the true nature of their business?

(j) Can the *customer's* or *beneficial owner's* source of *funds* or source of wealth be easily established, for example, through their occupation, inheritance or investments?

(k) Does the *customer* use the products and services they have taken out as expected when the *business relationship* was first established?

~~(k)~~(l) Has the customer made unexpected financial donations to NPOs whose activities could be abused for *FT* purposes?

3.17.2. Countries and Territories Risk Factors

~~99.~~100. When identifying the *risk* associated with countries and territories, the firm should consider the *risk* related to those countries and territories with which the *customer* or *beneficial owner* has a *relevant connection*.

~~100.~~101. The firm should note that the nature and purpose of the *business relationship* will often determine the relative importance of individual country and geographical *risk* factors. For example:

(a) Where the *funds* used in the *business relationship* or *occasional transaction* have been generated abroad, the level of predicate offences to *ML* and the effectiveness of a country's or territory's legal system will be particularly relevant.

(b) Where *funds* are received from, or sent to, countries or territories where groups committing terrorist offences are known to be operating, the firm should consider to what extent this could be expected to, or might give rise to, suspicion based on what the firm knows about the purpose and nature of the *business relationship* or *occasional transaction*.

(c) Where the *customer* is an *FSB*, the firm should pay particular attention to the adequacy of the country's or territory's AML and CFT regime and the effectiveness of AML and CFT supervision.

(d) Where the *customer* or *beneficial owner* is a *legal person* or *legal arrangement*, the firm should take into account the extent to which the country or territory in which the *customer* or *beneficial owner* is registered effectively complies with international tax transparency standards.

~~101.~~102. *Risk* factors the firm should consider when identifying the effectiveness of a country's or territory's AML and CFT regime include:

(a) Has the country or territory been identified by a mutual evaluation as having strategic deficiencies in its AML and CFT regime? In accordance with Paragraph 5(1)(c)(i) of *Schedule 3*, *ECDD* measures shall be applied where the *customer* or *beneficial owner* has a *relevant connection* to a country or territory that does not apply (or insufficiently applies) *the FATF Recommendations*. Further information can be found in Section 3.15. of this Chapter.

(b) Is there information from more than one credible and reliable source about the quality of the country's or territory's AML and CFT controls, including information about the quality and effectiveness of regulatory enforcement and oversight? Examples of possible sources include mutual evaluation reports by the FATF or FATF-style regional bodies (in particular Recommendations 10, 26 and 27 and Immediate Outcomes 3 and 4), the FATF's list of high-risk and non-cooperative jurisdictions, International Monetary Fund ("IMF") assessments and Financial Sector Assessment Programme reports. The firm should note that membership of the FATF or a FATF-style regional body (for example, MONEYVAL) does not, of itself, mean that the country's or territory's AML and CFT regime is adequate and effective.

~~102.~~103. *Risk* factors the firm should consider when identifying the level of *FT risk* associated with a country or territory include:

(a) Is there information (for example, from law enforcement or credible and reliable open media sources) suggesting that a country or territory provides funding or support for terrorist activities from official sources or from organised groups or organisations within that country or territory?

~~(a)~~(b) Is there information (for example, from law enforcement or credible and reliable open media sources) suggesting that groups committing terrorist offences are known to be operating in the country or territory?

(c) Is the country or territory subject to financial sanctions, embargoes or measures that are related to terrorism, financing of terrorism or proliferation issued by, for example, the UN or the EU?

(d) Are there communities within the country or territory that may be actively targeted by terrorist organisations for support or cover or who may be sympathetic to terrorist actors because of diaspora links or other connections?

(e) Is the country or territory rich in natural/environmental resources and is known to have active terrorist organisations operating within it.

(f) Is the country or territory a regional or international financial centre in close proximity to a conflict zone or to a country or territory identified as funding or supporting terrorist activities which could increase the risk of that finance centre being used as a transit jurisdiction to move funds linked with terrorist activity?

~~(b)~~(g) Is *FT* criminalised or inadequately criminalised in the country or territory? Information on which may be found in its FATF or equivalent mutual valuation report.

~~103.~~104. *Risk* factors the firm should consider when identifying a country's or territory's level of transparency and tax compliance include:

(a) Is there information from more than one credible and reliable source that the country has been deemed compliant with international tax transparency and information sharing standards? Is there evidence that relevant rules are effectively implemented in practice? Examples of possible sources include reports by the Global Forum on Transparency and the Exchange of Information for Tax Purposes of the OECD, which rate jurisdictions for tax transparency and information sharing purposes; assessments of the country's or territory's commitment to automatic exchange of information based on the Common Reporting Standard; assessments of compliance with Recommendations 9, 24 and 25 and Immediate Outcomes 2 and 5 of *the FATF Recommendations* by the FATF or FATF-style regional bodies; and IMF assessments (for example, IMF staff assessments of offshore financial centres).
(b) Has the country or territory committed to, and effectively implemented, the Common Reporting Standard on Automatic Exchange of Information, which the G20 adopted in 2014?
(c) Has the country or territory put in place reliable and accessible beneficial ownership registers?

~~104.~~105. *Risk* factors the firm should consider when identifying the *risk* associated with the level of predicate offences to *ML* in a country or territory include:

(a) Is there information from credible and reliable public sources about the level of predicate offences to *ML* in the country or territory, for example, corruption, organised crime, tax crime and serious fraud? Examples include corruption perceptions indices; OECD country reports on the implementation of the OECD's anti-bribery convention; and the UN Office on Drugs and Crime World Drug Report.
(b) Is there information from more than one credible and reliable source about the capacity of the country's or territory's investigative and judicial system to effectively investigate and prosecute these offences?

3.17.3. Products, Services and Transactions Risk Factors

~~105.~~106. When identifying the *risk* associated with its products, services or transactions, the firm should consider the *risk* related to:

(a) the level of transparency, or opaqueness, the product, service or transaction affords;
(b) the complexity of the product, service or transaction; and
(c) the value or size of the product, service or transaction.

~~106.~~107. *Risk* factors that may be relevant when considering the *risk* associated with a product, service or transaction's transparency include:

(a) To what extent do products or services allow the *customer* or *beneficial owner* structures to remain anonymous, or facilitate hiding their identity? Examples of such products and services include *bearer shares*, fiduciary deposits, personal asset holding vehicles, and legal entities such as foundations that can be structured in such a way as to take advantage of anonymity and allow dealings with shell companies or companies with nominee shareholders.
(b) To what extent is it possible for a third party that is not part of the *business relationship* to give instructions, for example, in the case of certain *correspondent banking relationships*?

~~107.~~108. *Risk* factors that may be relevant when considering the *risk* associated with a product, service or transaction's complexity include:

(a) To what extent is the transaction complex and does it involve multiple parties or multiple countries or territories, for example, in the case of certain trade finance transactions? Are transactions straightforward, for example, are regular payments made into a pension fund?
(b) To what extent do products or services allow payments from third parties or accept overpayments where this would not normally be expected? Where third party payments are expected, does the firm know the third party's identity, for example, is it 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 *FSB* that is subject to AML and CFT standards and oversight that are comparable to those in *the Bailiwick*?
(c) 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?

~~108.~~109. *Risk* factors that may be relevant when considering the *risk* associated with a product, service or transaction's value or size include:

(a) To what extent are products or services cash intensive, for example, many payment services and certain current *accounts*?
(b) To what extent do products or services facilitate or encourage high-value transactions? Are there any caps on transaction values or levels of premium that could limit the use of the product or service for *ML* and *FT* purposes?

3.17.4. Delivery Channel Risk Factors

~~109.~~110. When identifying the *risk* associated with the way in which the *customer* obtains the products or services they require, the firm 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 of business or other intermediaries the firm might use and the nature of their relationship with the firm.

~~110.~~111. When assessing the *risk* associated with the way in which the *customer* obtains the products or services, the firm should consider a number of factors including:

(a) Is the *customer* physically present for identification purposes? If they are not, has the firm used a reliable form of *identification data*? Has it taken steps to prevent impersonation or identity fraud?
(b) Has the *customer* been introduced by another part 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* or *FT risk*? What has the firm done to satisfy itself that the group entity applies *CDD* measures equivalent to those of the firm?
(c) Has the *customer* been introduced by a third party (for example, an *FSB* that is not part of the same group)? What has the firm done to be *satisfied* that:

(i) the third party applies *CDD* measures and keeps records to a standard equivalent to *the FATF Recommendations*;
(ii) the third party will provide, immediately upon request, relevant copies of *identification data* in accordance with Paragraph 10 of *Schedule 3* and Chapter 10 of this *Handbook*; and
(iii) the quality of the third party's *CDD* measures is such that it can be relied upon?

(d) Has the *customer* been introduced through a tied agent, that is, 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*?

(e) 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?

(f) Where a firm uses an *intermediary*, are there any indications that the *intermediary's* level of compliance with applicable AML legislation or regulation is inadequate, for example, has the *intermediary* been sanctioned for breaches of AML or CFT obligations?