Guernsey Financial Services Commission

Handbook on Countering Financial Crime (AML/CFT/CPF)

~~28 October~~XX December 2025

Table of Acronyms

The following acronyms are used within this *Handbook*. Where necessary definitions of these terms can be found in Appendix A.

AI	Artificial Intelligence
AML	Anti-Money Laundering
App	Application
BACS	Bankers' Automated Clearing System
CDD	Customer Due Diligence
CECIS	Closed-Ended Collective Investment Scheme
CFT	Countering the Financing of Terrorism
CMP	Compliance Monitoring Programme
CPF	Countering the Financing of Proliferation of Weapons of Mass Destruction
CIS	Collective Investment Scheme
DT	Drug Trafficking
ECDD	Enhanced Customer Due Diligence
ESAs	European Supervisory Authorities
EU	European Union
FATF	Financial Action Task Force
FIU	Financial Intelligence Unit
FSB	Financial Services Business
GP	General Partner
IBAN	International Bank Account Number
IC	Incorporated Cell
ICC	Incorporated Cell Company
IFSWF	International Forum of Sovereign Wealth Funds
IMF	International Monetary Fund
IOSCO	International Organization of Securities Commissions
IT	Information Technology
LCF	Lending, Credit and Finance
LLP	Limited Liability Partnership
LP	Limited Partnership
LPP	Legal Professional Privilege
MI	Management Information
ML	Money Laundering
MLCO	Money Laundering Compliance Officer
MLRO	Money Laundering Reporting Officer
MONEYVAL	The Committee of Experts on the Evaluation of Anti-Money Laundering and the Financing of Terrorism
MSP	Money Service Provider
MVTS	Money or Value Transfer Service
NATO	North Atlantic Treaty Organization
NGCIS	Non-Guernsey Collective Investment Scheme
NPO	Non-Profit Organisation
NRA	National Risk Assessment
OECD	Organisation for Economic Co-operation and Development

1.1. Introduction

1. The laundering of criminal *proceeds*, the financing of terrorism and proliferation financing (henceforth referred to collectively as "ML, TF and PF") through the financial and business systems of the world is vital to the success of criminal, terrorist and proliferation operations. To this end, criminals, terrorists and proliferators seek to exploit the facilities of the world's businesses in order to benefit from such *proceeds* or financing.

2. Increased use of technology and integration of the world's financial systems ~~and~~, combined with the removal of barriers to the free movement of capital, have enhanced the ease with which criminal *proceeds* can be laundered or terrorist or proliferation funds transferred and have added to the complexity of audit trails. The future of the Bailiwick of Guernsey ("*the Bailiwick*") as a well-respected international financial centre depends on its ability to prevent the abuse of its financial services business ("*FSB*") and prescribed business ("*PB*") sectors by criminals and terrorists.

1.2. Background and Scope

3. *The Bailiwick* authorities are committed to ensuring that criminals, including money launderers, terrorists and those financing terrorism or the proliferation of weapons of mass destruction, cannot launder the *proceeds* of crime through *the Bailiwick* or otherwise use *the Bailiwick's* finance and business sectors. The Guernsey Financial Services Commission ("*the Commission*") endorses the International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation issued by the Financial Action Task Force ("FATF" and "*the FATF Recommendations*"). This *Handbook* is a statement of the standards expected by *the Commission* of all *specified businesses* in *the Bailiwick* to ensure *the Bailiwick's* compliance with *the FATF Recommendations*.

4. Should a *specified business* assist in *ML, TF* and/or *PF*, it could face regulatory investigation, the loss of its reputation, and law enforcement investigation. The involvement of a *specified business* with criminal *proceeds*, terrorist funds or proliferation financing would also damage the reputation and integrity of *the Bailiwick* as an international finance centre.

5. Throughout this *Handbook* references to *PF* relate solely to the breach, non-implementation, circumvention or evasion of targeted financial sanctions that are imposed under any international sanctions measure implemented in *the Bailiwick* which relate to the proliferation of weapons of mass destruction ("WMD") and its financing. The term "proliferator" is used in the Handbook to refer to those involved in *PF* which could include State actors seeking to enhance their own WMD, individuals or entities seeking to profit from proliferation of WMD and terrorist groups which may acquire or develop WMD for use in terrorist acts. References to WMD relate to biological, chemical or nuclear (including radiological) weapons.

6. Under Section 1(1) of the Criminal Justice (Proceeds of Crime) (Bailiwick of Guernsey) Law, 1999 as amended ("*the Law*") all offences that are indictable under the laws of *the Bailiwick* are considered to be predicate offences and therefore funds or any type of property, regardless of value, acquired either directly or indirectly as the result of committing a predicate offence, are considered to be the *proceeds* of crime. Under *Bailiwick* law all offences are indictable, with the exception of some minor offences which mainly concern public order and road traffic. The range of predicate offences is therefore extremely wide and includes, but is not limited to, the following:

   (a) participation in an organised criminal group and racketeering;
   (b) terrorism, including *TF*;
   (c) financing of proliferation of weapons of mass destruction;
   (d) human trafficking and migrant smuggling;

(n) The Beneficial Ownership of Legal Persons (Alderney) Law, 2017;
(o) The Beneficial Ownership (Definition) Regulations, 2017;
(p) The Beneficial Ownership (Alderney) (Definitions) Regulations, 2017;
(q) The Beneficial Ownership of Legal Persons (Provision of Information) (Transitional Provisions) Regulations, 2017;
(r) The Beneficial Ownership of Legal Persons (Provision of Information) (Transitional Provisions) (Alderney) Regulations, 2017;
(s) The Beneficial Ownership of Legal Persons (Nominee Relationships) Regulations, 2017;
(t) The Beneficial Ownership of Legal Persons (Nominee Relationships) (Alderney) Ordinance, 2017; and
(u) The Beneficial Ownership of Legal Persons (Provision of Information) (Limited Partnerships) Regulations, 2017;

and such other enactments relating to *ML, FT* and *PF* as may be enacted from time to time in *the Bailiwick*.

10. Sanctions legislation is published by the States of Guernsey's Policy & Resources Committee and can be accessed via the below website:

www.gov.gg/sanctions

1.4. Handbook Purpose

11. This *Handbook* has been issued by *the Commission* and, together with statements and instructions issued by *the Commission*, contains the rules and guidance referred to in: Sections 49AA(7) and 48MB(1)of *the Law*; Paragraph 3(7) of *Schedule 3* to *the Law*; Sections 15(8) and 74C(1) of the Terrorism and Crime (Bailiwick of Guernsey) Law, 2002 as amended ("*the Terrorism Law*"); Section 15 of the Disclosure (Bailiwick of Guernsey) Law, 2007 as amended ("*the Disclosure Law*"); and Section 11 of the Transfer of Funds (Guernsey) Ordinance, 2017, the Transfer of Funds (Alderney) Ordinance, 2017 and the Transfer of Funds (Sark) Ordinance, 2017 ("*the Transfer of Funds Ordinance*").

12. This *Handbook* is issued to assist the firm in complying with the requirements of the relevant legislation concerning *ML, TF* and *PF* financial crime and related offences to prevent *the Bailiwick's* financial system and operations from being abused for *ML, TF* and *PF*. *The Law* and *the Terrorism Law* as amended state that *the Bailiwick* courts shall take account of rules made and instructions and guidance given by *the Commission* in determining whether or not the firm has complied with the requirements of *Schedule 3*.

13. This *Handbook* has the following additional purposes:

(a) to outline the legal and regulatory framework for AML, CFT and CPF requirements and systems;
(b) to interpret the requirements of *the Relevant Enactments* and provide guidance on how they may be implemented in practice;
(c) to indicate good industry practice in AML, CFT and CPF procedures through a proportionate, *risk*-based approach; and
(d) to assist in the design and implementation of systems and controls necessary to mitigate the *risks* of the firm being used in connection with *ML, TF* and *PF* and other financial crime.

14. The *Commission* acknowledges the differing approaches adopted by *specified businesses* to achieve compliance with the requirements of *the Relevant Enactments* and *Commission Rules*. The Commission encourages all firms to consider how developments in technology could assist them in complying with their obligations as well as streamlining business processes. This

Handbook therefore seeks to adopt a technology ~~neutral~~positive stance, allowing ~~the firm~~firms to embrace whichever technological solution(s) ~~it deems~~they have assessed and deem appropriate to meet ~~its obligations.~~their obligations. The Handbook still allows firms to utilise existing measures to meet their obligations, provided those measures remain effective, proportionate and do not unduly prevent other firms' use of technology. Further information about the use of technology can be found in Chapter 3 of this *Handbook*.

1.5. Requirements of Schedule 3

15. *Schedule 3* includes requirements relating to:

(a) *risk* assessment and mitigation;
(b) applying *CDD* measures;
(c) monitoring *customer* activity and ongoing *CDD*;
(d) reporting suspected *ML, TF* and *PF* activity;
(e) *employee* screening and training;
(f) record keeping; and
(g) ensuring compliance, corporate responsibility and related requirements.

16. Any paraphrasing of *Schedule 3* within parts of this *Handbook* represents *the Commission's* own explanation of that schedule and is for the purposes of information and assistance only. *Schedule 3* remains the definitive text for the firm's AML, CFT and CPF obligations. *The Commission's* paraphrasing does not detract from the legal effect of *Schedule 3* or from its enforceability by the courts. In case of doubt, you are advised to consult a *Bailiwick* Advocate.

17. In addition to the requirements of *Schedule 3,* section 48MA of *the Law* and section 74A of *The Terrorism Law* include offences relating respectively to failure to prevent money laundering and failure to prevent terrorist financing. Under these sections a firm licensed under *the Regulatory Laws* (for the purposes of this section, the "licensed firm") is guilty of an offence if a person is engaged in money laundering or terrorist financing when acting in the capacity of a person associated with the licensed firm, unless the licensed firm can prove it had in place prevention procedures in relation to the activities of the person associated with the licensed firm when the money laundering or terrorist financing offence occurred.

18. If the licensed firm has in place effective policies, procedures and controls to counter *ML*, *TF* and *PF* which are in line with the requirements of *Schedule 3* and the *Handbook*, they could be considered towards prevention procedures in relation to the offences under section 48MA of *the Law* and section 74A of *The Terrorism Law*.

1.6. Structure and Content of the Handbook

19. This *Handbook* takes a two-level approach:

(a) Level one ("*Commission Rules*") sets out how *the Commission* requires the firm to meet the requirements of *Schedule 3*. Compliance with the *Commission Rules* will be taken into account by the courts when considering compliance with *Schedule 3* (which is legally enforceable and a contravention of which can result in prosecution); and
(b) Level two ("*guidance*") presents ways of complying with *Schedule 3* and the *Commission Rules*. The firm may adopt other appropriate and effective measures to those set out in *guidance*, including policies, procedures and controls established by the group Head Office of the firm, so long as it can demonstrate that such measures also achieve compliance with *Schedule 3* and the *Commission Rules*.

20. When the requirements of *Schedule 3* are explained or paraphrased in this *Handbook*, the term 'shall' is used and the text is presented in blue shaded boxes for ease of reference. Reference is also made to the relevant paragraph(s) of *Schedule 3*.

21. When the requirements of *the Transfer of Funds Ordinance* and *the EU Regulation* are explained or paraphrased in Chapter 14 of this *Handbook*, the term 'shall' is used and the text is presented in clear boxes for ease of reference. Reference is also made to the relevant paragraph(s) of the Ordinance.

22. Where the *Commission Rules* are set out, the term 'must' is used and the text is presented in red shaded boxes to denote that these are rules.

23. In all cases the terms 'shall' and 'must' indicate that these provisions are mandatory and subject to the possibility of prosecution (in the case of a contravention of *Schedule 3* or *the Transfer of Funds Ordinance*) as well as regulatory sanction and any other applicable sanctions.

24. In respect of *guidance*, this *Handbook* uses the terms 'should' or 'may' to indicate ways in which the requirements of *Schedule 3*, *the Transfer of Funds Ordinance* and the *Commission Rules* can be satisfied, but allowing for alternative means of meeting the requirements as deemed appropriate by the firm.

25. References to the *Commission Rules* within this *Handbook*, are made by stating the Chapter number, followed by the paragraph number, for example, Commission Rule 7.23 refers to the rule stated within Chapter 7 at paragraph 23. Sections have also been included within this *Handbook* for ease of navigation.

26. *The Commission* will from time to time update this *Handbook* to reflect new legislation, developments in the financial services and *PB* sectors, changes to international standards, recommendations from mutual evaluations, good practice and amendments to *Schedule 3* or *the Relevant Enactments*.

27. This *Handbook* is not intended to provide an exhaustive list of appropriate and effective policies, procedures and controls to counter *ML, TF* and *PF*. The structure of this *Handbook* is such that it permits the firm to adopt a *risk*-based approach appropriate to its particular circumstances. The firm should give consideration to additional measures which may be necessary to prevent any exploitation of it and of its products, services and/or delivery channels by persons seeking to carry out *ML, TF* and/or *PF*.

1.7. Significant Failure to Meet the Required Standards

28. For any firm, whether regulated by or registered with *the Commission*, the primary consequences of any significant failure to meet the standards required by *Schedule 3*, the *Commission Rules* and *the Relevant Enactments* will be legal ones. In this respect *the Commission* will have regard to the firm's compliance with the provisions of *Schedule 3*, the *Commission Rules* and *the Relevant Enactments* when considering whether to take enforcement action against it in respect of a breach of any requirements of the aforementioned. In such cases, *the Commission* has powers to impose a range of disciplinary and financial sanctions, including the power to withdraw, restrict or suspend the licence of the firm where applicable.

29. Where the firm is regulated by *the Commission*, *the Commission* is entitled to take such failure into consideration in the exercise of its judgement as to whether the firm and its directors and managers have satisfied the minimum criteria for licensing. In particular, in determining whether the firm is carrying out its business with integrity and skill and whether a natural person is fit and

ensure a thorough assessment of the *ML* and *FT risks* presented by the individual sectors within the finance industry and products and services from within *the Bailiwick*. New information and analysis, as well as an update on the 2020 assessment, was published in 2023 and included for the first time an assessment of the *PF risks* to the Bailiwick. An extension of the 2023 *NRA* was published in 2024 on *legal persons* and *legal arrangements*.

36. The key finding of ~~both~~the *NRA*s with regard to *ML risk* is that as an international finance centre with a low domestic crime rate, *the Bailiwick's* greatest *ML risk* comes from the laundering of the proceeds of foreign criminality~~.~~ largely through *legal persons* and *legal arrangements* which are used for cross-border business, holding or managing assets. The underlying offences most likely to be involved are bribery and corruption, fraud and tax evasion. The key finding of ~~both~~the *NRA*s with regard to *TF risks* is that the greatest *risks* come from its cross-border business being used to support foreign terrorism, by funds being passed through or administered from the *Bailiwick*. However, this *risk* is much lower than the *ML risks* from cross-border business. *TF* from cross-border business is most likely to arise in the context of secondary terrorist financing, i.e. where criminal proceeds are used to fund terrorism. The key finding of the ~~most~~more recent *NRA* with regard to *PF risks* is that the greatest *risks* come from its cross-border business being used for the movement of funds linked to proliferation activity, by funds being passed through or administered from the *Bailiwick*. However, as the *Bailiwick* has no diplomatic connections, and no known economic, geographic, ideological or political links with the two sanctioned countries for proliferation – the Democratic People's Republic of North Korea and Iran, this *risk* is more remote than the *TF risks* from cross-border business.

37. The assessment of *risks* and vulnerabilities detailed within an *NRA* will naturally cascade through to *specified businesses* within *the Bailiwick*. In this respect, references are made throughout *Schedule 3* and this *Handbook* requiring the firm to have regard to the content of the latest ~~*NRA*~~*NRAs* when undertaking certain activities, for example, the formulation of its *business risk assessments* and *risk appetite*.

38. *The Bailiwick* reviews the ~~*NRA*~~*NRAs* on an on-going and trigger-event basis, making changes as necessary taking into account market changes, the advancement of technology and data collected from industry, for example, through various surveys and regulatory returns.

39. All references to the *NRA* in the Handbook refer to the latest ~~version~~versions published by the States of Guernsey, including the 2024 assessment of *legal persons* and *legal arrangements*. A copy of *the Bailiwick's NRA*s can be found on the website of the States of Guernsey's Policy & Resources Committee:

National Risk Assessment

1.11 MONEYVAL

40. The Committee of Experts on the Evaluation of Anti-Money Laundering and the Financing of Terrorism ("MONEYVAL") is a monitoring body of the Council of Europe. The aim of MONEYVAL is to ensure that its member states have in place effective systems to counter *ML, TF* and *PF* and comply with the relevant international standards in these fields.

41. On 10 October 2012 the Committee of Ministers of the Council of Europe, following a request by the United Kingdom ("UK"), adopted a resolution to allow *the Bailiwick*, the Bailiwick of Jersey and the Isle of Man (the "*Crown Dependencies*") to participate fully in the evaluation process of MONEYVAL and to become subject to its procedures.

42. MONEYVAL's most recent evaluation of *the Bailiwick* was conducted during ~~October 2014~~April 2024 and assessed *the Bailiwick's* compliance with the FATF ~~2003~~2012 Recommendations. In its report, published on ~~15 January 2016~~10 February 2025, MONEYVAL

concluded that since the last evaluation in 2014 *the Bailiwick* has '~~a mature~~made significant efforts to strengthen its legal and regulatory ~~system' and surpassed the equivalent review by~~AML/CFT framework' with a 'robust AML/CFT legal framework for technical compliance' with the ~~IMF in 2010.~~FATF Recommendations.

www.coe.int/en/web/moneyval/jurisdictions/guernesey

(m) Whether the value of transactions is expected to be particularly high;
(n) The nature, scale and countries/geographic areas associated with *funds* sent and received on behalf of *customers*;
(o) Whether payments to any unknown or un-associated third parties are allowed; and
(p) Whether the products/services/structure are of particular, or unusual, complexity.

Other potential sources of *risk* to consider:

(q) Internal and/or external audit findings;
(r) Typologies and findings of *ML, TF* and *PF* case studies;
(s) UNSCR targeted financial sanctions relating to *TF* and *PF*;
(t) UK and *Bailiwick* sanctions; and
(u) Designation of persons under EU, OFAC and other sanctions.

3.11. New Products and Business Practices

63. In accordance with Paragraphs 3(3)(c)(i) and 16A 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, TF* and *PF risks* arising from those products or practices.

64. 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, TF* or *PF risks* to the firm.

65. 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.

66. 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 and Developing Technologies

67. 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.

68. 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*, through to the use of electronic verification systems to establish the identity of a natural person or use of Artificial Intelligence ("AI") for monitoring purposes.

69. The *risk* assessment of a new or developing technology must include, as a minimum, an assessment of the *ML, TF* and *PF 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~~.~~, in advance of its deployment and through ongoing monitoring, or measurement, of its results.

70. 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~~objectives of the *risk* assessment ~~is~~are to assist the firm's understanding of the technology it is adopting, to evaluate the *ML, TF* and *PF risk*s ~~and~~which would arise from its use, including any new *risks* to the firm, and the vulnerabilities inherent in the use of the technology ~~and~~in order to identify the controls necessary to mitigate and limit the firm's exposure~~.~~ to those *risks*.

71. For firms which are part of a group which is introducing new technology or developing technology for use within the group, the firm may rely on the group's *ML/TF/PF risk* assessment, provided the assessment considers in sufficient detail the nature of the firm's business and risk profile, which may differ from other parts of the group. The firm should have a copy of the assessment with which its Board or its senior managers are familiar. If the assessment is not sufficient to meet the firm's obligations under Schedule 3 and the *Commission Rules* in this *Handbook*, the firm should conduct its own risk assessment of the technology.

72. It is also important that the firm considers and plans how the technology it is considering adopting will be implemented, particularly where it involves integration with existing systems, as poor implementation can create vulnerabilities in the firm's overall controls for preventing and detecting ML, TF and PF. Implementation plans should cover the following areas:-

a) ensuring that the firm's AML/CFT/CPF policies, procedures and controls accurately reflect how the technology is to be used and updating them as required;
b) good data governance around the underlying data to ensure it is accurate, complete, accessible, up to date and relevant;
c) appropriate user testing and management reporting of results before formal roll-out;
d) provision of appropriate training to staff who will be using the technology;
e) provision of appropriate training to staff in compliance roles testing its output as part of the firm's compliance monitoring programme;
f) ensuring appropriate risk-based systems testing, both before and during deployment of the technology; and
g) ensuring that the firm makes appropriate investment in the full suite of systems required, including any additional resourcing and system upgrade requirements.

The Commission's Cyber Security Rules and Guidance may also assist the firm's development of its use of technology.

Cyber Security Rules and Guidance, 2021.pdf

73. Depending on the nature of the technology being considered, a technology risk assessment should consider the following areas:

a) the robustness, resilience and security of the technology from the risk of data loss, particularly from cyber-attacks;
b) how the technology enables the firm to comply with its obligations under *Schedule 3* and this *Handbook*, including for example the regulatory requirements in relation to *CDD*, activity/transaction monitoring, record-keeping and sharing relevant data within the firm, its group (if applicable) and relevant authorities such as the Commission and the FIU, as relevant to the technology being considered;
c) where the technology leads to faster transaction times, the ability of the firm to monitor and intervene in an unusual transaction which may give rise to a suspicion of ML, TF or PF; and
d) any supplier related issues which could impact its operation.

A firm considering adopting electronic verification systems should ensure its assessment covers areas set out in *Commission Rules 5.28,* 5.34 and guidance in paragraph 5.35 of the *Handbook*.

~~71.~~74. 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.

~~72.~~75. 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, TF* and *PF business risk assessments* as described in Section 3.9. of this *Handbook*, particularly in light of the fast pace of technological developments.

Relationship Risk Assessment

3.13. Introduction

~~73.~~76. 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.

~~74.~~77. 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, TF* and *PF risks* identified in the *business risk assessments*.

~~75.~~78. There may be circumstances where the *risks* of *ML, TF* and *PF* 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

~~76.~~79. In order to consider the extent of its potential exposure to the *risk*s of *ML, TF* and *PF*, 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.

~~77.~~80. 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*.

~~78.~~81. 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:

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

~~79.~~82. The FATF publishes two lists identifying jurisdictions with weak measures to combat *ML, TF* and *PF*. The first list is of "High risk jurisdictions subject to a call for action" which identifies a

4.3.1. The Customer

13. In accordance with Paragraph 4(3)(a) of *Schedule 3*, the *customer* shall be identified and the identity of the *customer* verified using *identification data*.

14. Chapters 5 and 7 of this *Handbook* provide for the *CDD* measures to be applied where the *customer* is a natural person, or a *legal person* and *legal arrangement* respectively.

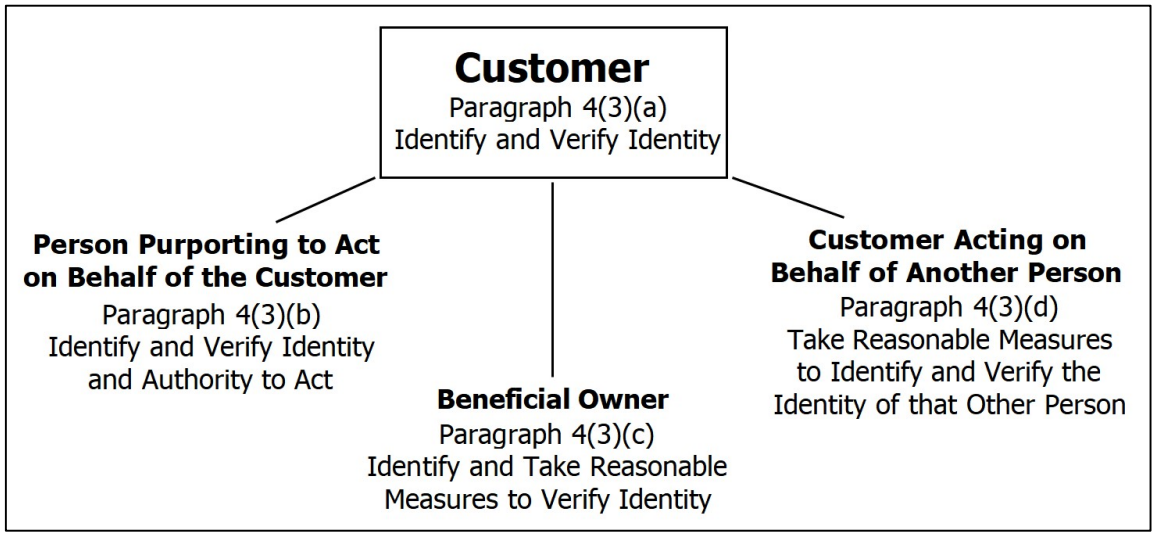


Fig. 1 – CDD Measures for Key Principals

4.3.2. A Person Purporting to Act on Behalf of the Customer

15. In accordance with Paragraph 4(3)(b) of *Schedule 3*, any person purporting to act on behalf of the *customer* shall be identified and that person's identity and authority to so act shall be verified.

16. Examples of such persons will include a guardian of a natural person, the authorised signatories (or equivalent) acting for or on behalf of a *legal person* or *legal arrangement*, those to whom powers of attorney have been granted, the directors (or equivalent) who are acting on behalf of a *legal person*, and any other person acting on behalf of the *customer* within a *business relationship* or *occasional transaction*.

17. In taking measures to verify the identity of any person purporting to act on behalf of the *customer*, the firm should take into account the *risk* posed by the *business relationship* or *occasional transaction*, the materiality of the authority delegated to the individual and the likelihood of that person giving the firm instructions concerning the use or transfer of *funds* or assets.

18. Examples of the measures the firm could take to verify the authority of a person to act could include obtaining a copy of the authorised signatories list, power of attorney or other authority or mandate providing the person with the authority to act on behalf of the *customer*.

19. The identification and verification of the identity of any person identified in accordance with Paragraph 4(3)(b) of *Schedule 3* should be undertaken in accordance with ~~Chapter~~Chapters 5 and 7 of this *Handbook*.

4.3.3. The Beneficial Owner of the Customer

20. In accordance with Paragraph 4(3)(c) of *Schedule 3*, the *beneficial owner* shall be identified and reasonable measures shall be taken to verify such identity using *identification data* and such measures shall include, in the case of a *customer* which is a *legal person* or *legal arrangement*,

measures to understand the nature of the *customer*'s business and its ownership and control structure.

21. Paragraph 22 of *Schedule 3* sets out the definition of *beneficial owner*. It should be noted that the definition varies based upon the type of *legal person* or *legal arrangement* involved in a *business relationship* or *occasional transaction*. Further detail can be found in Chapter 7 of this *Handbook*.

22. For the purposes of Paragraph 4(3)(c) of *Schedule 3*, 'reasonable measures' should be read as referring to the taking of measures, which are commensurate with the *ML, TF* and *PF risks* which have been identified within the *business relationship* or *occasional transaction*, to understand the nature of the *customer's* business and its ownership and control structure and to verify that the *beneficial owner* of the *customer* is who he or she is claimed to be.

23. Where the *business relationship* or *occasional transaction* involves a *legal person* registered in the *Bailiwick*, the firm may have access to the beneficial ownership register maintained by the Guernsey Registry or the Alderney Registry. Whilst the beneficial ownership register is not a substitute for *CDD* measures to identify the legal person's beneficial owners, it could be useful as an additional source to validate or otherwise confirm the firm's understanding of the ownership and control structure of the customer. This position also applies to foreign beneficial ownership registers the firm may be able to access.

~~23.~~24. Where the *business relationship* or *occasional transaction* is a *high risk relationship*, the measures to understand the nature of the *customer's* business and its ownership and control structure will be greater than for low or standard *risk* relationships and may require the firm to ask more questions of the *customer* and require additional information about the *customer's* business and its beneficial ownership. Similarly the extent of the measures considered to be reasonable to verify the identity of the *beneficial owner* will be greater for *high risk relationships* and may require the firm to undertake more rigorous checks on the *beneficial owner* or obtain more robust forms of *identification data* to *satisfy* the firm that it has accurately verified the *beneficial owner's* identity.

4.3.4. A Person on Behalf of Whom the Customer is Acting

~~24.~~25. In accordance with Paragraph 4(3)(d) of *Schedule 3*, a determination shall be made as to whether the *customer* is acting on behalf of another person and, if the *customer* is so acting, reasonable measures shall be taken to identify that other person and to obtain sufficient *identification data* to verify the identity of that other person.

~~25.~~26. For the purposes of Paragraph 4(3)(d) of *Schedule 3*, 'reasonable measures' should be read as referring to the taking of measures, which are commensurate with the *ML, TF* and *PF risks* which have been identified within the *business relationship* or *occasional transaction*, to establish the identity of any natural person on whose behalf the firm has determined the *customer* is acting. Where the *risk* of the *business relationship* or *occasional transaction* is high, the extent of the measures considered to be reasonable will naturally be greater than those applied to *low risk relationships*.

~~26.~~27. The firm should refer to the *CDD* measures set out in Chapters 5 and 7 of this *Handbook* which the firm should take reasonable measures to apply to any person which the firm determines to fall within Paragraph 4(3)(d) of *Schedule 3*.

4.4. Policies, Procedures and Controls

~~27.~~28. The firm must have take-on policies, procedures and controls in place which explain how to identify, and verify the identity of, the *customer*, *beneficial owner* and other *key principals*

identified by Paragraph 4(3) of *Schedule 3* to a level appropriate to the characteristics and assessed *risk* of the *business relationship* or *occasional transaction*.

~~28.~~29. The firm must assess, on the basis of *risk*, how much identification information to request, what to verify, and how to verify it, in order to be *satisfied* as to the identity of a *customer*, *beneficial owner* or other *key principal*.

~~29.~~30. The firm's policies, procedures and controls in respect of its *CDD* measures must:

(a) be *risk*-based to differentiate between what is expected in *low risk relationships*, what is expected in *high risk relationships* and what is expected in situations which are neither high *risk* nor low *risk*;
(b) provide for *enhanced measures* to be applied in the circumstances where such measures are required in accordance with Paragraph 5(2) of *Schedule 3*;
(c) impose the least necessary burden on *customers*, *beneficial owners* and other *key principals* consistent with meeting the requirements of *Schedule 3* and the *Commission Rules*;
(d) not constrain access to financial services (for example, by those without driving licences or passports); and
(e) deal sensibly and sensitively with special groups for whom special processes may be appropriate (for example, the elderly and students studying overseas).

~~30.~~31. *Identification data* providing evidence to verify identity and address can come from a range of sources, including physical or digital *documents*, databases and electronic data sources. These sources may differ in their integrity, suitability, reliability and independence, for example, some *identification data* is issued by governments after due diligence has been undertaken on an individual's identity, i.e. national identity cards and passports, while other *identification data* may be issued with few or no checks undertaken on the subject.

~~31.~~32. In light of this, the firm should consider the suitability of *identification data* prior to its acceptance, including its source and whether underlying identity checks have been undertaken by the issuing body or authority. The firm should also consider the susceptibility of a *document* or source to forgery when determining its acceptability.

~~32.~~33. Where the firm does not receive, or have sight of, the original physical *documentation* used to verify identity (unless it uses an electronic verification system as described in Chapter 5) and where instead copy *documentation* is provided, the firm must ensure that the copy *documentation* has been digitally or physically certified by a suitable third party.

~~33.~~34. Further information on the policies, procedures and controls required in respect of electronic identification and verification, digital certification and certification can be found within ~~Chapter~~Chapters 5 and 6 of this *Handbook*.

~~34.~~35. Where the firm is not familiar with the form of the *identification data* obtained to verify identity or address, appropriate measures should be undertaken by the firm to *satisfy* itself that the *identification data* is genuine. Evidence of the steps taken by the firm should be retained as proof of its understanding and conclusions in respect of the *documents* received.

~~35.~~36. All key *documents* (or parts thereof) must be understood by an *employee* of the firm and that understanding must be recorded and retained with the relevant *document*.

~~36.~~37. The translation of *documents* should be considered on a case by case basis as it may be obvious to the firm or an *employee* in certain instances what a *document* is and what it means. The firm may also use electronic translation services including AI to translate documents, providing it is

satisfied with the output. The firm may, in circumstances where the foreign language is less familiar to it, use more than one electronic translation service to validate its understanding of the document. The firm remains responsible for the resultant product of the electronically translated documents. In all cases the firm should record its understanding of the *document* and where relevant the reason why it has not sought to translate a *document*.

~~37.~~38. Notwithstanding the above, the firm must translate all key *documents* (or parts thereof) into English at the reasonable request of *the Commission* or the *FIU*.

~~38.~~39. Where *identification data* accepted by the firm to verify the identity of a natural person contains the individual's signature and/or a photograph of the individual, the firm should ensure that the photograph and/or signature is clearly legible on the copy or scan of the *document* retained by the firm.

4.5. Timing

~~39.~~40. In accordance with Paragraph 7(1) of *Schedule 3*, the identification and verification of the identity of any person or *legal arrangement* pursuant to Paragraphs 4 to 6 of *Schedule 3* shall, subject to Paragraphs 4(1)(b) and 7(2) of *Schedule 3*, be carried out before or during the course of establishing a *business relationship* or before carrying out an *occasional transaction*.

~~40.~~41. There will be occasions when the circumstances are such that the verification of the identity of a *customer* or *beneficial owner*, cannot commence or be completed until such time as a *business relationship* has been established. This may be acceptable in certain circumstances, provided the firm is *satisfied* as to the reasons causing the delay.

~~41.~~42. In this respect, Paragraph 7(2) of *Schedule 3* provides that the verification of the identity of a *customer* and any of the *beneficial owners* may be completed following the establishment of a *business relationship* provided that to do so would be consistent with the *risk* assessment of the *business relationship* conducted pursuant to Paragraph 3(4)(a) of *Schedule 3*, and:

(a) the verification is completed as soon as reasonably practicable thereafter;
(b) the need to do so is essential not to interrupt the normal conduct of business; and
(c) appropriate and effective policies, procedures and controls are in place which operate so as to manage *risk*, including, without limitation, a set of measures, such as a limitation of the number, types and/or amount of transactions that can be performed or the monitoring of large or complex transactions being carried outside the expected norms for that *business relationship*.

~~42.~~43. Paragraph 7(2) of *Schedule 3* does not, however, permit the retrospective identification of a *customer* or *beneficial owner* after the establishment of a *business relationship,* save in the circumstances detailed in Chapter 7 of this *Handbook*, for example, where beneficiaries are identified by class and are therefore unknown to the firm at the commencement of a *business relationship*.

~~43.~~44. Where the verification of the identity of a *customer* or *beneficial owner* takes place after the establishment of a *business relationship*, the firm must have appropriate and effective policies, procedures and controls in place so as to manage the *risk* arising from the delay. These policies, procedures and controls must include:

(a) establishing that it is not a *high risk relationship*;
(b) monitoring by senior management of the *business relationship* to ensure verification of identity is completed as soon as reasonably practicable; and
(c) ensuring *funds* received are not passed to third parties.

(c) consider whether a disclosure must be made pursuant to Part I of *the Disclosure Law*, or Sections 15 or 15A, or Section 12 (as appropriate) of *the Terrorism Law*.

~~52.~~53. It is recognised that the immediate *termination* of a *business relationship* may not be possible due to contractual or legal reasons outside the control of the firm. The timing of the *termination* of an established *business relationship* will also depend upon the nature of the underlying products or services. As an example, while a *bank* can close an *account* and return deposited *funds* to a *customer* relatively easily, the compulsory redemption of an investment in a CIS, particularly where it is closed-ended or where valuation dates are infrequent, may be more problematic.

~~53.~~54. Where *termination* of a *business relationship* cannot be completed (for example, because the firm has lost contact with the *customer*) the firm should have procedures and controls in place to ensure that assets or *funds* held are 'blocked' or placed on a 'suspense' *account* until such time as contact with the *customer* is re-established or the firm has otherwise dealt with the *funds* or assets in accordance with its policy for dormant *accounts*.

~~54.~~55. Where the immediate *termination* of a *business relationship* is not possible for whatever reason, the firm must ensure that the *risk* is managed and mitigated effectively until such time as the *business relationship* can be terminated.

~~55.~~56. The firm must ensure that where *funds* have already been received, they are returned to the source from which they originated, regardless of whether the source is the *customer* or a third party. Where the firm has been unable to return the *funds* to the *account* from which they were received, for instance because the originating *bank account* has been closed, the firm must take appropriate steps to return the *funds* to the same party in another form.

~~56.~~57. Where this is not possible (for example, if the relevant party no longer exists) the firm should take appropriate steps to return any *funds* to an appropriate third party and document the reasoning for the steps taken.

~~57.~~58. Where the firm has terminated, or not proceeded with establishing, a *business relationship* or *occasional transaction*, it must consider the circumstances giving rise to the failure to complete *CDD* measures and whether these warrant a disclosure to the *FIU*.

4.8. Collective Investment Schemes

4.8.1. Responsibility for Investor CDD

~~58.~~59. As part of the process of applying to *the Commission* for the authorisation or registration of a closed-ended CIS ("CECIS") or open-ended CIS ("OECIS"), the board of the CIS (or General Partner ("GP") of a Limited Partnership ("LP"); trustee of a unit trust; or *foundation official* of a *foundation* as appropriate) will nominate a firm (the "*nominated firm*") which is licensed under *the POI Law* and contracted to, or connected with, the CIS either as its manager or designated administrator, to be responsible for meeting the requirements of *Schedule 3* and this *Handbook* for investors into the CIS, in addition to its own obligations. Where the authorisation/registration of a CIS is suspended, it remains authorised/registered for the purposes of the *POI Law* and, as such, will continue to maintain a *nominated firm*. In cases where a third party liquidator is appointed to a CIS whose authorisation/registration has been suspended, and that liquidator is registered with *the Commission* as a *prescribed business*, *the Commission* will consider a request from the liquidator to be appointed as the *nominated firm* of the CIS.

~~59.~~60. The *nominated firm* must advise *the Commission* that it has been so nominated during the course of the application process, and in any case prior to the authorisation or registration of the CIS.

~~60.~~61. The *nominated firm* must treat all investors into the CIS as if they were its *customers* and ensure that the relevant provisions of *Schedule 3* and this *Handbook* are met, for example, conducting *relationship risk assessments* and identifying, and verifying the identity of, the investors, including the *beneficial owners* and other *key principals* thereof.

~~61.~~62. Whilst the application of *CDD* measures (including *ECDD* and *enhanced measures* as necessary) may be undertaken by another party (for example, under an outsourcing arrangement) the *nominated firm* will be responsible for ensuring that appropriate *identification data* is held on all investors, including the *beneficial owners* thereof, which meets the relevant requirements of *Schedule 3* and this *Handbook*.

~~62.~~63. Where the *nominated firm* provides services to a CIS, the shares of which are traded on a stock exchange, the *nominated firm* should refer to the provisions of Section 4.8.3. of this *Handbook*~~:~~.

~~63.~~64. Where the firm provides services to a CIS and has not been nominated under Paragraph 4.58. above, the firm should treat the CIS as its *customer* and conduct *CDD* in accordance with the requirements for a CIS authorised or registered by *the Commission*.

~~64.~~65. There may be occasions where the *nominated firm* will change throughout the life of a CIS, for example, as a result of a change of designated ~~manager.~~administrator. Where the firm becomes the nominated firm for a CIS which has already been authorised or registered by *the Commission*, it must advise *the Commission* in writing that it has been so nominated as soon as reasonably practicable after its nomination.

~~65.~~66. Where the firm becomes nominated for a CIS with existing investors, the firm should give consideration to the requirements of Section 4.6. of this *Handbook*.

~~66.~~67. Notifications made in accordance with *Commission Rule* 4.64. should be submitted via the Commission's Online Submissions Portal, through the completion of a Form 235. Liquidators requesting appointment as a *nominated firm* should do so through completion of a Form 200.

https://submit.gfsc.gg/

4.8.2. Identifying and Verifying the Identity of Investors in Collective Investment Schemes

~~67.~~68. This Section details the obligations for the application of *CDD* measures to investors, including the *beneficial owners* thereof, and applies where the firm:

(a) has been nominated under Paragraph 4.58. of this *Handbook;* or
(b) is acting in the capacity of the administrator or *transfer agent* of a non-Guernsey CIS ("NGCIS"), unless the contractual arrangements for the services provided by the firm require otherwise.

~~68.~~69. Fundamental to understanding the *CDD* obligations for CIS investors is a recognition that the overall arrangements by which interests in a CIS are offered to investors, together with the arrangements under which a CIS consequently deals with investors, will determine the *CDD* measures to be applied.

~~69.~~70. When undertaking its responsibilities, the firm should be mindful of the vulnerabilities of CISs and the methods by which CISs may be used by persons or entities for *ML, TF* and/or *PF* purposes. For example:

5.4. Verification of Residential Address

15. The following are examples of suitable methods to verify the residential address of a natural person:

(a) a recent *bank*/credit card statement or utility bill;
(b) correspondence from an independent source such as a central or local government department or agency (in *the Bailiwick* and the Bailiwick of Jersey this will include States departments and parish authorities);
(c) commercial or electronic data sources;
(d) a letter from an *Appendix C business* with which the individual has an existing *business relationship* and which confirms residential address;
(e) a tenancy agreement;
(f) a personal visit to the residential address; or
(g) an electoral roll.

16. Where a natural person's principal residential address changes during the course of a *business relationship*, the firm is considered to have verified the new address where it has maintained on-going written correspondence with the natural person at that new address (i.e. it has sent and subsequently received responses to written correspondence addressed and sent by post to the new address).

5.4.1. Overseas Natural Persons

17. There may be occasions when a natural person who is not resident in *the Bailiwick* is unable to provide evidence of his or her residential address using the means set out in Paragraph 5.15. above. Examples of such individuals include residents of countries without postal deliveries or street addresses who rely on post office boxes or an employers' addresses for the delivery of mail.

18. Notwithstanding the above, it is essential for law enforcement purposes that a record of a natural person's residential address (or details of how that person's place of residence can be reached) is held by the firm. As such, it is not acceptable to simply record details of a post office box number as a natural person's address.

19. Where the firm has determined that an individual has a valid reason for being unable to produce more usual *documentation* to verify their residential address and who would otherwise be excluded from establishing a *business relationship* or undertaking an *occasional transaction* with the firm, the residential address can be verified by other means, provided the firm is *satisfied* that the method employed adequately verifies the address of the natural person and any additional *risk* has been appropriately mitigated.

20. An example of such an alternative method could be a letter from a director or officer of a reputable overseas employer confirming residence at a stated overseas address (or providing detailed directions to locate a place of residence).

5.5. Online Bank Statements or Utility Bills

21. Where the residential address of a natural person is to be verified through the use of a *bank*/credit card statement or utility bill, the default option is to obtain a form of verification which has been delivered to that natural person by post. However, the receipt of such items via the traditional postal system ~~is being~~ has largely been replaced by ~~the use of~~ online billing ~~or~~, the delivery of *bank* or utility statements via e-mail (an "electronic statement~~").~~") or through logging on to the bank/card issuer's customer portal.

22. Examples of electronic statements include:

(a) an online statement ~~from~~issued by a recognised *bank*, building society, credit card company or recognised lender bearing the name and residential address of the natural person; or

(b) an online bill in relation to rates, council tax or utilities bearing the name and residential address of the natural person.

23. Where the firm wishes to accept an electronic statement as verification of a natural person's address, it must be *satisfied* as to the validity and veracity of the electronic statement presented.

24. The firm should recognise that some electronic sources may be more easily tampered with, i.e. the data contained within them subject to amendment, than others. If suspicions are raised in relation to the integrity of any electronic statement obtained, the firm should take whatever practical and proportionate steps are available to establish whether these suspicions are substantiated, and if so, whether the relevant electronic statement should be accepted.

25. An example of a step the firm could take where it has concerns over the veracity of a *document* is to corroborate the content of that *document* using an independent source, for example, a commercial or electronic data source such as a land registry, electoral roll or similar.

5.6. Electronic Verification

26. Electronic verification is the use of an electronic method or system to verify, in whole or in part, the identity of a natural person by matching specified personal information against electronically captured physical *documentation* and/or independent electronic data sources~~.~~ through verification technology.

27. An assessment of the risks associated with using such technology should be undertaken in accordance with Paragraph 3(3)(c)(ii) of Schedule 3 and the rules and guidance in both section 3.12 of Chapter 3 and the rules in this section of this *Handbook* in advance of adopting an electronic verification system to verify a customer's identity.

28. A firm must, when undertaking a technology risk assessment of an electronic verification system in accordance with Paragraph 3(3)(c)(ii) of Schedule 3, document the identity data and information that it collects about the customer, the nature of the data sources to be used (such as a current passport) and how their authenticity is assessed by the system.

~~27.~~29. Electronic verification can be used to verify all or any combination of the mandatory data points required by *Commission Rule* 5.8. Where an electronic verification system does not fulfil all of these requirements, the firm must use one or more other methods to ensure that a natural person is fully verified in accordance with the requirements of this *Handbook*.

~~28.~~30. Electronic verification systems range in scope from the electronic capture of identity information and *identification data* on a face-to-face basis through to the self-capture of uncertified *documentation* by a natural person using an interactive application ("App") on a tablet or mobile phone. In the latter example, a photograph (or a series of photographs or a video) of the natural person are obtained through the App, together with photographs of *identification data* and address verification *documents*. The photographs are then independently reviewed and corroborated constituting the verification.

~~29.~~31. Whilst the use of electronic verification can help to reduce the time and cost involved in gathering information and *identification data* for a natural person, the firm should be mindful of any additional *risks* posed by placing reliance on an electronic method or system. This should include

understanding the method and level of review and corroboration within the system and the potential for the system to be abused~~.~~, particularly through the advancement of AI derived "deepfakes" or synthetic identities. The FATF has issued an "horizon scan" in xx 2025 warning how criminals can exploit new technologies, including AI, to facilitate their illicit activities. [holding link/add link when published]

Outcomes FATF Plenary, 22-24 October 2025

~~30.~~32. Knowledge and understanding of the functionality and capabilities of a system can help provide assurance of its suitability. In particular, there should be certainty of the methods applied to corroborate *identification data*. The use of more than one confirmatory source to match data enhances the assurance of authenticity.

33. The firm's technology risk assessment must consider and document the measures within the electronic verification system which address the risk of identification data being forged or tampered with, including through manufactured audio-visual media content to create synthetic identities (i.e. "deepfakes") The assessment must be reviewed at least annually to ensure it remains current with technological developments.

34. In addition to the rules and guidance for technology risk assessments set out in section 3.12 of this *Handbook*, a firm should consider the following factors when undertaking an assessment of an electronic verification system:

a) the clarity and resolution of the electronic copy to detect its security features such as a watermark, invisible ink, hologram or the fraudulent insertion of a photograph or data;
b) how the system tests the authenticity of the electronic document, such as through biometric data comparison, live stream facial recognition, reading data on the document's electronic chip, analysis of security features and geotagging/geolocation confirmations;
c) whether the process for copying and transmitting the electronic document to the firm presents an opportunity for the document to be tampered with or manipulated;
d) the level of security over the process of transmitting the document, including application of security codes or anti-impersonation measures, such as requirements for the natural person to verbally repeat words, perform an action or use passcodes etc.;
e) the service provider's policy for testing the veracity and security of the system from cyber-attacks and in response to the criminal development of technology to create synthetic identities/deepfakes;
f) clearly documenting how identity information and addresses are verified, for example, biometric matching of an individual in a live video to an identity document which also has anti-fraud and authenticity checks conducted on it, or searching through multiple independent sources within a specified date range for address verification etc.; and
g) the extent to which a user, or the firm, is able to bypass any built-in security features of the electronic process, or adapt the system's use beyond that intended by the service provider.

35. Whether the firm uses an in-house, group or third-party system, it should periodically question and seek assurance that the system continues to remain robust in the face of developments in the criminal exploitation of technology, including being informed of any advanced identification measures which have been introduced.

36. The firm must ensure that sufficient customer records to comply with the record-keeping requirements under Paragraph 14 of Schedule 3 and rules on Chapter 16 are available to, and readily retrievable by, the firm for the *minimum retention period*.

37. Customer records verified through electronic verification systems should detail the identity checks undertaken by the system, and the sources it used. This is usually provided in a system generated report.

38. The firm must ensure that its CDD policies, procedures and controls and its compliance monitoring programme include its use of electronic verification, where used.

39. Video calls have a role in customer due diligence in enabling the firm to discuss aspects of a new business application or proposed transaction with an existing customer. Firms should be mindful that criminals are employing increasingly sophisticated techniques to forge identity documents therefore relying solely on video calls without independent verification could expose firms to these increased risks. Selfie-photographs of the natural persons with their identity document are also not an acceptable means for verifying their identity.

~~31.~~40. Further information on the certification of *identification data* received via an electronic verification system can be found in Section 6.5. of this *Handbook*.

5.7. Independent Data Sources

~~32.~~41. *Identification data* does not have to be in paper form. Independent data sources can provide a wide range of confirmatory material on natural persons and are becoming increasingly accessible, for example, through improved availability of public information and the emergence of commercially available data sources such as electronic databases and research firms. Sources include:

(a) electoral roll;
(b) telephone directories;
(c) credit reference agency checks;
(d) business information services; and
(e) electronic checks provided by commercial agencies.

~~33.~~42. Where the firm is seeking to verify the identity of a natural person using an independent data source, whether by accessing the source directly or by using an independent third party organisation (such as a credit reference agency), an understanding of the depth, breadth and quality of the data is important in order to determine that the method of verification does in fact provide satisfactory evidence of identity.

~~34.~~43. Independent data sources can be used to verify all or any combination of the mandatory data points required by *Commission Rule* 5.8. Where an independent data source does not fulfil all of these requirements, the firm must use one or more other methods to ensure that a natural person is fully verified in accordance with the requirements of this *Handbook*.

~~35.~~44. When relying on independent data sources to verify identity, the firm should ensure that the source, scope and quality of that data is suitable and sufficient and that the process provides for the information to be captured and recorded.

5.8. Guarding Against the Financial Exclusion of Bailiwick Residents

~~36.~~45. There may be occasions when a *Bailiwick* resident natural person encounters difficulties in providing evidence of his or her *Bailiwick* residential address using the sources identified previously in this Chapter. Examples of such circumstances include:

(a) a Short-Term Employment Permit holder who does not have a permanent residential address in *the Bailiwick*;

Chapter 6
Digital & Physical Certification and Electronic ID&V

Contents of this Chapter

6.1. Introduction

1. Certification is the process whereby, instead of a natural person presenting his/her self and *identification data* in person to the firm, the individual uses a suitable trusted third party to confirm a positive link between his/her identity and *identification data*. The certified *identification data* is then provided to the firm as verification of that natural person's identity.

2. The use of third party certification serves to mitigate the *risk* arising from a *business relationship* or *occasional transaction* where the firm has had no face-to-face contact with a natural person who is a *key principal* within that relationship. It also guards against the risk that *identification data* provided is fraudulent or misleading and does not correspond to the individual whose identity is to be verified.

3. Certification has two purposes:

   (a) to provide assurance to the firm that a natural person is who he or she purports to be; and
   (b) to confirm that the natural person is the owner of the *identification data* used for the purpose of the firm verifying identity.

4. Until recently, certification has required that trusted third parties are natural persons of sufficient professional standing and subject to appropriate ongoing requirements in respect of their integrity. However, with developments in technology the trusted third party could now take the form of an electronic system which, through the integration of controls such as those detailed later in this Chapter, can provide sufficient corroboration equivalent to that provided by a natural person certifier.

5. This Chapter is split into three sections and provides distinct requirements for certification depending upon the method of certification to be used:

   (a) natural persons certifying hard-copy *identification data*;
   (b) natural persons ~~electronically~~ certifying scanned *identification data* by the application of a digital signature; and
   (c) electronic methods of certifying *identification data*.

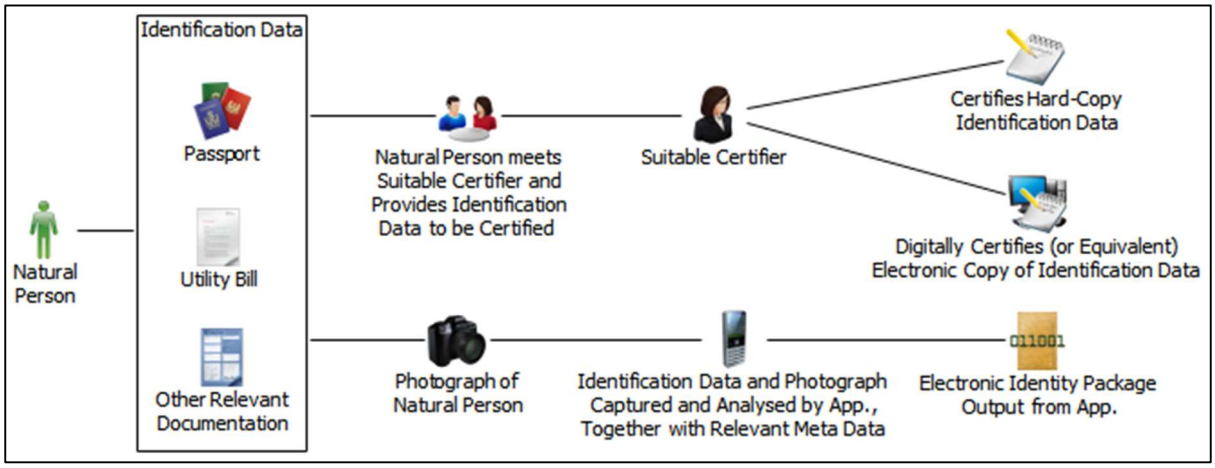


Fig. 2, Process of Certification

6.2. Obligations

6. For certification to be effective, the certifier should be a trusted third party who, in the case of natural person certification, has seen the original *identification data* and, where that *identification*

data includes a photograph, met the individual in person. Only following these two steps can the certifier provide the necessary assurance to the firm about the individual's identity.

7. In order to ensure this effectiveness, the firm should have as part of its compliance arrangements:

   (a) a policy and/or procedures which reflect the firm's *risk* appetite towards relying upon certified *identification data*;
   (b) a policy in relation to those third parties considered by the firm to constitute suitable certifiers; and
   (c) procedures allowing for the firm to verify the suitability of those third parties who have certified *identification data* upon which the firm intends to rely.

8. The firm must exercise caution when accepting certified *identification data*, especially where such *identification data* originates from a country or territory perceived to represent a high *risk*, or from unregulated entities in any country or territory.

6.3. Requirements for Natural Person Certifiers

9. Whilst there is no specific wording to be used by the certifier, the firm must ensure that the certifier signs and dates the certification and provides sufficient information within the certification or accompanying the certificaton for the firm to confirm the following:

   (a) that ~~he/she~~the certifier has seen the original *identification data* verifying identity or residential address;
   (b) that ~~he/she~~the certifier has met the natural person who is the subject of the *identification data;* and
   (c) adequate information about the certifier in order that the firm can undertake the required assessment of the suitability of the certifier and so that contact can be made with the certifier in the event of a query.

10. The certification should be provided by the certifier either on a copy of the *identification data* which is the subject of the certification or attached to that *document* by way of a covering letter or other record which accompanies the *identification data*. Where information in *Commission Rule* 6.9 above has not been provided on, or attached to, the *identification data*, it can be supplemented, for example by additional correspondence with the certifier, without the need to obtain renewed copies of the *identification data*. In this case, the additional correspondence forms part of the *CDD information* and the respective record-keeping requirements should be applied.

11. For the purposes of *Commission Rule* 6.9.(c) 'adequate information' should include:

   (a) the full name of the certifier;
   (b) the professional position or capacity held by the certifier (including professional body membership details where relevant); and
   (c) details of at least one contact method (for example, postal address, contact telephone number and/or e-mail address).

12. Certification by a natural person can take two forms;

   (a) paper-based certification where the certification is stamped or written onto a photocopy of the *identification data* or attached thereto; or
   (b) ~~electronic certification~~ where hard-copy *identification data* is scanned and certified ~~electronically by~~by application of a digital signature from the natural person to an electronic copy of the *identification data*.

13. The process for utilising a digitally signed electronic ~~certification as set out in Paragraph 6.12.(b) above~~copy of *identification data* which certifies its authenticity mirrors that for paper-based documentation as set out in Paragraph 6.12.(a) above. If the certifier accepts the *identification data* presented by the *customer*, then using digital encryption or a suitably robust alternative, the certifier will apply a digital signature (or equivalent) to an electronic copy of the *identification data*. This encrypted file is then provided electronically to the firm. This is as acceptable as a "wet-ink"or physical signature.

14. Where the firm utilises a system allowing for natural persons to certify by digital signature an electronic copy of the *identification data* ~~electronically~~, or otherwise receives electronic copies of *identification data* which has been certified by a natural person ~~electronically~~using a digital signature , it must *satisfy* itself as to the veracity of the certification process prior to accepting *identification data* certified in such a manner.

15. Where the firm wishes to accept soft-copy certified *identification data*, the preference should be to receive digitally certified (or equivalent) *identification data* using the process set out in Paragraphs 6.12.(b) to 6.14. above. However, there may be situations where the certifier does not have access to such technology, or is otherwise unable to digitally certify *documents*, and where the provision of hard-copy documentation via the postal system is unfeasible or uneconomical.

16. Where the firm receives *identification data* covered by Paragraph 6.12.(a) in scanned soft-copy form, the firm must be *satisfied* as to the veracity of the *identification data* provided and that the receipt of such *identification data* in soft-copy form does not pose an increased *risk* to the firm.

17. In *satisfying* itself as to the veracity of the scanned soft-copy *identification data* received, the firm should consider, amongst other factors, the type of *identification data* used (for example, is it known to be easily manipulated) and the source of the document(s) received (for example, were they provided by the subject of the *identification data*, or by an independent source such as the certifier or a representative thereof).

6.4. Assessing the Suitability of Natural Person Certifiers

18. Where copy *identification data* certified by ~~a natural person~~digital or physical signature is accepted, regardless of the manner or form of the *identification data*, the firm must *satisfy* itself that the certifier is a suitable and appropriate person to provide validation of the *identification data* based on the assessed *risk* of the *business relationship* or *occasional transaction*, together with the level of reliance being placed on the certified *documents*.

19. The firm should, as part of its compliance arrangements, have in place a policy which enables it to determine whether an individual is suitable to certify *documents* and therefore whether reliance can be placed upon the certified *identification data* provided. The policy should take account of factors including whether the certifier:

(a) is closely related or otherwise connected to the person whose identity is being certified;
(b) holds an appropriate public position with a high level of trust and for which background checks or similar vetting of the certifier's fitness and propriety will have been undertaken;
(c) is a member of a professional body which undertakes independent oversight of compliance with its own rules or standards of professional conduct;
(d) is required to satisfy criteria similar to the 'fit and proper' requirements of the minimum licensing criteria in *the Bailiwick* and is required to be vetted or approved as part of the regulation in the jurisdiction in which it operates;
(e) is employed by another business forming part of a group of which the firm is also a member where the same or equivalent AML and CFT policies, procedures and controls apply; or

(f) is subject to other professional rules or a member of an industry body (or equivalent) providing for the integrity of the certifier's conduct.

20. The firm's policy for assessing the suitability of a certifier should include consideration of the circumstances where the firm deems it appropriate to validate the credentials of the certifier.

21. As part of the steps taken to validate the credentials of a certifier, the firm may also include the consideration of factors such as:

(a) the reputation and track record of the certifier;
(b) the firm's previous experience of accepting certified *documents* from persons in the same profession or country or territory;
(c) the adequacy of the framework to counter *ML* and *FT* applicable in the country or territory in which the certifier is located; and
(d) the extent to which the framework applies to the certifier.

6.5. Certification Requirements for Copies of Identification Documents Verified Through Electronic System Certifiers

[An unmarked version of this section is two pages overleaf]

~~22.~~ In addition to ~~the traditional paper-based method of identity verification, the firm can also utilise electronic means~~accepting copies of ~~gathering natural person~~ identification data~~, details of which are provided in~~ certified by digital or physical signature in accordance with the aforementioned rules in this Chapter, the firm may also accept copies of identification data which have been certified as a true copy by a regulated firm which has verified the person through an electronic verification system. Sections 5.6. and 5.7. of this *Handbook*~~.~~

~~23.~~22. ~~As technology has evolved and software enhanced, greater controls have been incorporated into the validation process which have effectively negated the need for natural person certification. These~~ provide more detail about an electronic ~~controls can provide an equally robust confirmation of~~ verification system's role in verifying a natural person's identity~~, together with the corroboration between the natural person and the *identification data* used, and examples include:~~.

~~(a) a requirement for photographs to be taken at the time of the system's use (for example, the App takes control of the device's camera and automatically captures images of the~~ A firm may accept copies of identification data ~~and natural person);~~
~~(b) the inclusion of anti-impersonation measures (for example, a requirement for the natural person to verbally repeat words, phrases or passcodes dictated by the firm during a video call);~~
~~(c) the corroboration of the images within~~certified as a true copy of the original *identification data* ~~(both physically and/or stored on the Radio Frequency Identification ("RFID") chip), together with a self-taken photograph of the natural person;~~
~~(d) a process whereby the images taken are independently verified, either by a suitably trained individual or computer system, to confirm the authenticity of the~~from a firm which is subject to AML/CFT supervision by a competent authority, provided that the firm providing the copy *identification data* ~~used to verify identity (for example, that the *identification data*~~certifies that the natural person is its customer or a *key principal* of its customer and that the certifying firm has ~~not been fraudulently altered, is listed on a missing/stolen *documents* list, etc.);~~
~~(e) the corroboration of biometric information (for example, finger prints, voice identification, etc.); and/or~~

~~6.~~23. ~~geotagging/geolocation (i.e. the inclusion of geographical identification metadata to confirm the location in which the user interacted with the~~downloaded the document from an electronic verification system~~).~~ which it uses.

24. ~~Where the firm adopts a system providing for the electronic verification of natural person identity, the firm must assess the veracity of the controls inherent within the system in order to determine whether the firm can place reliance on the results produced, or if additional steps are necessary to complement the existing controls.~~The firm must establish that the certifying firm is supervised for compliance with AML/CFT measures. There is no specific wording for the certification, but it must be sufficient to ascertain that:

a) the natural person is a customer or *key principal* to a customer of the certifying firm;
b) the document is a true copy of the identification data verified by the electronic verification system the certifying firm uses; and
~~x)~~c) the copy of the *identification data* has been downloaded from an electronic verification system used by the certifying firm.

~~25. The additional steps undertaken by the firm could include:~~

~~(a) requiring a representative of the firm to be present with the natural person when the on-boarding software is being used; and/or~~
~~(b) issuing each relevant natural person with a code or similar unique identifier which is then included within the photographs taken of the natural person and/or *identification data*.~~

6.6. Certification of Documentation for Legal Persons and Legal Arrangements

~~26.~~25. Where the firm is provided with *documents* to verify the identity of a *legal person* which are copies of the originals, the firm must ensure they have been certified by the company secretary, director, manager or equivalent officer, or by a suitable third party certifier.

~~27.~~26. Where the firm is provided with *documents* to verify the identity and legal status of a *foundation* which are copies of the originals, the firm must ensure they are certified by a *foundation official* or by a suitable third party certifier.

~~28.~~27. Where the firm is provided with *documents* to verify the identity and legal status of a trust or other *legal arrangement* which are copies of the originals, the firm must ensure they are certified by a representative of the trustee (or equivalent) or by a suitable third party certifier.

~~29.~~28. Certification should be provided in a similar form to that set out under Section 6.3. of this Chapter, either through the certifying of a hard-copy *document*, or through the use of a digital signature (or equivalent) applied to an electronic copy of the *document*.

~~30.~~29. While there are no specific requirements in respect of the wording used, the firm must *satisfy* itself that the natural person certifying the *document* is a suitable and appropriate person within the specific circumstances of the *business relationship* or *occasional transaction*.

6.7. Chains of Physical Copy Certified Documentation

~~31.~~30. As detailed previously, the acceptance of original *identification data*, or *identification data* which has been certified in accordance with this Chapter, serves to protect the firm from the *risk* of it relying upon *identification data* which is fraudulent or misleading, or which does not correspond to the individual whose identity is to be verified. The benefits of this mitigation are limited, however, where *documents* have passed through a chain of certifiers (for example, other *FSBs*) and the link between the *customer* (or other *key principal*) and the firm has become distant.

~~32.~~31. Noting this concern, the firm should not place reliance upon copies of certified copies of original *identification data*, other than in justifiable instances. The firm should always consider the risk

Clean Version of Section 6.5 on Certification Requirements for Copies of Identification Documents Verified Through Electronic System Certifiers

20. The firm's policy for assessing the suitability of a certifier should include consideration of the circumstances where the firm deems it appropriate to validate the credentials of the certifier.

21. As part of the steps taken to validate the credentials of a certifier, the firm may also include the consideration of factors such as:

    (a) the reputation and track record of the certifier;
    (b) the firm's previous experience of accepting certified *documents* from persons in the same profession or country or territory;
    (c) the adequacy of the framework to counter *ML* and *FT* applicable in the country or territory in which the certifier is located; and
    (d) the extent to which the framework applies to the certifier.

6.5. Certification Requirements for Copies of Identification Documents Verified Through Electronic System Certifiers

22. In addition to accepting copies of identification data certified by digital or physical signature in accordance with the aforementioned rules in this Chapter, the firm may also accept copies of identification data which have been certified as a true copy by a regulated firm which has verified the person through an electronic verification system. Sections 5.6. and 5.7. of this *Handbook* provide more detail about an electronic verification system's role in verifying a natural person's identity.

23. A firm may accept copies of identification data certified as a true copy of the original *identification data* from a firm which is subject to AML/CFT supervision by a competent authority, provided that the firm providing the copy *identification data* certifies that the natural person is its customer or a *key principal* of its customer and that the certifying firm has downloaded the document from an electronic verification system which it uses.

24. The firm must establish that the certifying firm is supervised for compliance with AML/CFT measures. There is no specific wording for the certification, but it must be sufficient to ascertain that:

    a) the natural person is a customer or *key principal* to a customer of the certifying firm;
    b) the document is a true copy of the identification data verified by the electronic verification system the certifying firm uses; and
    c) the copy of the *identification data* has been downloaded from an electronic verification system used by the certifying firm.

6.6. Certification of Documentation for Legal Persons and Legal Arrangements

25. Where the firm is provided with *documents* to verify the identity of a *legal person* which are copies of the originals, the firm must ensure they have been certified by the company secretary, director, manager or equivalent officer, or by a suitable third party certifier.

26. Where the firm is provided with *documents* to verify the identity and legal status of a *foundation* which are copies of the originals, the firm must ensure they are certified by a *foundation official* or by a suitable third party certifier.

27. Where the firm is provided with *documents* to verify the identity and legal status of a trust or other *legal arrangement* which are copies of the originals, the firm must ensure they are certified by a representative of the trustee (or equivalent) or by a suitable third party certifier.

of placing reliance upon copies of certified copies of *identification data* and consider whether it would be more appropriate to obtain the original, or original certified copies of, *identification data*.

32. For the purposes of Paragraph 6.31. above, examples of justifiable instances include:

(a) the provision of copies of *identification data* held by the trustee of a trust in respect of the *beneficial owners* of that trust to a *bank* for the purposes of opening an *account* on behalf of that trust; or

(b) the provision of copies of *identification data* held by an *Appendix C business* to a legal professional engaged by the *Appendix C business* to provide advice in connection with a *customer* of, and at the request of, the *Appendix C business*.

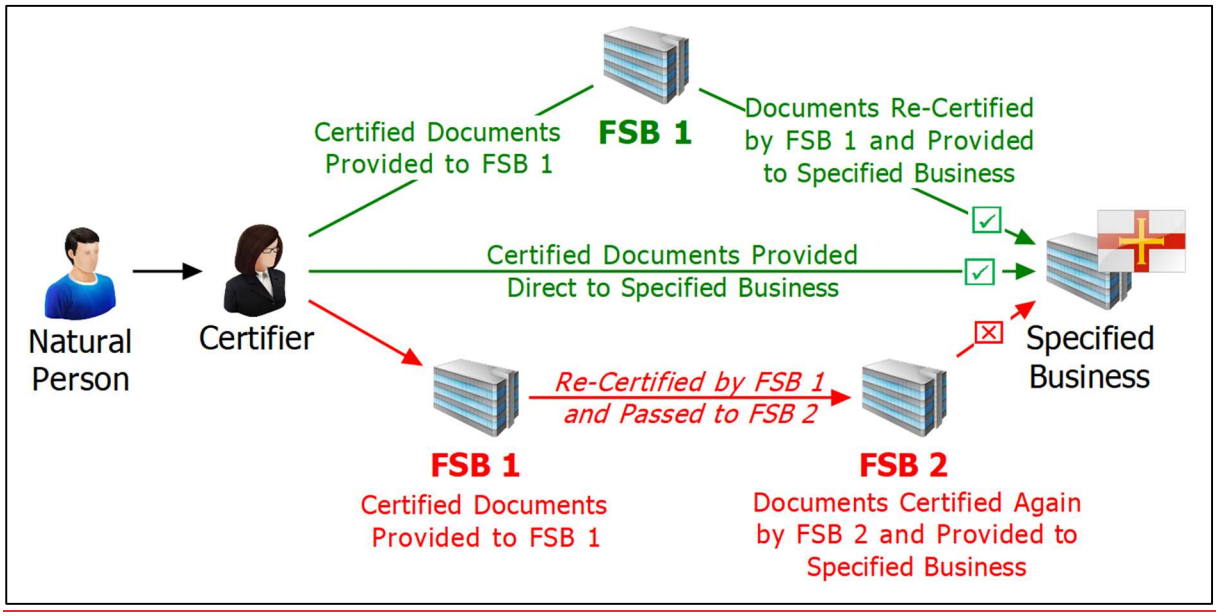


Fig. 3, Chains of Certification

33. Where the firm accepts copies of certified copy *identification data*, the following criteria must be met:

(a) the copy *identification data* has been provided by an *Appendix C business*;

(b) the *Appendix C business* has confirmed that the copy provided is a true copy of the *identification data* which it holds;

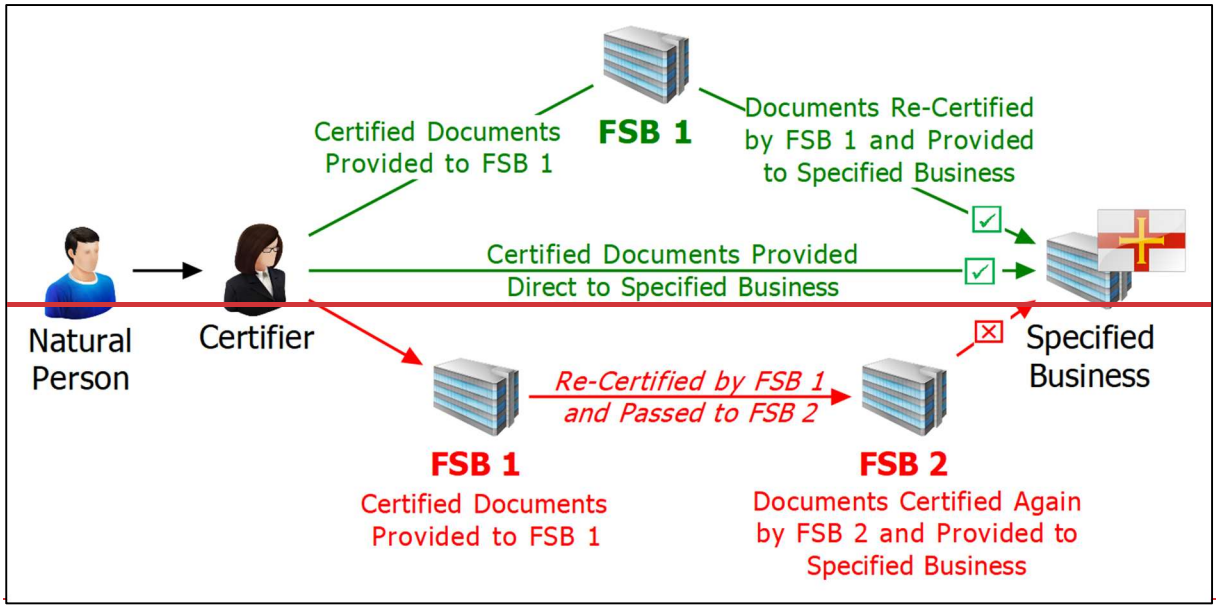
(c) the *Appendix C business* has seen the original *identification data* that it has copied to the firm, or the *identification data* that has been copied to the firm was provided to the *Appendix C business* by a suitable certifier, and in the case of the latter, the firm is *satisfied* that the individual who certified the *identification data* accepted by the *Appendix C business* which it is copying to the firm would qualify as a suitable certifier under the firm's policies and procedures; and

(d) where the *identification data* copied by the *Appendix C business* to the firm relates to the verification of a natural person's identity, the firm is *satisfied* that the copy *identification data* provides evidence that the natural person is who he or she is said to be.

~~34.1. For the purposes of Paragraph 6.32. above, examples of justifiable instances include:~~

~~(a) the provision of copies of *identification data* held by the trustee of a trust in respect of the *beneficial owners* of that trust to a *bank* for the purposes of opening an *account* on behalf of that trust; or~~

~~(b)~~(a) ~~the provision of copies of *identification data* held by an *Appendix C business* to a legal professional engaged by the *Appendix C business* to provide advice in connection with a *customer* of, and at the request of, the *Appendix C business*.~~



~~Fig. 3, Chains of Certification~~

~~35.~~34. For the avoidance of doubt this Section does not apply in respect of *business relationships* or *occasional transactions* falling within the introduced business provisions of Chapter 10 of this *Handbook* or where the firm acquires a business or block of *customers* in accordance with Paragraph 4.46. of this *Handbook*. In such circumstances, the firm places reliance upon a third party to have applied *CDD* measures to a *customer, beneficial owner* or other *key principal* in accordance with its own policies, procedures and controls. As such, the firm may accept copies of certified copy documentation either as part of the testing of that third party or through its acquisition of a block of *customers*.

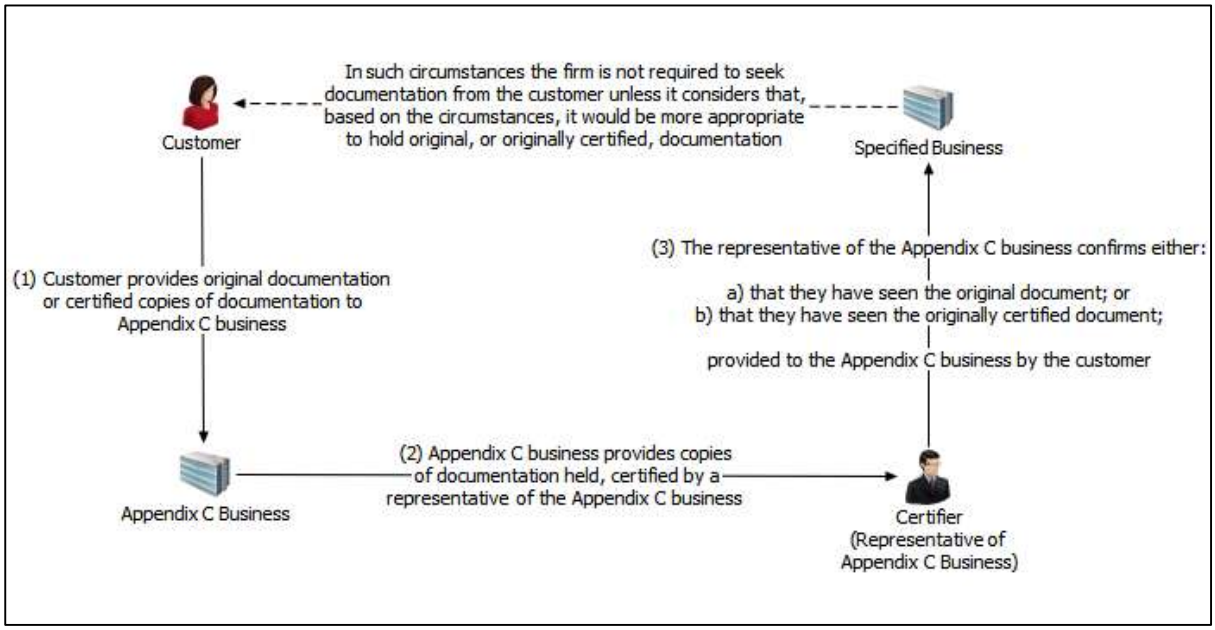


Fig. 4, Flow of Copy Certified Documentation

Obtaining beneficial ownership information from a beneficial ownership register maintained by a company registry or other public sector agency is not a substitute for applying *CDD measures* to establish beneficial ownership and control, however these registers may be useful as an additional source to validate, or otherwise confirm, a firm's understanding of the ownership and control structure of the customer if the firm has doubts.

7.5. Legal Bodies Listed on a Recognised Stock Exchange

In accordance with Paragraph 4(4) of *Schedule 3*, the firm shall not be required to identify any shareholder or *beneficial owner* in relation to:

(a) a *customer*, and
(b) a person which ultimately controls a *customer*,

that is a company listed on a recognised stock exchange within the meaning of *the Beneficial Ownership Regulations*, or a majority owned subsidiary of such a company.

Beneficial Ownership (Definition) Regulations, 2017, as amended

In order for the firm to consider the company as the principal to be identified, it must obtain *documentation* which confirms that the company is listed on a recognised stock exchange.

For the purposes of Paragraph 4(4) of *Schedule 3* and *Commission Rule* 7.58. above, in accordance with *the Beneficial Ownership Regulations* the following are deemed to be recognised stock exchanges:

(a) any regulated market within the meaning of the European Directive on Markets in Financial Instruments 2004/39/EU;
(b) the International Stock Exchange Authority Limited;
(e) the Australian Securities Exchange;
(f) the New York Stock Exchange;
(g) the National Association of Securities Dealers Automated Quotation System;
(h) the Cayman Islands Stock Exchange;
(i) the Bermuda Stock Exchange;
(j) the Hong Kong Stock Exchange;
(k) the Johannesburg Stock Exchange;
(l) the SIX Swiss Exchange;
(m) the London Stock Exchange Main Market, including the Alternative Investment Market and the Specialist Fund Segment;
(n) the Cboe Europe Equities Regulated Market; and
(o) Aquis Stock Exchange Limited.

EU Markets in Financial Instruments Directive 2004

7.6. Protected Cell Companies

A protected cell company ("PCC") is a single legal entity with one board of directors and one set of memorandum and articles of incorporation. A PCC can create an unlimited number of protected cells ("PCs"), the assets and liabilities of which are separate from those of the PCC (with the assets of the latter referred to as "non-cellular" or "core"). Importantly, the PCs are not separate legal entities and therefore cannot transact as such.

The *CDD* measures to be applied to a PCC authorised or registered by *the Commission* as a CIS under Section 8 of *the POI Law* where it acts as a *key principal* to a *business relationship* or *occasional transaction* are set out in Section 9.5. of this *Handbook.*

The *CDD* measures for PCCs which are licensed under the Insurance Business (Bailiwick of Guernsey) Law, 2002 as amended ("*the IB Law*") and where the *beneficial owner* of the relevant PC or PCC is a business which is listed on a recognised stock exchange within the meaning of *the Beneficial Ownership Regulations* (or by a majority owned subsidiary of such a listed business) are the same as those set out in Section 7.5. of this *Handbook.*

66.67.

67.68.

7.7. Incorporated Cell Companies

An incorporated cell company ("ICC") is structured similarly to a PCC with a non-cellular core and an unlimited number of cells ("ICs"). However, in contrast, the ICs of an ICC are separately incorporated and are therefore distinct legal entities with their own memorandum and articles of incorporation and boards of directors.

68.69.

It is of note that whilst the boards of the ICC and the boards of the ICs ~~must~~ are not required to be identically composed, ~~so any~~at least one director of ~~an ICC~~each of the ICs must also be a director of ~~each of its ICs~~ the ICC.

69.70.

Similar to a PCC, the assets and liabilities of each IC are segregated from the assets and liabilities of the ICC and from the assets and liabilities of the other ICs. While an IC can hold its own assets, those assets cannot include shares in its own ICC.

70.71.

As a result of each IC having separate legal personality, the ICs have the ability to contract with third parties and with other ICs in their own right. An IC must therefore contract in respect of its own affairs and the ICC has no power to enter into transactions on behalf of any of its ICs. Each IC can also have distinct *beneficial owners*.

71.72.

72.73.

Where an ICC or IC is a *key principal* to a *business relationship* or *occasional transaction*, the firm must apply *CDD* measures to the relevant ICC or IC, and to the *beneficial owners* thereof, in accordance with the requirements for *legal persons*.

73.74.

The *CDD* measures to be applied to an ICC or IC authorised or registered by *the Commission* as a CIS under Section 8 of *the POI Law* where it acts as a *key principal* to a *business relationship* or *occasional transaction* are set out in Section 9.5. of this *Handbook*.

74.75.

The *CDD* measures for ICs or ICCs which are licensed under *the IB Law* and where the *beneficial owner* of the relevant IC or ICC is a business which is listed on a recognised stock exchange within the meaning of *the Beneficial Ownership Regulations* (or by a majority owned subsidiary of such a listed business) are the same as those set out in Section 7.5. of this *Handbook.*

75.76.

7.8. Limited Partnerships and Limited Liability Partnerships

76.77.

An LP is a form of partnership with or without legal personality at the election of the GP. Its members include one or more GP, who has actual authority over the LP, for example to bind the LP in contracts with third parties, and is liable for all debts of the LP, and one or more limited partner who contributes (or agrees to contribute) to the capital of the LP and who (subject to certain provisions) is not liable for the debts of the LP.

A Limited Liability Partnership ("LLP") is a body corporate with legal personality separate from that of its members and is therefore liable for its own debts. As a consequence of this legal personality, LLPs established within *the Bailiwick* must be registered and therefore public records

(C) obtaining additional information to understand the purpose and intended nature of each *business relationship* and *occasional transaction*, and
(D) taking reasonable measures to establish and understand the source of wealth of *beneficial owners* not falling within Paragraph 5(3)(iii).

8. Examples of steps the firm could take in accordance with Paragraphs 5(3)(v)(A)-(D) of Schedule 3 could include:

(a) supplementing the firm's understanding of the purpose and intended nature of the *business relationship* by obtaining information on the reasons for intended or performed transactions;
(b) commissioning independent research by a specialist firm or consultant, pertaining to the purpose and objective of the *business relationship* or *occasional transaction* and evidencing information in relation to the *customer* and/or the *beneficial owner*;
(c) where the *customer* is a *legal person*, identifying, and verifying the identity of, other directors (or equivalent) of the *customer* in addition to those senior managing officials identified as *beneficial owners* in accordance with Step 3 of Paragraph 7.36. of this *Handbook* and/or those natural persons acting on behalf of the *customer* captured by Section 4.3.2.; ~~and/or~~
(d) obtaining internal information from group representatives or offices based in a jurisdiction where the *customer* has a connection~~.~~; and/or
(e) using AI to identify credible independent references about the *customer* or *beneficial owner* for the firm's due diligence considerations to draw on.

9. In addition to the requirements of Paragraph 5(3) of *Schedule 3* as set out above, listed below are examples of further steps the firm could take as part of its *ECDD* measures to address specific *risks* arising from a *high risk relationship*:

(a) in the case of an existing *business relationship* which has, following a *relationship risk assessment*, been assessed as high *risk* not involving a *foreign PEP*, obtaining senior management approval for continuing that relationship; and/or
(b) requiring the first payment be carried out through an *account* in the *customer's* name with an *Appendix C business*.

8.2.2. Enhanced Measures (Higher Risk Factors)

10. In accordance with Paragraph 5(2) of *Schedule 3*, the firm's policies, procedures and controls must require the application of *enhanced measures* as detailed in Sections 8.9. - 8.12. of this *Handbook* to *business relationships* and *occasional transactions* involving or in relation to one or more of the higher *risk* factors in Paragraph 5(2)(a)-(d) of *Schedule 3*.

11. There may be a *business relationship* or *occasional transaction* which involves or is in relation to more than one of the higher *risk* factors set out in Paragraph 5(2)(a)-(d) of *Schedule 3* (for example, a non-resident *customer* using private banking services). In such cases, the firm must apply *enhanced measures* sufficient to mitigate each of the higher *risk* factors present within the *business relationship* or *occasional transaction*.

8.2.3. ECDD and Enhanced Measures (High Risk Relationships with Higher Risk Factors)

12. There may also be circumstances in which a *high risk relationship* involves or is in relation to one or more of the higher *risk* factors in Paragraph 5(2)(a)-(d) of *Schedule 3*. In such cases the firm must apply *ECDD* measures as well as applying sufficient *enhanced measures* to mitigate the particular higher *risk* factor(s) present.

in a *business relationship* or *occasional transaction*, together with its overall assessed *risk*. Such *risk* factors include, inter alia, the value of the *customer's* or *beneficial owner's* assets, together with the value of the *funds* involved in the *business relationship* or *occasional transaction*, the type and complexity of the *customer* or *beneficial owner*, the *customer's* or *beneficial owner's* economic activity and employment, and the nature of the services provided by the firm.

22. Information on the source of *funds* and wealth will generally be obtained from the *customer* or *beneficial owner* in the first instance and the extent to which this is corroborated through additional information or documentation should be commensurate with the *risk*. The firm may have a *business relationship* where it can establish to its satisfaction the source of *funds* and source of wealth from the *customer* or *beneficial owner* without seeking to corroborate that information because it is consistent with the knowledge the firm holds about the *business relationship* or *occasional transaction* and because the values involved are relatively low and commensurate with the type of product or service being provided by the firm.

23. For example, the firm may have a natural person *customer* located in a higher *risk* jurisdiction utilising its products or services for a relatively small amount of *funds* and where the firm has determined that the only factor making it a *high risk relationship* is geographic *risk*. In such a case placing reliance upon the information provided by the *customer* on the source of *funds* and wealth as part of the firm's *ECDD* measures could be considered 'reasonable' because it is consistent with the information and knowledge it has built up about the *customer* through *CDD* measures, together with the other elements of its *ECDD* measures and the *enhanced measures* applied because the *customer* is not resident in *the Bailiwick*.

24. On the other hand, 'reasonable measures' will require corroborating information where the *customer* or *beneficial owner* is from a higher *risk* country or territory, where the values involved in the *business relationship* or *occasional transaction* are large and where the sources of *funds* and wealth are not easily discernible from the *customer's* or *beneficial owner's* disclosed income and business interests.

25. The extent to which the firm corroborates the information provided by the *customer* or *beneficial owner* on the source of *funds* and wealth is a function of *risk* and not a 'one size fits all' approach. Where corroboration of the information provided by the *customer* or *beneficial owner* is required, the firm could consider one or more of the means set out in the following non-exhaustive list:

(a) commissioning an independent and reliable report from a specialist agency;
(b) obtaining certified copies of corroborating documentation such as contracts of sale, property deeds, salary slips, etc.;
(c) where the firm is part of a group, obtaining reliable information from another member of the group with which the *customer* or *beneficial owner* has a connection~~;~~
(d) where the source of funds or source of wealth include virtual assets, using blockchain analysis products or services from a reliable commercial vendor;
~~(d)~~(e) obtaining information from a reliable third party (for example, a professionally qualified solicitor, accountant or tax advisor) who has an office in a country or territory connected with the *customer* or *beneficial owner*;
~~(e)~~(f) where the *customer* has been introduced to the firm, obtaining information from the *introducer*;
~~(f)~~(g) where information is publicly available, whether identified through online searches, through searches by AI, or available through subscription ~~databases~~services, obtaining information from a reliable public or private third party source; or
~~(g)~~(h) obtaining information from financial statements that have been prepared and audited in accordance with generally accepted accounting principles.

26. It would not be considered sufficient for the firm to accept a *customer's* or *beneficial owner's* responses on an application form at face value, particularly where vague answers are given (for

15. The firm must identify, and verify the identity of, *the Bailiwick* public authority, including as a minimum:

(a) the full name of the public authority;
(b) the nature and status of the public authority;
(c) the address of the public authority; and
(d) the names of the directors (or equivalent) of the public authority.

16. The following are examples of *Bailiwick* public authorities:

(a) a government department;
(b) an agency established by law;
(c) a parish authority/douzaine; and
(d) a body majority owned by an authority listed in points (a) to (c) above.

17. Where a natural person authorised to act on behalf of a *Bailiwick* public authority is acting in the course of employment, it is not necessary to identify and verify the identity of that person. However, the firm should verify the natural person's authority to so act.

18. It may be that an individual acting on behalf of a *Bailiwick* public authority falls within the definition of a *domestic PEP*. However, in the context of acting for *the Bailiwick* public authority, the individual is directing funds belonging to the authority and not their personal funds. The firm may therefore determine that the measures required under *Commission Rule* 9.15. are sufficient and that the prominent public function held by the natural person does not pose an increased *risk* to the firm in the context of the *business relationship* or *occasional transaction* with *the Bailiwick* public authority.

9.5. Collective Investment Schemes Authorised or Registered by the Commission

19. Where the *customer*, *beneficial owner* or other *key principal* to a *business relationship* or *occasional transaction* is a CIS authorised or registered by *the Commission*, the firm (other than where it has been nominated as the party responsible for applying *CDD* measures to investors in accordance with Section 4.8.1. of this *Handbook*) may consider the CIS to be the principal for the purposes of the firm's *CDD* measures.

20. Where this is the case, in verifying the identity of the CIS the firm must, as a minimum, obtain *documentation* which confirms the CIS is authorised or registered by *the Commission*.

21. Further information about CISs authorised and registered by *the Commission* can be found on *the Commission's* website:

https://www.gfsc.gg/industry-sectors/investment/regulated-entities

22. Where a natural person authorised to act on behalf of a CIS to which this Section applies is doing so in the course of employment with that CIS or its ~~Designated Manager~~designated administrator, it is not necessary to identify and verify the identity of that person. However, the firm should verify the person's authority to act on behalf of the CIS.

23. As an example, where a *bank* is opening an *account* for a CIS authorised or registered by *the Commission*, the *bank* may treat the CIS as the *customer* to be identified and verified.

(b) the *introducer* keeps such *identification data* and *documents*.

10. In accordance with Paragraph 10(2) of *Schedule 3*, the circumstances referred to in Paragraph 10.9. above are that the *introducer*:

(a) is an *Appendix C business*; or
(b) is either an overseas branch office of, or a member of the same group of *legal persons* or *legal arrangements* as, the firm, and

(i) the ultimate *legal person* or *legal arrangement* of the group of *legal persons* or *legal arrangements* of which both the *introducer* and the firm are members, is an *Appendix C business*; and
(ii) the conduct of the *introducer* is subject to requirements to forestall, prevent and detect *ML* and *TF* (including the application of any appropriate additional measures to effectively handle the *risk* of *ML* or *TF*) that are consistent with those in *the FATF Recommendations* in respect of such a business (particularly Recommendations 10, 11 and 12), and the *introducer* has implemented a programme to combat *ML* and *TF* that is consistent with the requirements of Recommendation 18; and
(iii) the conduct both of the *introducer*, and of the group of *legal persons* or *legal arrangements* of which both the *introducer* and the firm are members, is supervised or monitored for compliance with the requirements referred to in (ii) above, by *the Commission* or an overseas regulatory authority.

11. In addition to the confirmations required by Paragraph 10(1) of *Schedule 3*, when establishing an *introducer* relationship, the firm must also *satisfy* itself that the *introducer*:

(a) has appropriate *risk*-grading procedures in place to differentiate between the *CDD* requirements for *high risk relationships* and *low risk relationships*;
(b) applies appropriate and effective *CDD* measures to its *customers*, and the *beneficial owners* and other *key principals* thereof, including *ECDD* measures to *foreign PEPs* and other *high risk relationships*; and
(c) has appropriate record keeping requirements similar to those set out in Paragraph 14 of *Schedule 3*.

12. The *CDD* measures referred to in Paragraph 10(1) of *Schedule 3* include the following elements:

(a) identifying the *customer* and verifying the *customer's* identity using *identification data*; whether copied directly from the customer or collected through an electronic verification system used by the *introducer* to verify the customer;
(b) identifying any person purporting to act on behalf of the *customer* and verifying that person's identity and their authority to so act;
(c) identifying the *beneficial owner* and taking reasonable measures to verify the identity of the *beneficial owner*, including, in the case of a *customer* which is a *legal person* or *legal arrangement*, taking measures to understand the nature of the *customer*'s business and its ownership and control structure;
(d) determining whether the *customer* is acting on behalf of another person and, if the *customer* is so acting, taking reasonable measures to identify that other person and to obtain sufficient *identification data* to verify the identity of that other person; and
(e) understanding, and as appropriate obtaining information to support this understanding of, the purpose and intended nature of the *business relationship* or *occasional transaction*.

13. A template certificate which may be used by the firm for introduced business can be found in Appendix F to this *Handbook*.

14. The firm must take appropriate steps to be *satisfied* that the *introducer* will supply, immediately upon request, certified copies, evidence of electronically verified *identification data* or originals of the *identification data* and other relevant *documents* it has collected under the *CDD* measures applied to its *customers*, including the *beneficial owner* and other *key principals* thereof.

15. Where an introduced *business relationship* presents a high *risk* of *ML*, *TF* or *PF*, consideration should be given to whether it is appropriate for the firm to rely solely upon the information provided by the *introducer* or whether supplemental *CDD* information and/or *documentation* is required.

16. It is the responsibility of the *introducer* to inform the firm of any changes to the parties involved in an *introducer* arrangement, for example, to the relationship structure, the profile, or any *CDD* held. As part of establishing an introduced relationship the firm should seek confirmation from the *introducer* that it will notify the firm of changes to the *customer*, or the *beneficial owner* thereof, without delay.

10.4. Testing

17. The firm must have a scheduled programme of testing to ensure that, on an on-going basis, an *introducer* is able to fulfil the requirement that certified copy, evidence of electronically verified or original *identification data* that it has collected will be provided to the firm immediately upon request. This will involve the firm adopting ongoing procedures to ensure it has the means to obtain that *identification data*.

18. The testing programme should be *risk*-based and commensurate with the *risk* exposure, size and scope of the business introduced. The programme should provide appropriate and sufficient assurance to the firm that it can continue to rely upon an *introducer* to fulfil its obligation to provide *identification data* immediately upon request. In this respect, priority should be given to those *introducers* posing the highest *risk* to the firm, i.e. those with the greatest number of introduced relationships and/or the highest *risk customers*.

19. Notwithstanding the above, the firm should set a minimum timeframe within which all *introducers* will be subject to appropriate periodic testing and record this within its *introducer* testing procedure.

20. The scope of the testing undertaken should include verification that the information received from the *introducer* on a certificate or summary sheet containing information about the identity of the underlying *customer*, *beneficial owner* and other *key principals*, continues to be accurate and up to date. This allows the firm to determine whether, based on any changes, it wishes to continue to rely upon the arrangement or whether the firm may wish to seek further information from the *introducer* about the underlying *customer* and/or associated *key principals*.

21. Where, as a result of a test carried out, the firm is not *satisfied* that the *introducer* has appropriate policies and procedures in place, maintains appropriate records, or will provide evidence of those records immediately if requested to do so, the firm must apply *CDD* measures in accordance with Paragraph 4 of *Schedule 3* for that *customer*, including the *beneficial owner* and other *key principals* thereof, and give consideration to terminating its relationship with the *introducer*.

10.5. Termination

22. In the event that an *introducer* terminates its relationship with an introduced *customer*, the firm should consider how best it will continue to maintain compliance with its *CDD* obligations for that *customer* and associated *key principals*. In this respect, the firm should give consideration to the following:

(ii) to any *police officer*, the *FIU*, *the Commission* or any other person, where such *documents* or *CDD information* are requested pursuant to *Schedule 3* or any of *the Relevant Enactments*.

28. The firm must consider the implications for meeting the requirements of *Schedule 3* where *documentation*, data and information is held overseas or by third parties, such as under outsourcing arrangements, or where reliance is placed upon an *introducer*.

29. The firm must not enter into outsourcing arrangements or place reliance on third parties to retain records where access to those records is likely to be restricted.

30. Where the *FIU* or another domestic competent authority requires sight of records, either under *Schedule 3* or another of *the Relevant Enactments*, which according to the applicable procedures would ordinarily have been destroyed, the firm must nonetheless conduct a search for those records and provide as much detail to the *FIU* or other domestic competent authority as possible.

16.11. Manner of Storage

31. The record keeping requirements are the same regardless of the format in which the records are kept, or whether the transaction was undertaken by paper or electronic means.

32. Records may be retained:

(a) by way of original *documents*;
(b) by way of photocopies of original *documents* (certified where appropriate);
(c) on microfiche;
(d) in a scanned form; or
(e) in a computer or electronic form (including cloud storage or distributed ledger technology).

33. The use of technology to collect and/or store data and *documents* does not alter the obligations and requirements described in this *Handbook*.

34. Where the firm utilises an electronic method of gathering *identification data*, for example, an App. or other system as set out in Section 5.6. of this *Handbook* or a *CDD* Utility, the firm should include within its *risk* assessment of that technology an evaluation of the policy for the retention of *document*s. This evaluation should enable the firm to ensure that its use of the technology complies with the requirements of *Schedule 3* and this *Handbook* and that the firm will not incur legal evidential difficulties (for example, in civil court proceedings).

17. When transaction information is easily available on a public ledger or via other open sources, *VASP*s must still record and retain that information in accordance with Chapter 11 on monitoring transactions and activity.

18.4. Enhanced Customer Due Diligence

18. There are *ECDD* measures which can be undertaken in relation to *VA*s in addition to those already included within Chapter 8 on *enhanced customer due diligence*. Examples of additional steps the firm could take when meeting the requirements of Paragraphs5(3)(v)(A)-(D) of *Schedule 3* while undertaking *ECDD* in relation to *VA*s could include, but is not limited to, applying one or more of the following measures most relevant towards mitigating the *ML, TF* and/or *PF* risks:

    (a) corroborating the identity information received from the *customer*, such as a national identity number, with information in third-party databases or other reliable sources;
    (b) tracing the *customer*'s IP address;
    (c) using blockchain analysis products or services from a reliable commercial vendor;
    (d) using open source to corroborate activity information consistent with the *customer*'s transaction profile; and/or
    (e) collecting additional information on:
        i. the purpose of the transaction or payment;
        ii. details about the nature, end use or end user of the item;
        iii. proof of funds ownership;
        iv. parties to the transaction and the relationship between the parties;
        v. the identity and beneficial ownership of the counterparty; and
        vi. export control information, such as copies of export control or other licenses issued by a national export control authority, and end user certification.

18.5. Correspondent Banking and Other Similar Relationships

19. Correspondent banking (the provision of banking services by one *bank* to another *bank*) and other similar relationships do not include one-off transactions, but instead are characterised by their ongoing, repetitive nature. *VASP*s should define and assess the characteristics of their counterparty *VASP* relationships and ascertain whether they are undertaking activities similar to correspondent banking. Where it is established that a *VASP* is entering into a relationship that is similar to correspondent banking, it should adhere to the rules and guidance included within Section 8.6 of this *Handbook* on correspondent banking.

18.6. *Transfers*

20. *VASP*s are required to obtain, hold and submit required *originator* and beneficiary information associated with the *transfers* of *virtual assets* in order to identify and report suspicious transactions, take freezing actions and prohibit transactions with designated persons and entities. This is similar to the *wire transfer* requirements included within Chapter 14.

21. *The Commission* does not require a particular technology or software to be used to comply with the *transfer* rules. Any technology or software used must enable the *originator* and *beneficiary VASP*s to comply with their AML/CFT/CPF obligations.

22. The technology or software used should enable *VASP*s to comply with the *transfer* rules in an effective and efficient manner and enable *VASP*s to undertake the following actions:

    a) Enable a *VASP* to locate counterparty *VASP*s for *transfers* of virtual assets;

(vii) the circumstances in which the *customer* makes use of the 'cooling-off' period give rise to suspicion.
(viii) using multiple *accounts* without previous notification, especially when these *accounts* are held in multiple or high-*risk* jurisdictions.
(ix) the *customer* wishes to structure the relationship in such a way that multiple parties (for example, nominee companies) are used in different jurisdictions, particularly where these jurisdictions are associated with higher *ML, TF* and/or *PF risk*.

(b) the *customer's* nature, for example:

(i) the *customer* is a *legal person* or *legal arrangement* established in a jurisdiction associated with higher *ML, TF* and/or *PF risk*. The firm should pay particular attention to those jurisdictions that do not comply effectively with international tax transparency standards.
(ii) the *customer* is an investment vehicle that carries out little or no due diligence on its own clients.
(iii) the *customer* is an unregulated third party investment vehicle.
(iv) the *customer's* ownership and control structure is opaque.
(v) the *customer* or the *beneficial owner* holds a prominent position (other than a politically exposed position) that might enable them to abuse their position for private gain.
(vi) the *customer* is a non-regulated nominee company with unknown shareholders.

(c) the *customer's* business, for example, the *customer's funds* are derived from business in sectors that are associated with a high *risk* of financial crime.

37. The following factors may contribute to reducing *risk*:

(a) the *customer* is a government body from a country or territory listed in Appendix C to this *Handbook*.
(b) the *customer* is an institutional investor whose status has been verified by a government agency in a country or territory listed in Appendix C to this *Handbook*, for example, a government-approved pensions scheme.
(c) the *customer* is an *Appendix C business*.

Country or Geographical Risk Factors

38. The following factors may contribute to increasing *risk*:

(a) the investor or their custodian is based in a jurisdiction associated with higher *ML, TF* and/or *PF risk*.
(b) the *funds* come from a jurisdiction associated with higher *ML, TF* and/or *PF risk*.

Investment Fund Sector

39. The provision of CISs can involve multiple parties: the designated ~~manager/~~administrator, fund/principal manager, appointed advisers, the custodian/depositary and sub-custodians, registrars and, in some cases, prime brokers. Similarly, the distribution of these CISs can involve parties such as tied agents, advisory and discretionary wealth managers, platform service providers and independent financial advisers.

40. The type and number of parties involved in a CIS's distribution process depends on the nature of the CIS and may affect how much the *nominated firm* knows about the CIS' investors. In accordance with Section 4.6.1. of this *Handbook* the *nominated firm* retains responsibility for

Appendix F

Introducer Certificate

Name of Accepting Business:	
Name of Introducer:	
Account Name (in full):	
Details of Associated Account/s (which are part of the same structure):	

Introducer's Contact Details	
Address:	
Telephone:	
Fax:	
E-mail:	

The Introducer certifies that it is an Appendix C business and in respect of this account it has obtained and holds identification data equivalent to that required to satisfy the Handbook on Countering Financial Crime (AML/CFT/CPF) ("the Handbook") issued by the Guernsey Financial Services Commission, as updated from time to time.

The information disclosed for this account by the Introducer accurately reflects the information held and is being given for account opening and maintenance purposes only. The Introducer undertakes to keep the accepting business apprised of any changes to the information contained within this certificate and to supply copies of electronically verified, certified copies, or originals of the identification data upon request without delay.

Signature: _____ _____

Full Name: _____ _____

Official Position: _____ _____

Date: _____ _____

Please indicate the number of supplementary pages being submitted: IC2 ☐ IC3 ☐ IC4 ☐

Introducer Certificate IC5

Notes and Guidance

These notes and the definitions below are intended to assist the Introducer in completing the required forms and to enable greater consistency to be achieved.

Term	Definition
Associated accounts	Refers to an account with the same specified business where any of the principals are connected with an account in the same group or structure.
Account activity	An estimate of the total flow of funds in and out of the account should be provided. An estimate of the expected maximum account turnover should also be provided. For a trading operation, the scale and volume of transactions should be explained.
Bearer shares	Where bearer shares are subsequently issued (after the opening of the account) such that the "Yes" box needs ticking in IC2, an updated form should be supplied to the accepting specified business without delay.
Certified copy	An officer or authorised signatory of a regulated financial services business will be an acceptable certifier. An acceptable 'certified copy' document should be an accurate and complete copy of the original or electronic verification system document, such that the certifier will sign and date the copy document printing his position, capacity and company name.
Government issued personal identification number	Includes government issued personal identification number, for example a social security/ national insurance number, or other government issued unique identifier, for example a passport or driving licence number.
Handbook	The Handbook on Countering Financial Crime (AML/CFT/CPF) issued by the Guernsey Financial Services Commission, as updated from time to time.
Introducer	Is an Appendix C business (see definition in the Handbook).
Nature of activities or purpose and intended nature of business relationship	A sufficient description should be provided to enable the accepting specified business to properly categorise the underlying nature of the arrangements. If the activity is of a commercial nature, then additional information may be required.
PEP	A Politically exposed person, and includes such a person within the Bailiwick (domestic PEP) or any other jurisdiction ("foreign PEP"), as well as a person appointed with a prominent function by an international organisation. Further details about each can be found within Chapter 8 of the Handbook. The jurisdiction(s) associated with an individual's political exposure, either by a position held or any connection with a PEP, should also be provided.
Principal	Includes any person or other entity that has or is likely to receive a benefit in the foreseeable future or who the Introducer customarily treats as having an economic interest.
Role	This might include, for example, a beneficial owner, a shareholder, beneficiary, settlor, partner, etc.
Signatory	The General Introducer Certificate will need to be signed or initialled (where appropriate) in line with the Introducer's current mandate/authorised signatory list held with the accepting specified business.
Source of wealth	The origins of the wealth of the customer and any beneficial owner who is a PEP (and over what period) should be identified. Generally, simple one word answers will be unacceptable, for example, 'income', 'dividends', 'Bill Smith', or 'work'. A brief description to give a fuller picture is expected, for example, 'sale of UK private company in 1997', 'life time savings of settler who was a doctor', 'inheritance from parents' UK estate' and 'UK property development over the last 10 years'.
Specified business	A financial services business or a prescribed business in the Bailiwick of Guernsey.
Trading	Implies commercial activity which may include a business, invoicing or re-invoicing operations. For clarity, a 'trading company' does not include a personal service/employment company.

Please refer to the accepting specified business should you have any doubt or queries about completing this Introducer Certificate.