July 2023

ACRA
Accounting And Corporate Regulatory Authority

Strengthening AML/CFT Controls for Corporate Service Providers (CSPs)

Key Findings and Best Practices from Inspections and Reviews Conducted in 2021 and 2022

Introduction

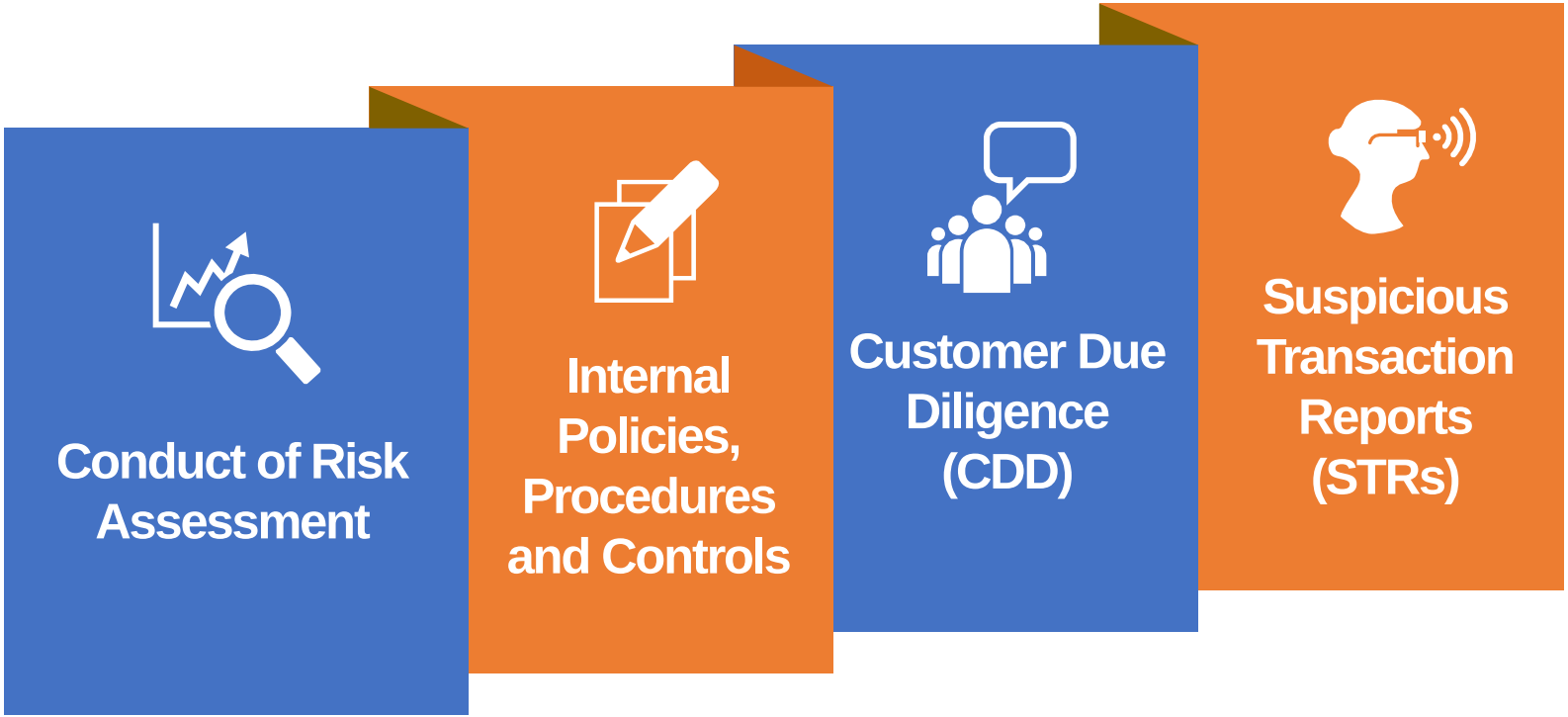
- Singapore is an international financial centre and global trading hub. Business entities, particularly companies, play a pivotal role in supporting commercial and entrepreneurial activities in Singapore.

- CSPs are a key touchpoint in facilitating the creation of business entities in Singapore, particularly where foreign customers are involved. Hence, they are inherently exposed to higher money laundering, terrorism financing and proliferation financing (ML/TF/PF) risks.

- CSPs face greater risk when they provide services involving (i) the use of their address; (ii) nominee arrangements; (iii) facilitating the creation of corporate bank accounts, particularly for foreign customers.

- ACRA has sieved out key findings and best practices from inspections and reviews conducted in 2021 and 2022. As CSPs play a critical gatekeeper role against ML/TF/PF, CSPs are expected to study and incorporate relevant best practices in a manner proportionate to the risk profile of their business activities and customers.

Key Areas of AML/CFT Control Weaknesses - CSPs



Inadequate Conduct of Risk Assessment

Risk assessments enable CSPs to identify and assess their ML/TF/PF risk exposure and to take relevant measures to mitigate such risks.

CSPs are required to:

- Take appropriate steps to identify and assess their exposure to ML/TF/PF risks and to take relevant steps to mitigate the risks identified.
- Document and keep their risk assessment up-to-date.

Key Weaknesses Observed

- No conduct of risk assessment.
- Inadequate conduct of risk assessment due to:
  - Failure to consider all relevant risk factors.
  - Inadequate differentiation of the levels of ML/TF/PF risk exposure arising from the different risk factors identified.
  - Failure to conduct enhanced due diligence (ECDD) measures to mitigate identified risks posed by higher-risk customers and/or transactions.
  - Failure to identify customers from jurisdictions in the FATF's latest black and grey lists and to subject them to ECDD measures.

Best Practices

- When assessing ML/TF/PF risks posed by customers or transactions, the following factors are also considered: (i) whether the customers are new/returning; (ii) jurisdictional risk (including consideration of whether the customer is local/foreign/based in Singapore and where a foreign customer is involved, the country the customer is from/based in); and (iii) whether there appears to be a genuine economic purpose behind the transaction/s.
- Update the risk assessment periodically to ensure that it is up-to-date. For example, updating the CSP's list of high-risk jurisdictions whenever it is alerted to an update to the FATF's black and grey list (may be obtained through a subscription to MAS' website).

Inadequate Internal Policies and Procedures and Controls (IPPC)

An adequate IPPC provides a framework which documents how CSPs discharge their responsibilities in relation to preventing ML/TF/PF and provides direction for such prevention.

- CSPs are required to establish and maintain detailed, up-to-date and risk sensitive IPPC. Minimally, this should be in line with Annex A of the AML/CFT Guidelines for RFAs.
- CSPs should regularly review and update their IPPC to ensure that it remains relevant to tackle key risk concerns and is in line with prevailing AML/CFT obligations.

Key Weaknesses Observed

- IPPC not formally documented and/or not comprehensive.
- Measures set out in the IPPC are not consistently applied.
- IPPC has not been updated since it was first established.

Best Practices

- IPPC refreshed periodically.
- Provide additional guidance within the IPPC. For example:
  - Elaborate on what constitutes higher-risk customers/transactions (as tailored to the CSP's risk profile and the sector's key risk concerns) and establish pertinent measures to deal with such customers/transactions.
  - Measures to take when dealing with a customer featuring red flags and/or who is unwilling or unable to provide requisite CDD information.
  - Establish the rationale for and provide guidance on when ECDD and STR filing is warranted.

More Robust Conduct of CDD Required

CDD enables the CSP to identify and verify its customers (and their beneficial owners) and establish the purpose and intended nature of the business relationship/transaction.

- CSPs are required to conduct CDD for all designated transactions, when they have reason to suspect that there is ML/TF/PF or when they doubt the veracity/adequacy of previously obtained documents/information.
- All CDD conducted should be properly documented.

Key Weaknesses Observed

- CDD not conducted on designated transactions.
- For non-individual customers such as corporate customers, CDD was not performed on the beneficial owner/s of the corporate.
- CDD not refreshed for returning customers (whose CDD documents are now dated and/or whose identification documents are now invalid).
- CDD documents not properly documented and/or not properly maintained.

Best Practices

- Where non-individual customers are involved (including those with complex structures featuring cross-jurisdictional elements), the ultimate beneficial owner/s are all identified and verified. The purpose and legitimacy of the use of such a structure is also established.
- Valid government-issued identification is sighted (for example, expired passports are rejected) and a copy is collected on the customer and its beneficial owner/s.
- Perform screening of all relevant parties (using valid government-issued identifiers) against commercial screening databases and pertinent listings. This also supports compliance with regulations for Targeted Financial Sanctions as well as ECDD requirements.

More Robust STR Procedures Required

STR filing is required when CSPs know or have reasonable grounds to suspect that any property may be connected to criminal activity.

- CSPs must have procedures for their employees to report or escalate suspicious transactions.
- Where necessary, STRs should be lodged in a timely manner (as soon as reasonably practicable).

Key Weaknesses Observed

- Insufficient information was obtained from customers or transactions to support (i) the filing of an STR, when there may have been grounds to suspect criminal activity; (ii) the filing of a more meaningful STR.
- STR not filed despite there being some grounds to suspect criminal activity.
- STR was not filed promptly, for example, due to a delay brought about by internal escalation processes.

Best Practices

- Provide additional guidance for employees on:
  - Red flag indicators, key risk concerns and typologies to which they should be alert to. These should be periodically refreshed.
  - Clear procedures for employees to escalate suspicious transactions (including information which should be made available in the STR) and timelines for such transactions to be reviewed/decision to be made on whether an STR should be filed.
- Where there are grounds to suspect criminal activity and a decision is made not to file an STR, the basis for the non-filing is documented.

Case study

CSP A was engaged by Customer B to help it to incorporate 14 companies. During ACRA's inspection of CSP A, ACRA found that CSP A had failed to perform CDD adequately. In particular, CSP A had failed to identify and verify the ultimate beneficial owners of the newly incorporated companies and did not adequately establish the purpose and legitimacy of Customer B's requested transactions. Some of the companies were subsequently found to be used as conduits for the laundering of criminal proceeds from scams. ACRA established that CSP A had committed 29 severe AML/CFT breaches, including:

- Failing to inquire on the existence of any beneficial owner;
- Failing to document the details of its risk assessment when performing due diligence measures;
- Failing to conduct on-going monitoring of every business relationship with a customer; and
- Failing to establish and maintain appropriate and risk-sensitive IPPC to prevent activities related to ML/TF/PF.

ACRA cancelled CSP A's registration and barred it from acting as a CSP for a period of two years.

Conclusion

While there has been an overall improvement in the strength and coverage of AML/CFT controls for the CSP sector, there is still room for improvement.

CSPs should maintain robust AML/CFT controls and ensure that the risk mitigation measures they have in place are up-to-date and effective.

ACRA expects the directors/owners/partners and senior management of CSPs to maintain adequate oversight and risk management standards.

CSPs should study and incorporate relevant best practices, in a manner proportionate to the risk profile of their business activities and customers.

Thank you

www.acra.gov.sg

Connect with us:

facebook.com/SG.ACRA

go.gov.sg/LinkedIn-ACRA

instagram.com/ACRA_SG

youtube.com/ACRAadmin

Scan Me!