AlgoCandy

AML / CPF / CFT Compliance Knowledge Map

For Singapore CSPs

ALgoCandy

A one-stop AML/CPF/CFT compliance platform built for Singapore CSPs, helping corporate service providers improve CDD efficiency, reduce compliance risk and deliver a better client experience.

Produced by AlgoCandy

1 Risk Assessment

Risk Assessment Requirements

- **Must identify, assess and understand ML/PF/TF risks**
  The scope includes customers, countries or jurisdictions, place of business, corporate services provided, products and transactions.
- **Must document risk assessment results**
  Relevant risk factors should be considered before determining customer risk ratings, the extent of CDD measures and risk mitigation measures.
- **Must keep risk assessments and controls up to date**
  Relevant records must be made available when required by the authorities.

Situations Requiring Enhanced CDD and Risk Controls

- High-risk customers
- Non-face-to-face transactions
- FATF blacklisted / greylisted or other high-risk jurisdictions
- Company incorporation with no apparent commercial or lawful purpose
- Involvement of nominee directors or nominee shareholders

Key Risk Factors to Consider

2 Customer Identity Verification

Identity Verification Requirements

- Must identify each customer and the customer's agent
- Must verify identity using reliable and independent sources
- Must retain copies of identity verification documents

Information Required for Identity Verification

- Name
- Address
- Contact details
- Identification number /registration number
- Date of birth / incorporation / registration
- Nationality / dual nationality / place of registration

Customer Is a Company or Other Legal Entity

Must identify and record relevant directors, sole proprietors, partners, or persons with executive authority.

Transaction Involves Setting Up a Company or Other Legal Person

Must identify the proposed directors, or persons holding equivalent positions in the relevant legal person, and understand its legal form, constitutional documents and management powers.

3 Beneficial Owner Identification and Verification

Must Inquire Whether Beneficial Owners Exist

- If beneficial owners exist, they must be identified
- Their identity must be verified using reliable source information or data

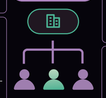
Customer Is a Legal Person, Legal Arrangement or Unincorporated Body

- Must understand its business nature, ownership structure and control structure
- Must consider shareholding structure, control chain, cross-shareholdings and aggregated holdings when identifying beneficial owners

BO Identification Exemption for Certain Low-Risk Customers

- Includes eligible listed entities, financial institutions, and investment vehicles managed by qualifying financial institutions
- Includes confirmed Singapore government entities
- If there are doubts about the accuracy of information, or suspicion of ML/PF/TF, relevant CDD measures must still be performed

Beneficial Owner



For Legal Person Customers, Identify in Order

- Natural persons who ultimately own the assets or business
- If none can be identified, natural persons who ultimately control or exercise ultimate effective control
- If still not identifiable, natural persons with executive authority or equivalent positions.

Legal Arrangement Customers e.g. Express Trusts

- Identify the settlor, trustee, protector, beneficiaries or class of beneficiaries
- Identify any natural person who ultimately owns or controls the legal arrangement
- For other legal arrangements, identify persons in equivalent or similar positions

CDD records for identifying and verifying beneficial owners must be retained, together with written records supporting the exemption assessment, and provided to ACRA when required.

4 Customer Screening

Persons to Be Screened

- Customer
- Agent
- Related parties
- Beneficial owners

Screening Scope

- Lists and information provided by the Registrar and relevant law enforcement agencies
- Other ML/PF/TF-related information sources designated by the Registrar

Screening Channels

- Public search tools
- Commercial databases
- Other reliable sources

Check whether the customer and relevant persons are linked to adverse news, and consider screening results in the customer risk assessment.

Screening Requirements

- Whether the person is a designated person under United Nations sanctions
- Whether the person is a terrorist or terrorist entity under the Terrorism (Suppression of Financing) Act 2002

Records to Keep

- Screening results
- Relevant decisions
- Basis of assessment

For example, retain search screenshots, printouts or system records to evidence that screening has been completed.

For ongoing business relationships, screening should be conducted periodically based on the customer's risk level. If relevant lists or information are updated, re-screening should be performed promptly.

AlgoCandy

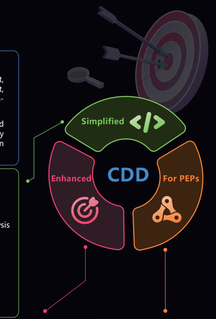
5 CDD Measures

Risk-Based CDD Measures

- Must apply CDD measures according to the customer risk assessment, including identification and verification of the customer and agent, identification and verification of beneficial owners, customer screening, and simplified or enhanced CDD where applicable.
- When determining the extent of CDD measures, the CSP should consider the customer's risk level. CDD measures previously performed, and whether existing documents, data or information remain adequate, accurate and current.

Simplified CDD Measures

- Simplified CDD may be applied where the customer is assessed as lower risk
- The lower-risk assessment must be supported by sufficient risk analysis
- Simplified CDD must not be applied where the customer is from or located in a relevant high-risk country or jurisdiction
- Eligible MAS-regulated financial institution customers may apply simplified CDD based on risk assessment
- Must record the customer risk assessment details, assessment date, and simplified CDD measures applied



CDD Record Keeping

- Must retain all records obtained through CDD measures
- Records must be kept for 5 years from the date the CSP ceases to provide corporate services to the customer
- Records should be sufficient to reconstruct individual transactions, including transaction amount and currency

Ongoing Monitoring and Enhanced Ongoing Monitoring

- Must conduct ongoing monitoring of each customer business relationship
- Enhanced ongoing monitoring must be applied in higher-risk situations
- The responsibility for ongoing monitoring remains with the CSP and must not be fully delegated to a third party.

CSPs should monitor changes to FATF blacklists and greylists, and update screening standards, risk assessment rules and IPPC accordingly.

CSPs should keep customer information up to date. Expired identity documents or changes in customer information should be updated promptly.

Enhanced CDD Measures

Enhanced CDD measures must be applied where higher risks are identified.

Situations Requiring Enhanced CDD Include

- Complex or unusually large transactions
- Unusual transaction patterns with no apparent economic or lawful purpose
- Customer is from or located in a relevant high-risk country or jurisdiction
- Customer or transaction is assessed as high risk
- Customer lacks an apparent operational or commercial purpose
- Involvement of PEPs
- Other higher-risk situations

Enhanced CDD Measures Include

- Obtaining more information on the customer and beneficial owners
- Understanding the purpose of the business relationship
- Examining the background and purpose of transactions
- Verifying source of wealth and source of funds
- Obtaining senior management approval
- Enhancing ongoing monitoring

Enhanced CDD for PEPs

Principles

- A risk-sensitive approach may be used to decide whether, and to what extent, enhanced CDD should be applied to certain PEPs, their immediate family members or close associates.
- Foreign PEPs, their immediate family members and close associates should generally be treated as high risk, subject to enhanced CDD and enhanced ongoing monitoring.
- Where the transaction or corporate service presents higher risks, a risk-sensitive approach alone should not be applied. The CSP should apply enhanced CDD measures.

Scope of Politically Exposed Persons, PEPs

- Individuals who hold or have held prominent public functions in Singapore
- Individuals who hold or have held prominent public functions outside Singapore
- Individuals who are or have been entrusted with prominent public functions by international organisations
- Immediate family members and close associates of the above persons

6 Remote Transactions — Live Video Call

Remote Transaction Measures

- Where the customer has not met the CSP face to face, the transaction is regarded as non-face-to-face or "not in the physical presence" of the CSP
- This applies whether the customer is a foreigner, Singapore citizen or permanent resident
- Where corporate services involve company incorporation, or the transfer or sale of management or ownership of a shelf company, a live video call must be conducted
- A live video call cannot simply be replaced by notarised documents, e-signatures or third-party identity verification tools
- For non-face-to-face appointment of directors, the CSP must confirm that the proposed director consents to act and personally signs Form 45

Persons Required for the Live Video Call

- At least one proposed director, excluding nominee directors
- At least one proposed member holding not less than 50% of the voting rights in the proposed company
- If the proposed member is a legal person, the live video call should be conducted with its individual authorised representative.

Record Keeping Requirements

- Must keep records sufficient to evidence compliance
- ACRA does not require video recording
- Must retain screenshots of the live video call
- More complete process records are recommended

7 Internal Policies, Procedures and Controls IPPC

Must Establish and Maintain Appropriate IPPC

- CDD measures
- Ongoing monitoring
- Customer screening
- Reporting
- Record keeping
- Internal audit
- Risk assessment and management
- Internal communication
- Employee hiring and training
- Compliance monitoring

IPPC should cover

Key Mechanisms Required Under IPPC

- Mechanisms to identify and examine complex or unusually large transactions, and unusual transaction patterns with no apparent economic or lawful purpose
- Risk assessment and measures for new products, new business practices, new delivery mechanisms, and new or developing technologies
- Mechanisms to identify whether the customer, customer's agent or beneficial owner is a PEP
- IPPC should consider the CSP's ML/PF/TF risks and business scale, and be tailored to its business circumstances
- Senior management should participate in and approve the IPPC to ensure it is suitable for actual operations and effectively implemented
- Where the CSP has branches or subsidiaries, group-wide ML/PF/TF controls must be developed and implemented as required
- The effectiveness of IPPC must be assessed periodically to ensure relevant measures can effectively prevent ML/PF/TF risks
- External auditors or external audit firms may be engaged to audit the IPPC
- A sole proprietor CSP acting as compliance officer should not also act as internal auditor, and should appoint an independent third party to conduct the audit
- Must establish compliance management arrangements, review and update IPPC on an ongoing basis, and appoint a compliance officer responsible for AML/CPF/CFT compliance matters

8 Suspicious Transaction Reporting STR

Must Establish STR Procedures

- Reporting persons
- Reporting channels
- Information to be included in an STR
- Submission timelines

Where a senior officer, QI or employee knows or has reasonable grounds to suspect that any property may be connected with ML/PF/TF, the matter should be reported or escalated promptly to the compliance officer or senior management.

STR Handling Timelines

The compliance officer or senior management should assess whether an STR should be filed with STRO.

Generally, an STR should be filed as soon as practicable after suspicion is formed, and no later than 5 business days;

For high-risk situations involving TFS/sanctions, filing should be made within 1 business day

Where necessary, filing should be made immediately.

STRs may be filed electronically via the SONAR platform. If a decision is made not to file an STR, the reasons must be recorded and provided to the Registrar when required.

9 Employee Hiring and Training

Must establish employee screening procedures to ensure suitable persons are hired. This may include considering whether the person has been involved in fraud or dishonesty offences, past conduct and compliance records.

Must ensure employees receive AML/CPF/CFT training

- Relevant legal requirements
- ML/PF/TF risks and trends
- Registered CSP's IPPC
- CDD and ongoing monitoring measures
- PEP risk identification
- Identification and handling of suspiciousactivities and transactions

Training frequency should be sufficient to ensure employees can properly perform their compliance duties, and should be conducted at least annually.

Registered CSPs must retain written records of employee screening and training measures.

10 Nominee Director Arrangements

Requirements for Arranging Nominee Directors

- When arranging for a person to act as a nominee director by way of business, the CSP must ensure that the person is fit and proper.
- Unless the nominee director is itself a CSP, a person acting as a nominee director by way of business must be arranged by a CSP.
- The fit and proper assessment requirement does not apply to persons already appointed as nominee directors before the Corporate Service Providers Act 2024 came into force.
- For each nominee director arrangement, the CSP must ensure that the person arranged meets the fit and proper requirements, and retain the supporting basis for the assessment.

Fit and Proper Assessment for Nominee Directors

Key considerations include whether the person has been involved in fraud, dishonesty, money laundering, terrorism financing, sanctions, company law breaches or other relevant offences; whether the person is an undischarged bankrupt; and whether the person has good past conduct and compliance records.

The CSP should also consider whether the person has the qualifications, ability and practical capacity to perform directors' duties, including whether the person understands directors' duties, is mentally fit to take on the role, has excessive existing commitments, and whether the number of existing directorships affects the person's ability to discharge duties.

Generally, the person's compliance history over the past 5 years should be considered. If the person already holds a large number of nominee directorships, for example more than 50, the CSP should further assess whether the person can still take on additional directorships, and recommend additional directors' duties training.

Disclaimer: This material is prepared by AlgoCandy based on publicly available ACRA materials. It is for learning and general reference only and does not constitute legal or compliance advice. Actual requirements should be based on the latest requirements of ACRA and applicable Singapore laws and regulations.