Aurora Capital Markets

AML/CTF Program

Issue Date 1 March 2021

Table of contents

Introduction

1 Information about this Program

1.1 Purpose

Aurora (Aurora) provides a Designated Service and therefore must comply with the AML/CTF Obligations. The purpose of this Program is to set out how Aurora complies with its AML/CTF Obligations. In particular, this Program sets out the key measures Aurora will apply to

(a) assess the ML/TF risks relating to its activities

(b) mitigate and control those risks, and

(c) explain the manner in which Aurora carries out client identification and verification.

1.2 Structure of this Program

(a) This Program comprises the following two parts:

(i) *Part A - General* sets out how Aurora identifies, mitigates and manages the ML/TF risks it faces in providing Designated Services.

(ii) *Part B - Client identification* explains the process by which Aurora identifies and verifies clients.

(b) The structure and content of this Program has been based on the following:

(i) The nature of the Designated Services.

(ii) The Designated Services are only provided from Aurora's registered office in Australia.

(iii) Aurora does not have any permanent establishments in any foreign countries.

Part A - General

The purpose of Part A of this Program is to set out the procedures by which Aurora may identify, manage and mitigate the ML/TF risks it may reasonably face in the provision of its Designated Service. This Part A applies to all areas of Aurora's business which involve the provision of its Designated Service (including any relevant functions carried out by third parties).

2 AML/CTF compliance structure

2.1 AML/CTF reporting structure

The flowchart in 2 - AML/CTF reporting structure lists the personnel and reporting lines for Aurora's AML/CTF compliance system.

2.2 Board approval and oversight

(a) This Program has been approved by the Board of Aurora.

(b) The Board of Aurora is responsible for ongoing oversight of the AML/CTF activities carried out under this Program.

(c) The Board receives recommendations from the AML/CTF Compliance Officer and may consider amendments to this Program. Board approval is required to make amendments.

2.3 **AML/CTF Personnel**

(a) (a) AML/CTF Compliance Officer

(i) Aurora has appointed a person as its AML/CTF Compliance Officer. The AML/CTF Compliance Officer's role is to ensure the procedures described in this Program are complied with.

(ii) The AML/CTF Compliance Officer reports to the Board on a quarterly basis (which may be via the Compliance Officer's quarterly report to the Compliance Committee which is in turn provided to the Board).

(b) Other resources

The AML/CTF Compliance Officer is assisted, where necessary, by additional compliance personnel. AML/CTF Key Employees may carry out specific duties in respect of AML/CTF matters and must report to the AML/CTF Compliance Officer.

3 Risk assessment process

Aurora identifies, assesses and evaluates ML/TF risks associated with operation of its business (including the provision of the Designated Service), which involves considering whether any risk remains after Aurora has applied its mitigation and management strategies.

3.1 **Risk identification**

Aurora considers the business risks posed by all of the following:

(a) The types of Designated Services it provides (product and service risk).

(b) The methods by which it delivers Designated Services (channel risk).

(c) The foreign countries in which its clients reside or do business (jurisdiction risk).

(d) The types of client, including any PEPs, to whom Designated Services may be provided (client risk).

Aurora also considers the regulatory risks posed by breaches of the AML/CTF Obligations.

3.2 **Changes to business risks**

(a) The AML/CTF Compliance Officer and the Board (where required) will review any changes or additions to Aurora's products, services, delivery methods and use of technology as they occur and at least on an annual basis to ensure any change to Aurora's risk profile is reflected in the procedures contained in this Program.

(b) The AML/CTF Compliance Officer will follow the procedure described in clause 3.3 of this Program to assess any changes to business risks.

3.3 **Risk assessment**

Aurora has assessed the business and regulatory risks in providing the Designated Services. An assessment of the risks is set out Schedule 3 - Risk assessment.

3.4 **Risk mitigation and management (treatment)**

Aurora has implemented a number of controls to mitigate and manage AML/CTF risks. These are set out in Schedule 3 - Risk assessment, which also includes an analysis of the risks that still remain, if applicable, after the controls have been put in place.

4 Initial customer due diligence

Part B - Client identification and verification set out the procedures Aurora carries out to ensure a client exists and is who it claims to be.

5 Ongoing customer due diligence

5.1 What is customer due diligence?

In addition to initial customer due diligence procedures set out in Part B - Client identification and verification, Aurora also conducts ongoing customer due diligence which may involve any or all of the following:

(a) Screening of client recorded in the register of clients and prohibited person/entity identification (see clause 18(a)).

(b) Monitoring of client's transactions for suspicious transactions (see clause 5.2).

(c) Enhanced customer due diligence where a Red Flag has been raised in relation to a client (see clause 5.4).

5.2 Transaction monitoring program

As part of its customer due diligence procedures, Aurora has implemented a transaction monitoring program to identify transactions that appear suspicious. Aurora's transaction monitoring program comprises a three step process, as follows:

(a) Monitor all client transactions in accordance with the systems and procedures set out in this Program. This involves

(i) the AML/CTF Compliance Officer being alerted or notified by Key Employees if a transaction appears unusual, and

(ii) quarterly review of applications.

(b) Identify suspicious transactions (see clause 6.2).

(c) Take appropriate action, which may include reporting to AUSTRAC (see clause 6).

5.3 Red Flags - medium or high ML/TF risk

If Aurora's customer due diligence procedures reflect a medium to high risk for a client, then a Red Flag is raised. Examples of situations which indicate a Red Flag include the following:

(a) A client's name matches the name of a PEP or prohibited person/entity (following a search of the client register (see clause 18(a)).

(b) A significant[1] transaction or series of transactions takes place involving the client.

(c) A significant change occurs in the way a client interacts with Aurora compared to the client's previous dealings.

(d) A client requests redemption proceeds or distributions to be paid to a bank account held in the name of a third party.

(e) A client requests redemption proceeds or distributions to be paid to a bank account held in another country.

[1] 'Significant' means significant in terms of the amount, size or volume or any other characteristic which would cause DMSL to consider the transaction or change to be noteworthy.

(f) The client appears to be acting as an agent for an undisclosed principal, but declines or is reluctant, without legitimate commercial reasons, to provide information or is otherwise evasive regarding that person or entity.

(g) The client makes an investment followed shortly thereafter by a request to redeem the investment.

(h) The client requests that a transaction be processed to avoid Aurora's normal documentation requirements.

(i) There are any doubts about the identity of a client.

(j) If a Red Flag results from Aurora's customer due diligence procedures, then Aurora will follow the enhanced customer due diligence procedures set out in clause 5.4.

5.4 Enhanced customer due diligence program

(a) Where a Red Flag has been associated with either an applicant (see examples in clause 20.4), and Aurora decides to proceed to process the application, or an existing client (see examples in clause 5.3), then Aurora must carry out enhanced customer due diligence on that individual or entity.

(b) The type of enhanced customer due diligence may include any action Aurora deems appropriate in the circumstances having regard to the specific nature of the Red Flag.

(c) Generally, Aurora will carry out one or more of the following:

(i) Seek further KYC Information from the client (the AML/CTF Rules set out an exhaustive list of further KYC Information which may be provided).

(ii) Seek further KYC Information from other sources.

(iii) Verify or re-verify the client's information using existing information.

(iv) Undertake more detailed analysis and monitoring of the client's transactions (both past and future).

(v) Lodge a suspicious matter report with AUSTRAC.

(vi) Lodge a transaction threshold report with AUSTRAC.

(d) Following the completion of the enhanced customer due diligence, Aurora may either:

(i) accept or reject an application (where an applicant is involved); or

(ii) take further action including lodging a suspicious matter report (see clause 5.2), contacting the Australian Federal Police or seeking legal advice (if an existing client is involved).

6 Reporting to AUSTRAC

Aurora is obliged to lodge regular compliance reports, as well as report suspicious matters and certain 'threshold transactions' to AUSTRAC.

6.1 Annual compliance report

(a) For each reporting period (determined by AUSTRAC), Aurora must lodge an AML/CTF compliance report with AUSTRAC regarding Aurora's compliance with the AML/CTF Act.

(b) The AML/CTF compliance report will be prepared by the AML/CTF Compliance Officer.

(c) The AML/CTF compliance report will be in the form required by AUSTRAC from time to time.

6.2 Suspicious matter reports

(a) What is a suspicious matter?

Whether a transaction is suspicious will be determined by Aurora having regard to the risks discussed in clause 3.1 and the risk assessment in Schedule 3 - Risk assessment of this Program.

(b) Examples of suspicious behaviour

Aurora has developed list of Red Flags which may alert Aurora to suspicious activities, as follows:

(i) Suspicious behaviour associated with an applicant is set out in clause 20.4.

(ii) Suspicious behaviour which has arisen in relation to an existing client is set out in clause 5.3).

(c) Reporting suspicious matters

Suspicious transactions must be reported to AUSTRAC within three business days of Aurora forming a suspicion. A suspicious matter report is carried out online (via AUSTRAC's website) using the prescribed form. The form requires, amongst other things, a description of:

(i) any designated service to which the suspicious matter relates, and

(ii) the reasonable grounds for suspicion relating to the suspicious matter.

Aurora will also include in the suspicious matter report any other information it considers relevant having regard to the nature of the suspicious matter in question.

6.3 Threshold transaction reports

(a) Aurora must report 'threshold transactions' to AUSTRAC.

(b) A 'threshold transaction' is defined in the AML/CTF Act as

(i) a transaction involving the transfer of physical currency[2], where the total amount transferred is not less than $10,000;

(ii) a transaction involving the transfer of money in the form of e-currency[3], where the total amount transferred is not less than $10,000; or

(iii) transactions from time to time specified in the regulations to the AML/CTF Act.

(c) Threshold transactions must be reported to AUSTRAC within 10 business days of the day on which the transaction takes place. The report should include the contents specified in Chapter 19 of the AML/CTF Rules and must be lodged by post to the CEO, AUSTRAC.

[2] For the purpose of the definition of 'threshold transaction', 'physical currency' means coin or printed money of Australia or another country which is designated as legal tender.

[3] 'e-currency' means an electronic form of currency which is backed by precious metal, bullion or a kind specified in the AML/CTF Rules.

7 AUSTRAC liaison procedure and feedback

Aurora undertakes to ensure any correspondence or contact from AUSTRAC is dealt with promptly and smoothly.

7.1 Handling AUSTRAC correspondence

(a) If Aurora receives correspondence, enquiry or feedback from AUSTRAC or any of its authorised officers then those enquiries must be immediately directed to the AML/CTF Compliance Officer.

(b) All enquiries must be responded to by the AML/CTF Compliance Officer who will co-ordinate any necessary input from the relevant areas of Aurora.

(c) If the AML/CTF Compliance Officer receives any enquiry or correspondence from AUSTRAC, the AML/CTF Compliance Officer must do the following:

(i) Log the enquiry or correspondence in the AML/CTF correspondence register.

(ii) Copy the correspondence to the CEO.

(iii) Seek input to formulate a response to the enquiry or correspondence from the relevant groups/department/personnel to which it relates.

(iv) Seek external legal, accounting or other assistance as required to enable Aurora to produce an accurate, complete and up-to-date response to AUSTRAC.

(v) Provide the response to AUSTRAC within the time required.

(vi) Provide a copy of the correspondence register to the CEO on a quarterly basis (who in conjunction with the AML/CTF Compliance Officer will determine appropriate reporting to the directors).

7.2 Approach to AUSTRAC feedback regarding AML/CTF policies and procedures

Aurora will, through the AML/CTF Compliance Officer, take the following steps in the event feedback is received from AUSTRAC regarding Aurora's policies and procedures:

(a) Log the AUSTRAC feedback in the AML/CTF correspondence register.

(b) Assess the feedback against the policies and processes in this Program.

(c) If the feedback has been generated as a result of an error or breach, then the AML/CTF Compliance Officer will arrange an investigation of the relevant event and report to the Board as to the root cause or causes of the relevant event (if known).

(d) If the root cause relates to a failure or error or omission in the application of Aurora's policies and procedures, then actions need to be taken by the AML/CTF Compliance Officer to modify future behaviours. This will include ensuring relevant employees are trained or directed to observe Aurora's policies and procedures.

(e) If the root cause relates to a defect in Aurora's policies, procedures, documentation or training, then actions need to be taken by the AML/CTF Compliance Officer to review the particular policies, procedures, documentation or training and implement necessary amendments. All amendments to this Program must be approved by the Board.

8 Employee due diligence

8.1 Competence of AML/CTF personnel

(a) Only certain employees will be engaged in the provision of Designated Services or other activities which could give rise to a risk of ML/TF (i.e. Key Employees).

(b) Aurora must ensure each Key Employee has the relevant competence to continue to carry out their duties under the AML/CTF Program efficiently, honestly and fairly.

8.2 Employee due diligence program

Aurora screens employees in accordance with the following employee due diligence program:

(a) Roles and responsibilities - identify roles where an employee is a Key Employee for AML/CTF purposes and requires screening. This review occurs on an annual basis.

A Key Employee is an employee whose role involves the provision of Designated Services or other activities which could give rise to ML/TF operations. In order to understand the inherent AML/CTF risk which is associated with an employee's roles and responsibilities, the following features must be considered:

(i) Business area, ie, the inherent risk of the business with regard to products and services, client base, and/or jurisdiction.

(ii) Extent of client contact.

(iii) Degree of access to client accounts.

(iv) Segregation of duties (eg, account opening compared with client due diligence).

(v) Remuneration structure (eg, commissions or bonuses).

(vi) Level of seniority and/or authority.

(vii) Reporting lines and level of supervision.

(viii) Employee status, i.e., whether permanent or temporary.

(b) Employment agreement - every employment agreement for Key Employees must include an obligation to comply with the AML/CTF Obligations which relate to the relevant job description.

(c) Employee screening - prior to the appointment of a Key Employee, the individual must be screened, as follows:

(i) Employee credentials (eg, reference checks or criminal history checks).

(ii) Fit and proper characteristics (eg, the person's character, competence and experience and whether they have shown willingness to comply with legal/regulatory requirements or professional standards).

(d) Employee re-screening - employees must be screened or re-screened if they are transferred or promoted to a position which may enable the facilitation of ML/TF. Aurora may elect to re-screen employees at any time.

8.3 Disciplinary measures

(a) Any breach of this Program (including a breach of the AML/CTF Obligations) is handled in accordance with clause 10.

(b) If any aspect of the employee's performance is found not to be of an acceptable standard[4], then:

(i) further training will be provided, or

(ii) if appropriate, the employee will be disciplined or their appointment suspended or terminated.

9 Training and awareness

9.1 Objectives

(a) The objectives of the AML/CTF training program are to enable Key Employees to understand the following:

(i) The obligations under the AML/CTF Act and AML/CTF Rules.

(ii) The consequences of non-compliance with the AML/CTF Act and AML/CTF Rules.

(iii) The types of ML/TF risk Aurora might face and the potential consequences of such risk.

(iv) The processes and procedures in this Program which are relevant to the work carried out by the Key Employee.

(b) All other relevant employees of Aurora will undergo training (which may comprise reading of this document) to ensure they understand the following:

(i) A broad outline of Aurora's obligations in regards to compliance with the AML/CTF Act.

(ii) A broad outline of the ML/TF risks Aurora faces in the operation of its business.

9.2 Employee risk awareness training program

(a) Overall approach

Aurora is committed to ensuring every relevant employee is aware of the need to minimise the risk of ML/TF and that Aurora has a program in place to enable it to manage its risk. Aurora will provide more extensive risk awareness training of Key Employees as compared to other relevant employees.

(b) Determination of Key Employees

It is the role of the AML/CTF Compliance Officer to determine which employees are Key Employees and to tailor their training accordingly, which may include on the job training. Refer to clause 8.2(a) for the characteristics of the roles and responsibilities which indicate a Key Employee.

(c) Frequency

Aurora understands it is essential for the creation of a robust AML/CTF compliance environment and that training is provided at relevant times. The frequency of training will differ for employees depending on their position, role and responsibilities, as follows:

(i) For Key Employees

(A) new Key Employees - training will be provided for new Key Employees within one month of induction

[4] In this case, an 'acceptable standard' is one that at least facilitates compliance with this Program (which includes the AML/CTF Obligations).

(B) employees moving to positions of greater ML/TF risk exposure - depending upon the individual's role, additional training may be required when staff are appointed to positions carrying additional AML/CTF responsibilities or exposure to additional or new ML/TF risks

(C) ongoing basis - training must be provided annually, as required, and/or

(D) targeted training - additional training will be provided following the introduction or amendment of major changes to AML/CTF Obligations or procedures.

(ii) For all other relevant employees - provision of information on the AML/CTF program as required. No ongoing training is required unless the individual is considered a Key Employee.

(d) Assessment

The AML/CTF Compliance Officer will determine the method of assessment for any training under this Program, if determined necessary. There is no requirement for an assessment to be included in any training provided under this Program.

(e) Record keeping

The AML/CTF Compliance Officer will retain the following records of all AML/CTF risk awareness training received:

(i) Name of each employee who received the training.

(ii) Whether the employee is a Key Employee.

(iii) The type of training received.

(iv) The date the training was implemented.

(v) The assessment results of the employee (if applicable).

(vi) If follow is training required, and if applicable, the date the follow up training was implemented.

10 Breaches

10.1 Identifying and assessing breaches

(a) Breach reporting (including the notification of potential breaches) is the responsibility of all Aurora employees. Any potential breach or incidence of non-compliance of the AML/CTF Obligations or this Program must be reported to the AML/CTF Compliance Officer.

(b) The AML/CTF Compliance Officer must assess the breach (or potential breach) and determine whether it is material, having regard to the circumstances surrounding the breach (or potential breach) and the prevention of ML/TF.

10.2 Reporting breaches

(a) The AML/CTF Compliance Officer must report all material breaches to the CEO.

(b) The CEO will then consider what action to take in respect of the breach, including instigating further training or reviewing/amending systems to prevent a similar breach occurring. If necessary, the CEO will refer to the matter to the Board for consideration.

(c) The AML/CTF Compliance Officer must also report to the Board on material breaches on a quarterly basis (which may be via the Compliance Officer's quarterly report to the

Compliance Committee which is in turn provided to the Board). The report must provide details of

(i) any material breaches which have been discovered since the last report

(ii) action taken to remedy any material breaches, and

(iii) the status of any outstanding breaches.

(d) If required by AUSTRAC, details of breaches may be included in the annual compliance report.

(e) A breach of this Program and/or the AML/CTF Obligations does not of itself constitute a breach of the *Corporations Act 2001*.

10.3 **Recording breaches**

All breaches must be recorded in the compliance breach register.

11 Reporting and review

11.1 **Quarterly report**

The AML/CTF Compliance Officer will report to the Board at least quarterly (which may be via the Compliance Officer's quarterly report to the Compliance Committee which is in turn provided to the Board) on the following:

(a) Material breaches (refer to clause 10.2(c)).

(b) The continued adequacy of this Program (including Schedule 3 - Risk assessment).

(c) Any changes to regulatory or industry standards that impact this Program.

(d) Any feedback from staff on AML/CTF operating structures and procedures.

11.2 **Regular review of this Program**

(a) Part A of this Program (which includes Schedule 3 - Risk assessment) must be independently reviewed regularly. The review may be undertaken by either by an internal or external party. Aurora carries out this review annually. The independent review must assess

(i) the effectiveness of Part A of this Program having regard to the ML/TF risk of Aurora

(ii) whether Part A of this Program complies with the AML/CTF Rules

(iii) whether Part A of this Program has been effectively implemented, and

(iv) whether Aurora has complied with Part A of this Program.

(v) Part B review - Aurora may determine to review Part B of this Program, as part of the independent review of Part A or as a separate review. The review of Part B is optional.

(b) Reporting - the party conducting the review must provide a report to the Board which may include recommended amendments to this Program.

12 Record keeping

12.1 **Comply with AML/CTF Obligations and privacy laws**

Aurora must comply with the AML/CTF Obligations and *Privacy Act 1988* (Cth) in relation to records kept under this Program.

12.2 **Documentation**

(a) Aurora must keep records documenting what it has done to comply with this Program and all AML/CTF related decisions, including Board reports and minutes. Aurora must ensure these records are clearly documented and easily accessible.

(b) Documents and records may be kept electronically where appropriate.

12.3 **Retention of documents**

Aurora must keep the following records for at least seven years:

(a) Records of Aurora's Designated Services (i.e. how and when transactions were conducted with clients).

(b) Any document a client provides to Aurora relating to the provision of the Designated Service.

(c) A copy of this Program.

Part B - Client identification and verification

Part B sets out the client identification procedure that must be carried out for each client. The identification and verification requirements of Part B tie in with the risk-based results of Part A of this Program.

13 Objective of Part B

13.1 **Responsibility**

(a) Aurora may also rely on client identification by a Licensee Intermediary if it has a Customer Identification Management Agreement in place with that Licensee Intermediary.

(b) Aurora acknowledges that it has primary responsibility for these obligations.

13.2 **Reliance**

(a) Under the AML/CTF rules, Aurora is deemed to have carried out the customer's identification where that identification has been carried out by the Licensee Intermediary and agents provided the conditions in the AML/CTF Rules are met.

(b) When considering identification programs conducted by Licensee Intermediaries and agents, Aurora considers the following points and constructs its policies and procedures as part of the overall customer identification program to address them:

(i) This practice is not failsafe and there may be difficulties in achieving effective 'know your customer information'.

(ii) Aurora is still responsible for the duty to know who its own customers are.

(iii) Aurora will need to be satisfied that Licensee Intermediaries and agents have conducted the 'know your customer information' and customer identification procedures according to at least the minimum standards required under the AML/CTF Act and Rules.

(iv) The Licensee Intermediaries and agents may not have a customer identification procedure in place that is as stringent as that utilised by Aurora. As such, it may be more difficult to create relevant and meaningful 'know your customer information' profiles for investors introduced in this manner, including accurate ML/TF risk assessments for each investor.

13.3 **Mitigation of Customer Identification Procedure risk posed by Licensee Intermediaries and agents**

Aurora has resolved to mitigate the risk posed by using Licensee Intermediaries and agents in the customer identification of clients. Where practicable, Aurora must observe measures such as the following:

Mitigating steps	Timing
Be discerning about the Licensee Intermediaries and agents on which Aurora is prepared to rely to fulfil its customer identification program and obligations under the legislation.	Before entering into an arrangement with the Licensee Intermediary or agent for the carrying out of the Customer Identification Procedure and reviewing on an annual basis.
Provide the Licensee Intermediary and agent with a preferred Customer Identification Procedure.	Before agreeing with the Licensee Intermediary or agent that they will provide this service.
Conduct steps such as reviewing the Licensee Intermediary's and agent's compliance with the preferred (or its own) Customer Identification Procedure in place and ask the intermediary and agent specific questions about its 'know your customer information' procedures.	Annually.
Follow an analysis of the AML/CTF risk assessment model to determine how to manage record retention- Low risk—have an AML/CTF Customer Identification Management Agreement in place whereby Aurora has access to records (only available for Licensee Intermediaries) Medium risk—require the Licensee Intermediary or agent to provide the Customer Identification Procedure records to Aurora, and High risk—require the Licensee Intermediary or agent to provide scanned copies of each of the Customer Identification Procedure documents to Aurora and determine whether additional information should be requested through the intermediary.	The level of risk is to be evaluated on an annual basis.
Conduct audits of the Licensee Intermediary and agent's records.	On a half-yearly basis.

13.4 **Identification objective**

(a) The aim of these Part B procedures is to ensure Aurora is 'reasonably satisfied' that a client exists and is who they claim to be.

(b) The identification objective for each client type is as follows:

(i) Individual - the client is the individual he or she claims to be.

(ii) Domestic company - the company exists and (in respect of unregulated proprietary companies), the name and address of all shareholders that own more than 25 percent of the issued share capital has been provided.

(iii) Foreign company - the company exists and (in respect of certain companies), the name and address of any beneficial owner of the company has been provided.

(iv) Trust - the trust exists and the name of each trustee and beneficiary, or a description of each class of beneficiary, of the trust has been provided.

(v) Partnership - the partnership exists and the name and residential address of the partners in the partnership has been provided.

14 Timing of identification

14.1 **Upon investment**

Identification information must be collected by Aurora when a prospective client applies for services. This allows for an assessment to be made by Aurora to determine whether any further KYC Information is required and to determine how often KYC Information should be updated and/or verified.

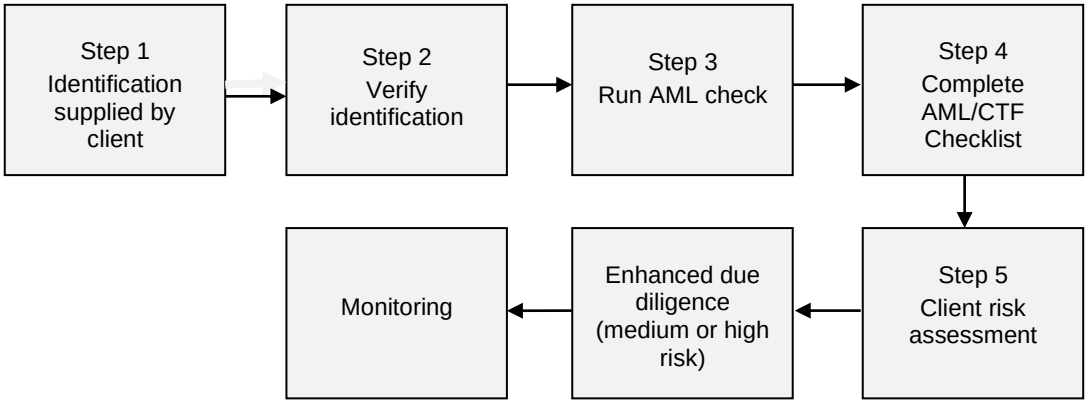
14.2 **Existing clients**

(a) Clients whose identity has previously been verified will not be required to be re-identified and verified unless determined by Aurora.

(b) Aurora must carry out further identification of existing clients where a suspicious matter reporting obligation arises in relation to a client.

15 Procedure for identification and verification - the steps

The client identification procedure follows a similar pattern for each type of client:



Steps 1 to 5 are set out below. Enhanced due diligence and monitoring procedures are set out in Part A (in clause 5.4 and clause 5.2 respectively).

16 Step 1 - Identity

To identify the clients, Aurora must receive the following as a complete application from prospective clients applying for services:

(a) a correctly completed application form from the PDS; and

(b) minimum prescribed KYC Information from the client type (as set out in the PDS).

If one of the above items has not been provided or is not adequate, then Aurora must contact the applicant to obtain the relevant information or return the application.

17 Step 2 - Verify

The Key Employees must verify each client's identity from KYC Information supplied by the client by checking all details match those listed on the application form. Signatures should be cross-checked where possible (eg, the signature on the application form should be checked to the signature on the sales advice or sale contract). The name on the application form should be checked to ensure it matches the name on the sale contract.

18 Step 3 - Run AML check

(a) Aurora may carry out any of the following searches to determine whether an applicant (or existing client if applicable) is listed as a PEP[5] or other prohibited person, but will always carry out one or more of the following the searches in relation to clients where a Red Flag has been raised:

(i) www.deloitteamlcheck.com.

(ii) www.complinet.com

(iii) Any commercial PEP list provider (such as WorldCompliance or Dow Jones Watchlist).

(iv) FinCEN intelligence reports which are used to search the client register for individuals and entities who are 'blacklisted' by FinCEN.

(v) DFAT's Consolidated List, which contains names of persons or entities believed to be involved in terrorism.

(vi) FINRA search.

(b) Where there is a match of a client' s name with one of the above, then the AML/CTF Compliance Officer may make further enquiries to determine if the client is actually the PEP or prohibited person (in accordance with the enhanced due diligence procedures (see clause 5.4)).

(c) Aurora does not transact persons identified by intelligence authorities as 'prohibited' or believed to be involved in ML/TF activities.

(d) Aurora may choose to transact with PEPs after undertaking the enhanced due diligence procedures in respect of the PEP.

[5] DMSL is not obliged to identify Australian PEPs unless there is a specific need to identify, within the context of the ML/TF risk DMSL faces, a domestic PEP for client due diligence purposes.

19 Step 4 - Complete client identification and verification checklists

The Key Employee must complete Aurora's internal application checklist. This involves reviewing a client's entire application and confirming whether adequate information has been received.

20 Step 5 - Client risk assessment

20.1 **Determine level of risk**

The Key Employee makes an assessment of the risk associated with a client and categorises them as 'high', 'medium' or 'low'.

20.2 **Low risk**

If an applicant is deemed 'low' risk and Steps 1 to 4 have been carried out to allow Aurora to reasonably believe the client is who they say they are, then the application may be accepted.

20.3 **Medium to high risk**

(a) If the risk analysis of an applicant reflects a 'medium' to 'high' risk, then a Red Flag is raised (see examples of Red Flags set out in clause 20.4).

(b) An application attracting a medium to high risk rating must be brought to the attention of the AML/CTF Compliance Officer who will then determine an appropriate course of action in accordance with the enhanced due diligence procedures (see clause 5.4).

(c) Following the completion of the enhanced due diligence procedures, Aurora must determine how to proceed, which may include

(i) accepting the client subject to review of further KYC Information;

(ii) rejecting the client's application, and/or

(d) lodging a suspicious matter report with AUSTRAC.

20.4 **Red Flags - at the time of application**

Examples of Red Flags which may be raised at the time of application include the following:

(a) An applicant (or the beneficiaries, as applicable) is from a high risk country. This includes countries

(i) with no AML/CTF regulation

(ii) which are viewed as supporters of terrorist activity, and

(iii) which are regions where known criminal activity occurs (eg, Iraq or Indonesia).

(b) An applicant requests to make their investment in cash.

(c) The source of funds cannot be identified (i.e. payment is not by electronic funds transfer or a cheque from a recognised financial institution).

(d) An applicant requests a reduced level of secrecy.

(e) An applicant's name matches the name of a PEP (see clause 18(a)).

(f) An applicant's name matches the name of a person listed by a regulatory authority as a prohibited person for AML/CTF purposes (see clause 18(a)), including known criminals or terrorists.

(g) An applicant (or a person publicly associated with the applicant) has a questionable background or is the subject of news reports indicating possible criminal, civil or regulatory violations.

(h) An applicant appears to be acting as an agent for an undisclosed principal, but declines or is reluctant, without legitimate commercial reasons, to provide information or is otherwise evasive regarding that person or entity.

(i) An applicant requests their application be processed to avoid Aurora's normal documentation requirements.

(j) Where a discrepancy arises in the information collected from an applicant.

(k) There are any doubts about the identity of an applicant following a check of KYC Information received.

(l) Upon request, an applicant refuses to identify or fails to indicate any legitimate source for his or her funds and other assets.

Schedule 1

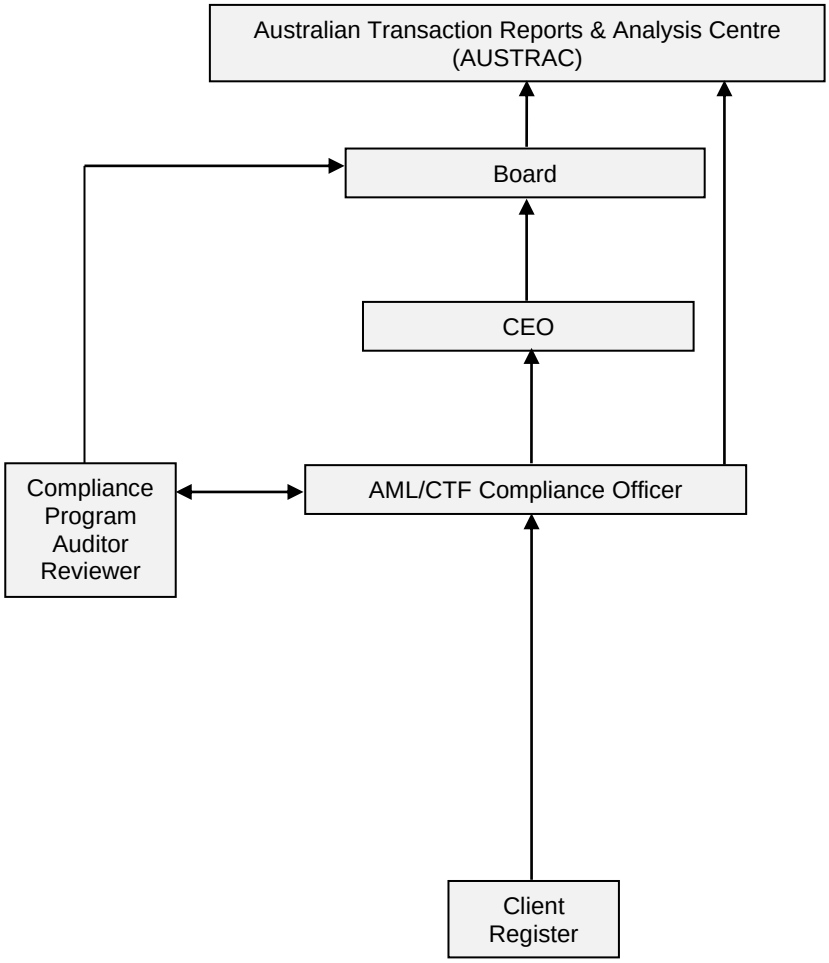
Dictionary

AML/CTF	Anti-money laundering and counter terrorism financing.
AML/CTF Act	The *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* for the time being in force together with any regulations.
AML/CTF Compliance Officer	The AML/CTF compliance officer appointed by Aurora from time to time, as required by the AML/CTF Obligations.
AML/CTF Obligations	The obligations imposed under the AML/CTF Act, AML/CTF Rules, and any other relevant AML/CTF regulatory policies from time to time.
AML/CTF Rules	The *Anti-Money Laundering and Counter-Terrorism Financing Rules 2006* for the time being in force together with any regulations
ASIC	Australian Securities and Investments Commission
AUSTRAC	Australian Transaction Reports and Analysis Centre.
Board	The board of directors of Aurora.
CEO	A suitably qualified person engaged b y Aurora to carry out this role.
Corporations Act	*Corporations Act 2001* for the time being in force together with any regulations.
Customer Identification Management Agreement	A customer identification management agreement between Aurora and a Licensee Intermediary to govern the Customer Identification Procedure and which complies with the AML/CTF Rules.
Customer Identification Procedure	The customer identification procedure to be carried out on all clients as provided in clause 15 of this AML/CTF Program.
Designated Services	In relation to Aurora, Item 35 of table 1 of the AML/CTF Act, namely trading in securities and derivatives.
DFAT's Consolidated List	The list of persons or entities believed to be associated with terrorism which is maintained by the Australian Department of Foreign Affairs and Trade pursuant to the *Charter of the United Nations (Dealing with Assets) Regulations 2008*, reflecting Australia's commitment to financial measures under UN sanctions regimes and the terrorist asset freezing regime. The list is available at http://www.dfat.gov.au/icat/regulation8consolidated.xls.
Aurora	Aurora ACN Aurora, a reporting entity for AML/CTF purposes.
FinCEN	The Financial Crimes Enforcement Network of the United States Treasury Department, which is responsible for financial intelligence and analysis in the United States of America.
FINRA	The Financial Industry Regulatory Authority which is the largest independent regulator for all securities firms doing business in

	the United States.
FINRA Search	An online search of the U.S. Treasury's Office of Foreign Asset Control's (**OFAC**) Sanctions Program Listings for prohibited persons and organisations (ie, persons or entities listed on the OFAC website as 'Terrorists' and 'Specially Designated Nationals and Blocked Persons', as well as listed embargoed countries and regions). FINRA searches are available at http://apps.finra.org/rulesregulation/ofac/l/Defaultaspx.
Key Employee	The personnel referred to in clause 8.1(a).
KYC Information	'Know your customer information' as described in the AML/CTF Rules.
Licensee Intermediary	An Australian financial services licensee who arranges for the investor to receive a Designated Service from the Reporting Entity and is carrying out 'a designated service (item 54)' role.
Client (or client)	A person applying for services or a person currently named in the client register. Referred to in the relevant AML/CTF Obligations as a 'customer' being a person who acquires a Designated Service'.
ML/TF	Money laundering or terrorism financing.
PEP	Politically exposed person. The Financial Action Task Force defines a PEP as "individuals who are or have been entrusted with prominent public functions in a foreign country, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials. Business relationships with family clients or associates of PEPs involve reputational risks similar to those with PEPs themselves.
Program	This AML/CTF program including all annexures and schedules.
Red Flag	A red flag that possible ML/TF may be in existence, either at the time of application or as a result of ongoing customer due diligence, examples of which are set out in clauses 5.2 and 20.4.
Risk Assessment	The risk assessment model at Schedule 3 - Risk assessment.

Schedule 2

AML/CTF reporting structure



Schedule 3

Risk assessment

1 AML/CTF Obligations

The AML/CTF Obligations require a risk-based approach to AML/CTF compliance, meaning a commercial approach may be taken by Aurora, having regard to Aurora's business and the ML/TF risks Aurora may face. The risk-based approach places the onus on Aurora to identify and assess its ML/TF risks and to take appropriate measures to manage and monitor those risks.

Aurora has developed its risk assessment process having regard to:

(a) AUSTRAC's guidance note—Risk management and AML/CTF programs issued September 2007, and

(b) risk management standard AS/NZS 4360:2004 (and the related guidelines).

2 How risks are assessed

(a) Aurora assesses ML/TF risks by considering the 'consequence' and 'likelihood' of those risks arising based on the nature of its business (i.e. its product and services).

(b) To assess risk, Aurora has adopted the following matrix which sets out the relationship between risk and its components:

Likelihood	Minor	Major
Probable	**Medium risk**	**High risk**
Improbable	**Low risk**	**Medium risk**
	Consequence	

3 Risk evaluation

Aurora must evaluate each risk associated with the provision of the Designated Services and evaluate an 'inherent risk' rating i.e. an overall level of ML/TF risk that each new client, or each transaction when evaluated, may pose to Aurora. The 'inherent risk' rating assigned must be "high", "medium" or "low".

4 Risk mitigation and management (treatment)

(a) To mitigate the risk associated with the provision of the Designated Services, Aurora has implemented a number of controls, each of which are set out below.

(b) The 'residual risk' rating is the risk of ML/TF occurring after controls are taken into account. The 'residual risk' rating assigned must be "high", "medium" or "low".

5 Review of this model

Aurora must update this risk assessment model if it determines it necessary and as part of the annual review of Part A of this Program (refer to clause 11.2(a)). The risk assessment must also be updated to take into account additional risks and issues which may impact on the provision of Designated Services by Aurora. Additional risks and issues may be identified through a number of sources, such as Financial Action Task Force and FinCEN. The AML/CTF Compliance Officer will review the AUSTRAC website to determine if AUSTRAC requires a review of identified risks on a weekly basis.

Risk Assessment Model

Risk identification	Risk factors	Assessment		Evaluation	Treatment	
		Consequence	**Likelihood**	**Inherent Risk** (before controls)	**Control**	**Residual Risk** (after controls placed)
Product/service risk	The Designated Service is targeted as a high risk by regulators.	AUSTRAC may require a further risk assessment to be carried out and may require further KYC Information to be collected for clients.	Improbable	Low	Annual review of identified issues by AML/CTF Compliance Officer. Quarterly review of AUSTRAC website (or other sources).	Low
	The Designated Service involves a large volume of transactions.	A suspect transaction could slip through.	Probable	Medium	Risk awareness training will cause a Red Flag to be raised for suspicious transactions.	Medium
Client risk	The client is involved in a complex business ownership structure with no legitimate commercial rationale.	May be a vehicle for ML.	Improbable	Low	Such an occurrence may raise a Red Flag and enhanced due diligence at the oversight of the AML/CTF Compliance Officer is carried out.	Low
	The non-individual client (for example, a trust, company or partnership) has a complex structure with little commercial justification, which obscures the identity of ultimate beneficiaries of the client.	May be a vehicle for ML.	Improbable	Low	Such an occurrence may raise a Red Flag at the identification and verification stage and enhanced due diligence at the oversight of the AML/CTF Compliance Officer is carried out.	

Risk identification	Risk factors	Assessment		Evaluation	Treatment	
		Consequence	**Likelihood**	**Inherent Risk** (before controls)	**Control**	**Residual Risk** (after controls placed)
	The client is in a position which may expose them to the possibility of corruption.	May be more susceptible to ML.	Improbable	Medium	Where a Red Flag is raised in respect of a prospective client, that person will be subject to an AML/CTF check. PEPs (high risk clients) will (at the election of the AML/CTF Compliance Officer) be subject to enhanced due diligence.	Low
	An undue level of secrecy is requested regarding a designated service (including the identification and verification of the client).	May lead to ML or TF being undetected.	Improbable	Low	A request such as this would raise an immediate Red Flag and enhanced due diligence at the oversight of the AML/CTF Compliance Officer is carried out.	Low
	The beneficial owners of a non-individual client are difficult to identify and/or verify.	The non-individual client may be an entity created to facilitate ML/TF.	Improbable	Medium	Interests will not be issued where complete identification and verification has not been carried out. Where a client raises objections to identification and verification or creates too many difficulties, this may result in a Red Flag and enhanced due diligence is carried out.	Low
	There is a one-off transaction in comparison with an ongoing business relationship or series of transactions.	Could be a ML/TF event.	Improbable	Low	Inconsistent transactions will raise a Red Flag and will e identified as part of the transaction monitoring program.	Low

Risk identification	Risk factors	Assessment		Evaluation	Treatment	
		Consequence	**Likelihood**	**Inherent Risk** (before controls)	**Control**	**Residual Risk** (after controls placed)
	The client is represented by another person, such as under a power of attorney.	Leading to ML from a source that has not been fully and completely identified	Improbable	Low	A certified copy of the power of attorney must be provided along with all identification and verification material for the client. Where a client appoints an agent (not as an attorney) such an appointment is made on the application form (executed by the client) and executed by the agent.	Low
	The client is a PEP or other prohibited person.	The client may be more susceptible to ML.	Improbable	Low	Where a Red Flag is raised in respect of a prospective client, that person will be subject to an AML/CTF check. PEPs (high risk clients) will (at the election of the AML/CTF Compliance Officer) be subject to enhanced due diligence.	Low
Channel risks	The Designated Service allows for the acceptance of physical cash.	Unlawfully gained funds used to acquire Designated Services.	Probable	High	Aurora does not accept physical cash. Any such request raises a Red Flag.	Low
	Ability to transact using non face-to-face channels (higher risk for non-face-to-face).	ML can more easily be facilitated by use of forged documents.	Probable	High	Identification Checklist set out what materials are required. Risk awareness training provides training on documentary evidence. Identification/application form checklist provides a prompt for cross checking signatures.	Low

Risk identification	Risk factors	Assessment		Evaluation	Treatment	
		Consequence	**Likelihood**	**Inherent Risk** (before controls)	**Control**	**Residual Risk** (after controls placed)
Jurisdiction risks	The client or the beneficial owners of the non-individual client are resident in a high-risk jurisdiction.	Higher risk that the non-individual client may have been established as a vehicle for ML/TF.	Probable	Medium	Red Flag will be raised and client will be the subject of enhanced due diligence at the oversight of the AML/CTF Compliance Officer.	Low
	The client is based in, or conducting business through or in, a high-risk jurisdiction.	May be more susceptible to ML.	Probable	Medium	Where a Red Flag is raised in respect of a prospective client, that person will be subject to an AML/CTF check. PEPs (high risk clients) will (at the election of the AML/CTF Compliance Officer) be subject to enhanced due diligence AML/CTF Compliance Officer carries out annual risk assessment reviews incorporating an assessment of any information provided by AUSTRAC.	Low
Regulatory risks	Failure to include all mandatory legislative components in Aurora's policies and procedures.		Improbable	Medium	The AML/CTF program includes all mandatory legislative components as at date of issue. The AML/CTF program is reviewed on an annual basis.	Low
	Failure to gain Board approval of the AML/CTF Program.	Leading to a lack of commitment to this AML/CTF program at senior levels and no culture of compliance within Aurora.	Improbable	Low	The AML/CTF program has received Board approval. Further, all amendments are approved by the Board.	Low

Risk identification	Risk factors	Assessment		Evaluation	Treatment	
		Consequence	**Likelihood**	**Inherent Risk** (before controls)	**Control**	**Residual Risk** (after controls placed)
	Failure to undertake sufficient and appropriate employee due diligence.	Leading to potentially undesirable people holding positions that may facilitate ML/TF.	Improbable	Medium	The AML/CTF program has an employee due diligence program in place that is overseen by the AML/CTF Compliance Officer. See procedure in clause 8.2.	Low
	Failure to hold adequate risk awareness training.	Leading to employees failing to comply with Aurora's policies and procedures and a breach of law by Aurora.	Improbable	Medium	The AML/CTF program has a risk awareness training program in place that is overseen by the AML/CTF Compliance Officer. See procedure in clause 9.	Low
	Failure to monitor AUSTRAC website and consider feedback from AUSTRAC.	Leading to a failure to become aware and manage an emerging ML/TF risk.	Improbable	Low	AUSTRAC's website is monitored by the AML/CTF Compliance Officer on a regular basis. Aurora has an AUSTRAC liaison procedure in place to deal with AUSTRAC feedback.	Low
	Failure to adequately review and monitor the content and effectiveness of the AML/CTF program.	Leading to AML/CTF program not being changed to address risk.	Improbable	Low	The AML/CTF program is reviewed by an independent person (either internal or external) on an annual basis. The AML/CTF Compliance Officer AML/CTF Compliance Officer is to report to the Board quarterly on the content and effectiveness of the AML/CTF Program.	Low

Risk identification	Risk factors	Assessment		Evaluation	Treatment	
		Consequence	**Likelihood**	**Inherent Risk** (before controls)	**Control**	**Residual Risk** (after controls placed)
	Failure to incorporate changes in business functions in the AML/CTF Program (i.e. introduction of new product).	Leading to potential AML/CTF risks not being appropriately identified, mitigated and managed.	Improbable	Low	Any changes in business functions will be picked up in t he annual review of the AML/CTF program.	Low
	Failure to interpret and apply the AML/CTF Act and AML/CTF Rules correctly (such as for client identification procedures).	Leading to a breach of the obligations in the AML/CTF Act.	Improbable	Low	AML/CTF Compliance Officer has ongoing oversight of the client identification procedure and will undertake a review of the AUSTRAC website on a regular basis.	Low
	Client identification procedures fails to:					
	(i) prompt for further identification and/or verification when the ML/TF risk posed by a client increases;	Leading to ML/TF activities going unchecked.	Improbable	Low	Where a Red Flag is raised pursuant to the risk assessment training, the client risk increases. Red Flags must be reported to the AML/CTF Compliance Officer who will advise on need for enhanced due diligence. Further, the transaction monitoring program will assist in the identification of risks.	Low

Risk identification	Risk factors	Assessment		Evaluation	Treatment	
		Consequence	**Likelihood**	**Inherent Risk** (before controls)	**Control**	**Residual Risk** (after controls placed)
	(ii) detect where a client has not been sufficiently identified and prevent the client from receiving the Designated Service;	Leading to a breach of the AML/CTF Act and AML/CTF Rules and potential ML/TF.	Improbable	Low	The AML/CTF Identification Checklists are very specific in relation to what documentation is acceptable. Unless a client has been adequately identified and verified, no interest will be issued to that client.	Low
	(iii) take appropriate action where a client provides insufficient or suspicious information in relation to the identification check;	Leading to a breach of the AML/CTF Act and the AML/CTF Rules and potential ML/TF.	Improbable	Low	The AML/CTF Identification Checklists are very specific in relation to what documentation is acceptable. Unless a client has been adequately identified and verified, transactions will be conducted with that client. Any suspicious information will prompt a Red Flag and enhanced due diligence to be carried out.	Low
	(iv) take appropriate action where the identification document provided is neither an original nor a certified copy;	Potential that the documentation is false.	Improbable	Low	The AML/CTF Identification Checklists are very specific in relation to what documentation is acceptable. This includes a check box/requirement for original and certified copies.	Low

Risk identification	Risk factors	Assessment		Evaluation	Treatment	
		Consequence	**Likelihood**	**Inherent Risk** (before controls)	**Control**	**Residual Risk** (after controls placed)
	(v) recognise foreign documentation issued by a high-risk jurisdiction;	Potential that the documentation is false.	Improbable	Medium	The AML/CTF Identification Checklists are very specific in regard to what foreign documentation is acceptable. Clients from high-risk jurisdictions are subject to enhanced due diligence which will scrutinise foreign documentation.	Low
	(vi) record comprehensive details of identification documents;	Leading to an inability to carry out a thorough independent review.	Improbable	Medium	The AML/CTF Checklists are very specific in relation to what records are recorded.	Low
	(vii) consult appropriate resources in order to identify high-risk clients;	High risk clients may not be identified as such and hence not suspect to additional due diligence.	Probable	Medium	Where a Red Flag is raised in respect of a prospective client, that person will be subject to an AML/CTF check. PEPs (high risk clients) will (at the election of the AML/CTF Compliance Officer) be subject to enhanced due diligence.	Low
	(viii) identify when an expired or old identification document has been used; or	Expired or old documents may be used to circumvent the AML/CTF Act in respect to client identification and verification.	Improbable	Low	Key employees ensure documentation supplied under the PDS Identification Requirements are not expired.	Low

Risk identification	Risk factors	Assessment		Evaluation	Treatment	
		Consequence	**Likelihood**	**Inherent Risk** (before controls)	**Control**	**Residual Risk** (after controls placed)
	(ix) Client Acceptance of documentation that may not be readily verifiable.	Leading to a client that has not been adequately identified and verified receiving a Designated Service.	Improbable	Low	The AML/CTF Identification Checklists are very specific in relation to what documentation is acceptable. Unless a client has been adequately identified and verified, no transactions will be conducted with that client.	Low
Overall risk evaluation **Inherent risk rating**		**Residual risk rating**				
Aurora has assessed the overall inherent ML/TF risk posed by its clients and transactions in providing the Designated Services to be medium.		Overall, after following the procedures set out below, Aurora considers the residual ML/TF risk can be categorised as 'medium' because of the following: Aurora verifies all client identities. Designated Services are only provided in respect of identified clients. Where a client is a trust, the client identification procedures require identification of the beneficiaries or their class of holding in the trust.				