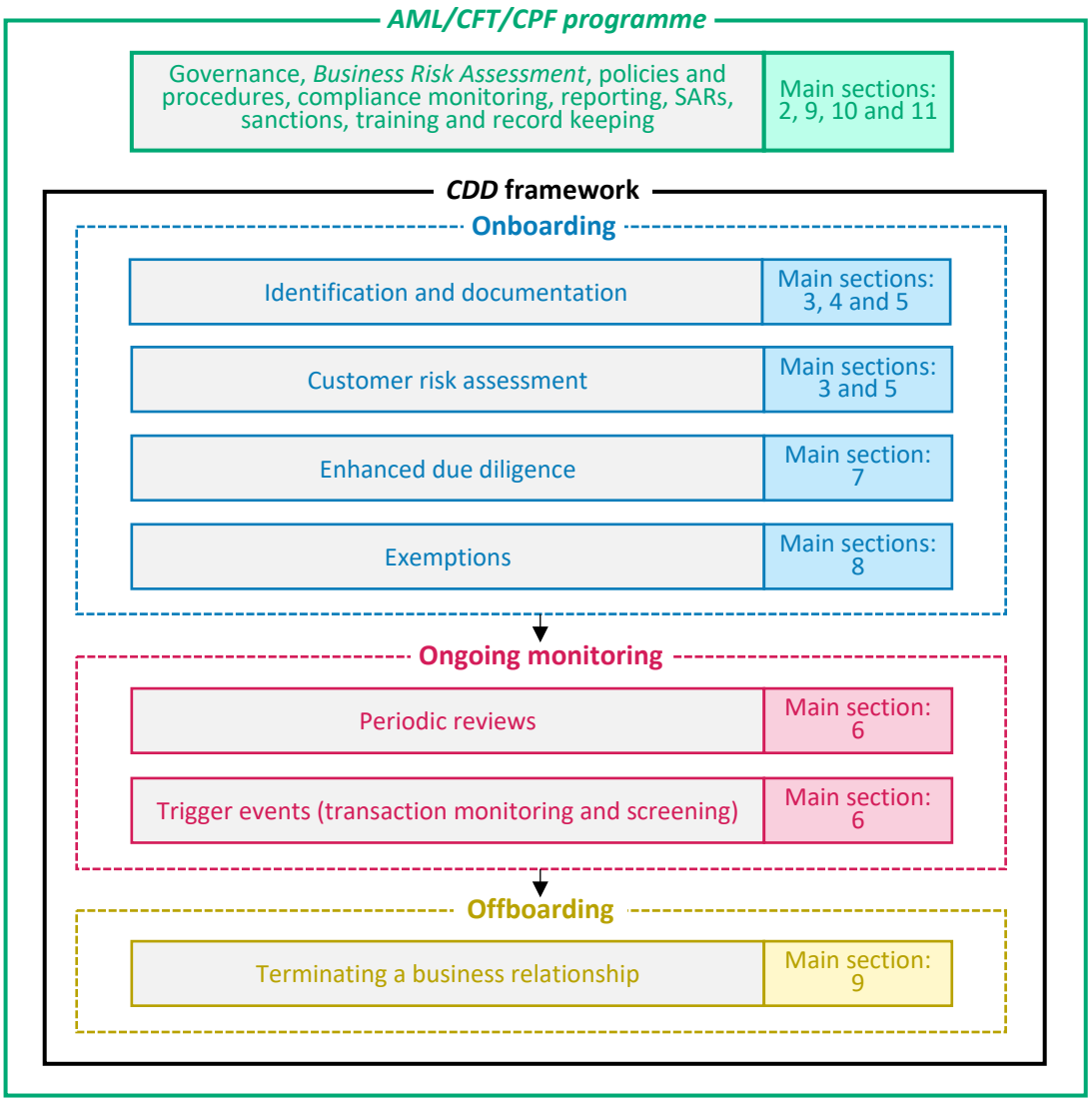
PART III: DESIGNATED NON-FINANCIAL BUSINESSES AND PROFESSIONALS (*DNFBPs*)

17 OBLIGATIONS OF NOTE FOR ALL *DNFBPS*

1. Sections 1-11 are applicable to all entities/sectors classified as *supervised persons* and sections 17 – 21 apply to specific *DNFBPs*. High level mapping of the sectors to key processes in an *AML/CFT/CPF* programme are outlined below, which forms the content outlined in 'Part I: General Guidance':



2. **Important note**: Sections 17.1 and 17.2 are not intended to be a complete list of obligations for all *DNFBP*s, they are included to provide additional details and guidance over specific areas of note. This does not supersede the obligations and guidance outlined in Sections 1 - 11 of *this Handbook* but is intended to provide enhanced guidance over specific obligations.

17.1 Timing of *identification measures*

Overview

3. This section is supplementary to and should be read in conjunction with section 4.7 of *this Handbook*.

4. This refers to finding out identity, and obtaining evidence of identity, for a business relationship or one-off transaction. This sits in wider *CDD* procedures which include amongst other activities: risk assessing, enhanced due diligence and ongoing monitoring.

5. Section 4.7 of *this Handbook* sets out statutory requirements under the *Money Laundering Order* regarding when *identification measures* must be applied, in respect of a *business relationship* or *one-off transaction*.

6. Article 13 of the *Money Laundering Order* requires a *supervised person* to apply *identification measures*:

- before the establishment of a *business relationship* or before carrying out a *one-off transaction*; and
- in the course of a *business relationship*, where the *supervised person* has doubts about the adequacy of information previously obtained under *identification measures*.

7. As noted in section 4.7 of *this Handbook*, Article 13(4) of the *Money Laundering Order* allows, in certain circumstances, a *supervised person* a reasonable timeframe to undertake the necessary enquiries for obtaining evidence of identity after the initial establishment of a business relationship. No similar concession is available for finding out identity. Where a reasonable excuse for the continued delay in obtaining evidence of identity cannot be provided; to comply with Article 14(2) of the *Money Laundering Order*, a *supervised person* must terminate the relationship (see section 4.8 of *this Handbook*).

17.1.1 Ongoing Monitoring

8. This section is supplemental to and should be read in conjunction with Section 6.

9. Where *supervised persons* are involved in longer matters, periodic reviews should be undertaken on a risk sensitive basis, to ensure no significant factors have changed. For example, new parties to the matter, change of ownership or control (including control by other means), new sources of funds, new beneficiaries.

17.1.2 Duration of relationship with a *customer*

10. This section is supplemental and should be read in conjunction with sections 1.6 and 3.2 of *this Handbook.*

11. A relationship is considered to be established as soon as a *supervised person* undertakes to act on instructions as to the operation of that relationship, for example, by receiving and accepting signed terms of business from the *customer*.

12. In the case of *real estate agents, high value dealers, Accountants* and *Lawyers* this means a *business relationship* established before the *Money Laundering Order* came into force on 1 May 2008 and which continues. Refer to section 4.9.2 for further details on legacy *customer*s.

AML/CFT/CPF Codes of Practice

[COP169] A *supervised person* must not permit final agreements to be signed or pay away funds to an external party (or to another account in the name of the *customer*), other than to deposit the funds on behalf of the *customer*, until such time as evidence of identity has been obtained.

13. As noted above, where a relationship between a *supervised person* and a *customer* has no "element of duration" and is not a one-off transaction within the meaning of Article 4 of the *Money Laundering Order*, *identification measures* within the meaning of Article 13 of the *Money Laundering Order* are not required unless:

- The *supervised person* suspects *money laundering*, the *financing of terrorism* or the financing of proliferation; or
- The *supervised person* has doubts about the veracity or adequacy of any documents, data or information previously obtained under the *CDD* measures.

AML/CFT/CPF Codes of Practice

[COP170] In the circumstances set out in paragraph 13 above, the identity of the person undertaking the transaction must still be found out and recorded.

[COP171] A *supervised person* must record the basis that it has applied for determining the value of a transaction for the purposes of establishing whether it is a *one-off transaction* under Article 4 of the *Money Laundering Order*, and why that basis is appropriate.

[COP172] A *supervised person* must have in place measures to identify when linked transactions are being undertaken which would, in total, amount to €15,000 or more (for all *supervised persons* save for *MVTS*, *VASP*, or those operating a casino where different thresholds apply as set out in Article 4(1) of the *Money Laundering Order*), and therefore be a one-off transaction within the same meaning of Article 4 of the *Money Laundering Order*. *Supervised persons* must also consider when the frequency of regular *one-off transactions* by the same *customer* would constitute a *business relationship*.

[COP173] A *supervised person* must consider the nature of those transactions which are determined not to be a *one-off transaction* for which *identification measures* are not required. Where these transactions are considered to present a higher risk of *money laundering* or the *financing of terrorism* or *proliferation financing*, consideration must be given to applying full *CDD* measures.

[COP174] A *supervised person* must be able to demonstrate that their decision not to apply *identification measures* in respect of such transactions was reasonable considering its business risk profile.

17.2 Governance

14. The below are selected areas of focus and should be read in conjunction with sections 1 – 11 of *this handbook*.

AML/CFT/CPF Codes of Practice

[COP175] A *supervised person* must ensure that the *MLRO* maintains a record of all enquiries received from law enforcement authorities.

17.2.1 Business Risk Assessment (BRA)

Statutory requirements (paraphrased wording)

Activity	*Related statute (MLO)*
	15. *Article 11(1)(f): A relevant person must maintain appropriate and consistent policies and procedure relating to risk assessment and management.*
Business Risk Assessment	16. *Article 11(2)(a): Policies and procedures must take into account the level of risk identified in a national or sector-specific risk assessment in relation to money laundering carried out in respect of Jersey.*
	17. *Article 11(2)(b): Policies and procedures must take into account the type of customers, business relationships, products and transactions with which the relevant person's business is concerned.*

18. This section is supplemental and should be read in conjunction with sections 2.3 and 2.3.1 of *this Handbook.*

19. A *Business Risk Assessment* is a strategy document that assesses how exposed a *supervised person* may be to certain *financial crime* threats, and in turn, sets out how these threats and the associated risks of them occurring are mitigated and reduced.

20. The *BRA* relating to *customers* and services will depend on the *supervised person's* size, type of *customers* and the practice area it engages in or chooses not to. The *supervised person* should have a business risk appetite which will detail what the board have assessed and determined is beyond the *supervised person's* risk appetite, for example businesses where their profits are derived from selling weapons (see further guidance in Section 2.3.1)

21. *Supervised persons* should consider the different types of risk to which they are exposed. The risks should be considered within the context that a *supervised person* may be used to launder funds or assets through the *supervised person* or, alternatively, that the *customer* or its counterparties may launder criminal funds or assets.

22. As a minimum, a *Business Risk Assessment* should look to consider:

- The size and complexity of a *supervised person*, its day-to-day activities, who the *customer*s are, what kind of payments are received;
- a *supervised persons* organisational structure;
- a *supervised persons customer*s, and the countries and territories with which its *customer*s are connected;
- a *supervised persons* products and services, and how it delivers those products and services;
- the type of transactions a *supervised person* is subject to (for example, the use of cash and whether there is a limit to cash usage); and

- criteria for obtaining information from a client whose cash payment exceeds a certain threshold (either in a single transaction or several transactions which appear to be linked).

23. A BRA should document:

- how a *supervised person* plans to stay aware of the various kinds of criminal activities related to *money laundering*, *terrorist financing* and *proliferation financing and respective national risk assessments*;
- a record of the *supervised persons* staff training on understanding and identifying ML and TF risks, suspicious transactions and activity, and potential threats; and
- how the *supervised person* tests the knowledge and understanding it's staff have regarding the above points.

24. Specialisation within a sector that undertakes higher risk activity from a *money laundering, terrorist financing, and*/or *proliferation financing* perspective will affect the *BRA*. Examples of higher risk sectors and sensitive business areas for *money laundering*, the *financing of terrorism,* or the *financing of proliferation* purposes include:

- *financial services businesses* (including *MVTS* activity);
- high cash turnover businesses: bars and clubs, taxi firms, launderettes, takeaway restaurants, market traders;
- gaming and gambling businesses;
- real estate and construction;
- computers and high technology, telecommunications, and mobile phone businesses;
- arms and armaments;
- activities related to cryptocurrencies and similar assets;
- antique/art dealerships (including auction houses); and
- dealers in high value or precious goods (e.g., jewels, gems, precious metals).

25. *Customers* who are *supervised persons* - such as *financial services businesses*, *MVTS* activity and *real estate agents* should have taken steps to mitigate their risks by implementing robust internal controls.

26. A non-exhaustive list of sector specific risks and threats are included in each sector specific section (13 – 21) which may be considered whilst building a BRA.

17.2.2 The *MLCO*

27. This section is supplemental to and should be read in conjunction with section 2.6 of *this Handbook*.

28. Section 2.6 of *this Handbook* sets out statutory requirements under the *Money Laundering Order* and *AML/CFT/CPF Codes of Practice* regarding the appointment of a *MLCO*.

17.2.3 The *MLRO*

29. This section is supplemental to and should be read in conjunction with section 2.7 of *this Handbook*.

30. Section 2.7 of *this Handbook* sets out statutory requirements under the *Money Laundering Order* and *AML/CFT/CPF Codes of Practice* regarding the appointment of a *MLRO* and, where relevant, *Deputy MLROs*.

17.2.4 Monitoring effectiveness of DNFBP's compliance

Statutory requirements (paraphrased wording)

Activity	*Related statute*
Compliance Monitoring Plan	31. *Article 11(2)(a): A relevant person must maintain adequate procedures for monitoring and testing the effectiveness of the following actions –* *(a) the policies and procedures maintained under paragraph (1);* *(b) the measures taken under paragraph (9); and* *(c) the training provided under paragraph (10).*

32. Because the BRA is a dynamic document it is necessary for the *supervised person* to devise a mechanism to monitor how effectively they implement preventative measures to mitigate the risks they are exposed to by their business. This is an ongoing process and is often described as a 'compliance monitoring programme'. Issues that should be considered as part of this process include:

- Procedures to be undertaken to monitor compliance, e.g. random file audits or file checklists to be completed before opening and closing a file whether periodic reviews of *CDD* are up to date;
- The frequency and content of reports that have been provided to senior management on compliance;
- How to rectify lack of compliance, when identified, and how remediation is monitored until completion and the metrics regarding this process; and
- How findings or lessons learned will be communicated to staff and fed back into the BRA of the business.

33. The resources allocated to appropriately implement the risk-based approach to *AML/CFT/CPF* compliance will vary. A small practice or sole practitioner is not expected to devote the same level of resources as a large practice. Having a smaller practice or being a sole practitioner with a smaller number of clients does not mean that this business is automatically lower risk. The risk of the business will depend on the type of work undertaken, the services provided, and the nature of the *customer*s. Smaller practices may be targeted by money launderers who may think they lack the resources to identify them.

34. Design of a robust CMP may include the following seven steps:

- identifying relevant legislative and regulatory requirements;
- identifying relevant controls;
- conducting a risk assessment;
- producing and approving a CMP;
- undertaking testing;

- reporting; and
- overseeing remedial action.

35. Under Article 11(12) of the *Money Laundering Order* the size and type of testing described above should be commensurate with the risk of *money laundering* that exists in respect of the *supervised persons* business and as such will vary between sectors, client types and services offered – which as outlined in 17.2.1 may be defined by the outputs from the BRA.

17.2.5 Non supervised business related activities

36. Whilst the *Money Laundering Order*, and consequently *this Handbook*, only brings within its scope the business activities where *DNFBP*s are carrying on a supervised business, the Anti-Money Laundering and Counter-Terrorism Legislation and the general offences and penalties cover all persons and all business activities within Jersey. Consequently, *DNFBP*s undertaking supervised business may wish to consider applying the systems and controls to counter *money laundering*, *the financing of terrorism,* or the *financing of proliferation* across the whole of their business activities.