AML/CFT Industry Partnership

Best practices for banks to manage money laundering, terrorism financing and proliferation financing risks associated with receiving referrals from corporate service providers

February 2024

Contents

1. Introduction

1.1. Background

ACIP Legal Persons and Arrangements Working Group (LPA WG)

The misuse of Legal Persons and Arrangements (LPA) remains a priority risk for Singapore. The LPA WG was set up under ACIP to strengthen the industry's understanding of risks associated with the misuse of LPA (including use of complex structures, front and shell companies, trusts, and other arrangements). This best practices paper is produced as part of the LPA WG's ongoing work to address such risks.

As observed in international and domestic typologies, Corporate Services Providers (CSP) have, in some instances been utilised by criminal elements to aid in the incorporation of shell and front companies (including via the provision of nominee directors by CSPs) and misused for illicit purposes. CSPs have also facilitated setting up of bank accounts to enable these companies to receive or move illicit proceeds. It has also been observed[1] globally that CSPs, among other professionals[2], may knowingly or unknowingly facilitate ML/TF/PF and other financial crime activities. Domestically, CAD has observed a range of companies, including front, shelf[3] and shell companies, which were misused in both domestic and foreign-predicate ML cases involving fraud, tax evasion and trade-based money laundering and sanctions evasion (or PF). In several cases, the incorporation of Singapore companies and/or setting up of bank accounts were facilitated by CSPs.

The LPA WG has thus looked into the role of CSPs and collated a set of best practices for banks (and the broader financial sector) to consider applying when they take referrals from CSPs in the setting up of banking relationships for their customers. This paper describes the collated best practices.

Corporate Service Providers

Under the Financial Action Task Force (FATF) glossary[4], Trust and Company Service Providers refers to all persons or businesses that are not covered elsewhere under the FATF Recommendations, and which as a business, provide any of the following services to third parties:

i. Acting as a formation agent of legal persons;

ii. Acting as (or arranging for another person to act as) a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons;

iii. Providing a registered office; business address or accommodation, correspondence or administrative address for a company, a partnership, or any other legal person;

iv. Acting as (or arranging for another person to act as) a trustee of an express trust or performing the equivalent function for another form of legal arrangement; and

v. Acting as (or arranging for another person to act as) a nominee shareholder for another person.

This paper focuses on CSPs providing services (i), (ii), (iii) & (v) above. (iv) is not covered in this paper as such service providers would not be CSPs in Singapore's context. Instead, they are subject to MAS' AML/CFT requirement as trust companies, and supervised as financial institutions.

In Singapore, persons and business entities providing such services (i.e. those described under (i), (ii), (iii) & (v) above), are required to be registered[5] with the Accounting and Corporate Regulatory Authority (ACRA) and

[1] FATF paper titled "Professional Money Laundering" (July 2018)
[2] Other professionals featured in the FATF paper include accountants, lawyers, trust service providers, banks, money value transfer service providers, brokers, fiscal specialists/tax advisors etc.
[3] A shelf company is an incorporated company with inactive shareholders, directors, and secretary and is left dormant for a longer period even if a customer relationship has not already been established.
[4] Please see definition of the term "trust and company service providers" within "Designated Non-Financial Businesses and Professions" in the FATF Glossary (https://fatf-gafi.org/en/pages/fatf-glossary.html)
[5] As Registered Filing Agents, under Part 2 of the First Schedule of the ACRA (Filing Agents and Qualified Individuals) Regulations 2015.

to comply with anti-money laundering, countering the financing of terrorism (AML/CFT) requirements. Other professional service providers like lawyers and accountants that may assist their customers with the above-mentioned services, such as to set up companies, would also have to be registered with ACRA and be subject to its regulation and supervision. This is in addition to their respective AML/CFT obligations as a lawyer or an accountant where they are separately supervised by their respective supervisor.

Other jurisdictions outside of Singapore may have different standards and regulatory frameworks for such CSPs. The scope of this paper includes interactions with foreign CSPs as well as local CSPs, and some subsequent sections elaborate on the recommended approaches towards local and foreign CSPs.

1.2. Objectives

The LPA WG prepared this paper with the objective of:

- Raising banks' awareness on the potential ML/TF/PF risks involved in collaborating with CSPs by providing an overview of:
  - The risks that may arise from receiving customer referrals from CSPs; and
  - The AML/CFT controls framework that they should expect partner CSPs to have in place to comply with regulatory requirements; and
- Providing recommendations that banks may impose, to effectively mitigate ML/TF/PF risks that they may be exposed to, through receiving customer referrals from CSPs.

Banks are reminded to file a Suspicious Transaction Report (STR) to the Suspicious Transaction Reporting Office (STRO) if, in the course of your trade, profession, business or employment, you know or have reasonable grounds to suspect that any property may be connected to a criminal activity. Should your institution file a STR on an activity identified as a result of this ACIP product, please include the reference code "**ACIP_CSPBPP_2024**" in the "Notice Reference Number" field in the <Reporting Institution> tab in the STR form. This will facilitate authorities' review and monitoring.

1.3. Sources

This paper is compiled by the core members of the Legal Persons WG. Members comprise representatives from commercial banks conducting business in Singapore. Contributions were also obtained from ACRA, MAS, CAD, and Oliver Wyman, a consulting firm.

Reference was also taken from relevant international papers such as those published by the FATF.

1.4. Scope

This paper applies to banks that receive customer referrals from all entities providing FATF-defined CSP services in Singapore and overseas.

Currently, banks are required to conduct robust due diligence on the customers as well as apply controls (e.g., to identify shell/front company indicators); banks would typically require customers to declare any relationships with CSPs, and/or perform data analytics to identify such relationships (e.g., common address and director analysis). However, there may be circumstances where banks' due diligence does not reveal if the customer has any relationship with a CSP (apart from circumstances where the customer is referred by a CSP to the bank) or has engaged a nominee director. In such circumstances, the expectations are for the recommendations in this paper to be applied to the extent operationally feasible and in line with the banks' current AML/CFT controls. Notwithstanding this, banks should remain apprised of the risks associated with collaborating with CSPs, and ensure it understands its risk exposure within its customer base, and apply adequate controls as guided by this paper to manage such risks.

2. Key risks which can potentially be introduced to banks from receiving customer referrals from CSPs

Two key means in which CSPs could potentially introduce risks to banks are set out as follows:

- Typology 1: The CSP may **unknowingly**, in spite of complying with regulatory requirements of customer due diligence (CDD), due to false documentation and/or declarations provided by the customer, **take on a customer that is involved in ML/TF/PF and refers said customer to the bank**. In this instance, both the CSP and the bank are being misused for ML/TF/PF.
- Typology 2: The CSP is complicit with the customer and **knowingly refers said customer to the bank** despite being aware of potential ML/TF/PF activities and hence the bank is unknowingly exposed to the collusion between the CSP and the prospective customer. For example: the bank may, in spite of complying to regulatory requirements of CDD, unwittingly rely on false documentation and/or declarations provided by the prospective customer and decide to onboard the customer.

In both scenarios above, the risk is elevated for foreign CSPs which may be subject to differing (and sometimes weaker) AML/CFT requirements and/or supervision.

Case study for typology 1: CSP may unknowingly take on a customer that is involved in ML/TF/PF

A CSP ("CSP A") provides corporate secretarial services to small and medium-sized enterprises. CSP A helps to incorporate companies on behalf of customers and arranges for individuals to act as the resident director of these incorporated companies.

CSP A incorporated a company ("Company B") on behalf of a foreign customer after conducting due diligence. CSP A also appointed one of its employees ("Individual C") as a resident director of Company B. Individual C was tasked by the foreign customer to approach a Singapore bank ("Bank D") on behalf of Company B to open a banking account for the company. At the bank account opening stage, Bank D proceeded to perform CDD on Company B as per MAS 626 Notice requirements. In the interview with Company B, the resident director declared on Company B's behalf, that the purpose of establishing a banking relationship in Singapore was to engage in business activity.

Upon the establishment of the relationship, Bank D noticed that there were large volumes of transactions moving in and out of Company B's account. These included cross-border transactions to a variety of jurisdictions. Subsequently, there were fund recall requests from banks which these transactions originated from. Further investigation by the bank found that these transactions involved proceeds from ML/TF/PF activities.

This case study demonstrates the risk of CSPs being misused, **and lack of awareness and knowledge by Individual C who was acting as a resident director of Company B that facilitated the opening of** a corporate bank account for foreign criminal elements for illicit purposes.

Case study for typology 2: Foreign CSP knowingly creating shell companies for ML

Person R, a foreign professional intermediary, personally recruited foreign individuals resident in Singapore, to become directors of shell companies in Singapore. Thereafter, Person R provided these resident directors with forged documents to open bank accounts in Singapore for these shell companies. A criminal syndicate paid Person R between US$1,500 and US$5,000 for each company he successfully incorporated.

Between August 2016 and March 2017, CAD received several complaints from foreign victims based in the United States, Australia, Hong Kong etc. These victims had fallen prey to spoofed emails purportedly sent by their business associates and wired a total sum of US$660,817.50 into 6 corporate bank accounts in Singapore. Investigations revealed that Person R facilitated the opening of these bank accounts. CAD further identified 19 other local shell companies related to Person R, and seized more than US$1.1 million in 15 bank accounts.

In October 2019, Person R was convicted of 8 counts of money laundering offences and 22 counts of forgery offences, and was sentenced to 88 months' imprisonment.

This demonstrates how CSPs may knowingly refer customers to banks to facilitate ML activities, highlighting the importance of banks putting robust AML/CFT controls in place.

Although receiving customer referrals from CSPs can potentially introduce risks to banks, it should be noted that the root of such risk frequently originates from the underlying customer. As such, **banks are reminded that all customers, CSP-referred or otherwise, must be subject to robust CDD checks**, in compliance with the requirements set out in MAS 626 Notice, its associated Guidelines and relevant MAS' guidance, and the banks' internal policies and procedures. These controls should include identification and verification of the customer's identity, unwrapping of complex structures to identify beneficial owners of the customers, establishing source of wealth and source of funds of customers, name screening, customer risk rating etc., and be supplemented by ongoing monitoring and periodic reviews. Best practices that banks could put in place to better address risks arising from the misuse of legal persons are also detailed in MAS' publication titled "Effective Practices to Detect and Mitigate the Risk from Misuse of Legal Persons" (June 2019)[6] as well as MAS' Information Paper titled "Effective Use of Data Analytics to Detect and Mitigate ML/TF risks from the Misuse of Legal Persons" (June 2023)[7].

[6] *"Effective Practices to Detect and Mitigate the Risk from Misuse of Legal Persons" (June 2019);* effective-practices-to-detect-and-mitigate-the-risk-from-misuse-of-legal-persons-june-2019.pdf (mas.gov.sg)

[7] *"Effective Use of Data Analytics to Detect and Mitigate ML/TF risks from the Misuse of Legal Persons" (June 2023)* effective-use-of-data-analytics-to-detect-and-mitigate-mltf-risks-from-the-misuse-of-legal-persons.pdf (mas.gov.sg)

3. Recommendations on how banks can manage ML/TF/PF risks associated with receiving referrals from CSPs

To manage and mitigate the specific risks described above, which could arise from receiving referrals from CSPs, banks could establish an additional controls framework. An illustration of the controls framework that may be imposed is set out below:

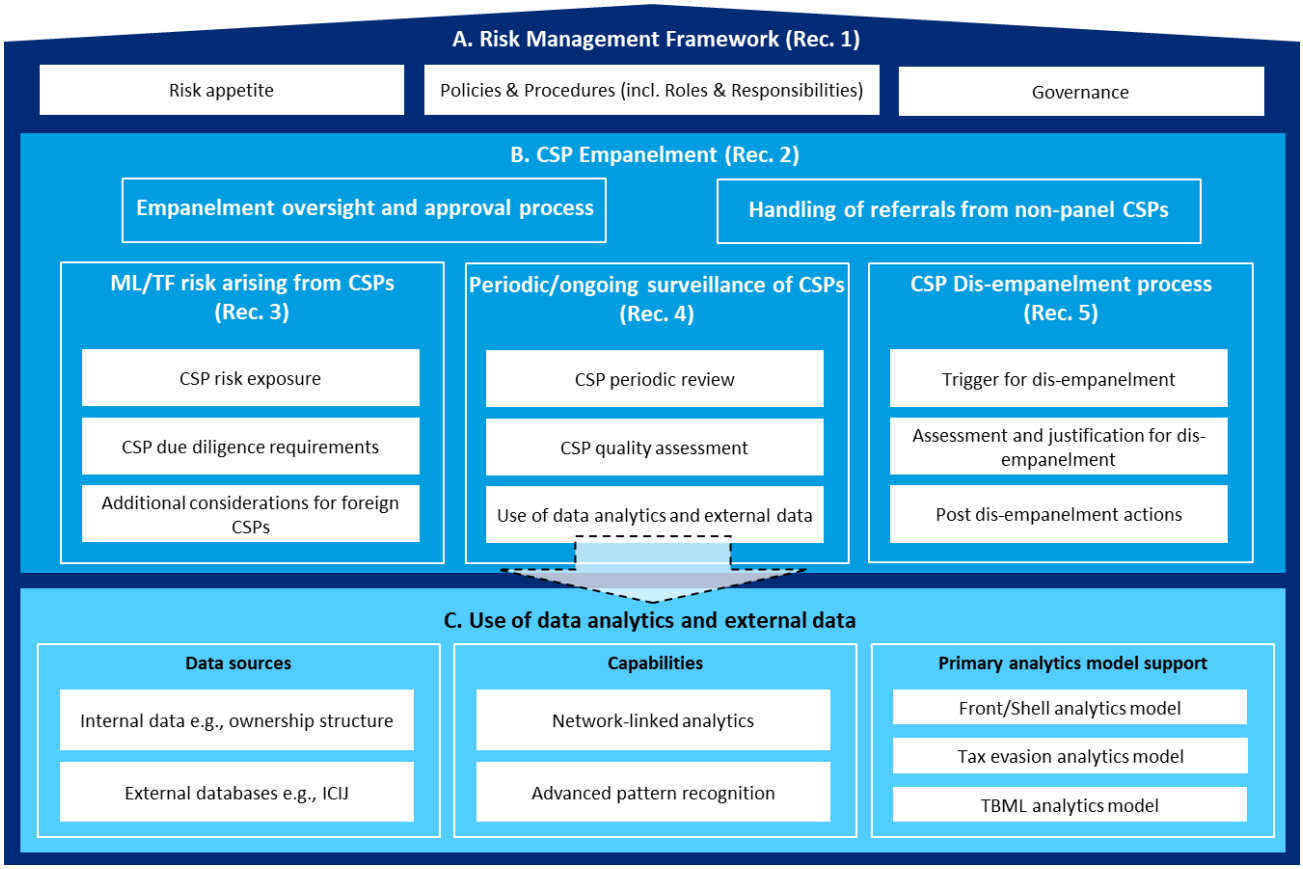


Figure 1 – Overview of control framework comprising the five recommendations

The extent to which the controls set out above are imposed should depend on the bank's risk appetite and exposure to risk from misuse of legal persons (which may include risks relating to the CSP and its activities). The proposed controls framework is premised on the following recommendations, and is summarised in the table below, with details included in sections 3.1 to 3.5.

Recommendation	Summary
1. Formalisation of a risk management framework to manage risks associated with CSP	Banks should set out a formal risk management framework to manage ML/TF/PF risks associated with receiving customer referrals from CSPs. This will ensure that there is an adequate structure in place to manage and mitigate risks which CSPs can potentially introduce to banks.
2. CSP empanelment	Banks should introduce an empanelment process to formalise the management of CSPs that they receive referrals from.
3. Assessment of the level of ML/TF/PF risk arising from CSPs	Banks should set out the key factors used to assess the level of ML/TF/PF risk arising from each CSP which the banks receive customer referral from. These factors include the effectiveness of the CSP's controls framework, the risk attached to the controllers of the CSP, determining the risk associated with foreign CSPs, and others etc.
4. Periodic and ongoing surveillance of CSPs	Banks should have processes in place for the periodic and ongoing surveillance of the CSPs that they receive referrals from. These could cover (a) ongoing monitoring and review of the CSP (e.g., adverse information, intelligence, etc.); (b) a feedback loop to assess the quality of previous underlying customers referred by the CSP, including prospective customers who are rejected at onboarding by bank for ML/TF/PF reasons , (c) the use of data analytics in a variety of use cases including (i) understanding the network of one or multiple known CSPs within the bank's portfolio; and (ii) identifying unusual transaction patterns involving underlying customers linked to a specific CSP(s).
5. CSP Dis-empanelment process	Banks should set out clear internal triggers/criteria within their framework that should be used to initiate the dis-empanelment of a CSP

3.1. Recommendation 1: Formalisation of a risk management framework to manage risks associated with receiving customer referrals from CSPs

Banks should consider formalising a risk management framework to ensure consistent standards are applied throughout the bank to understand and evaluate the ML/TF/PF risks associated with receiving customer referrals from CSPs, and allow for risk-based decisions to be made. The risk management framework should consider including the following elements:

i. Risk appetite

The bank should set out its risk appetite on the type of CSPs that it can receive customer referrals from. Some examples of factors for consideration to derive the risk appetite include:

a. Whether a foreign CSP is registered in high-risk jurisdictions.

b. Whether a foreign CSP is (or is not) supervised by a foreign authority for compliance with AML/CFT requirements.

c. Whether the AML/CFT requirements in foreign jurisdiction where foreign CSP is supervised are consistent with standards set by the FATF.

d. Whether a legal and accounting firm that also provides CSP related services is low risk such as not to require empanelment. An example is a legal and accounting firm that the bank deems as having "well-established" AML/CFT controls or standards.

e. Whether certain conditions have been imposed on the UBO and/or key representative of the CSP. For example, the UBO and/or key representative is a professional, such as a lawyer or accountant subject to AML/CFT regulation and supervision, consistent with FATF standards, with no adverse information against him/her to be determined by name screening on an ongoing basis.

ii. Policies & procedures and clearly defined roles and responsibilities

There should be clearly articulated policies and procedures, along with clear operational guidance, that include the following elements:

- A clear definition of the roles and responsibilities across the Three Lines of Defence:
  - For example, the business unit in first Line of Defence (1LoD) would typically be the party responsible for performing due diligence on the CSP and making an assessment on the CSP's suitability as a customer referrer;
  - Establish escalation requirements for Compliance involvement in second Line of Defence (2LoD) when material ML/TF/PF risks are identified and involvement for advisory on the ML/TF/PF risks and controls, as well as ensuring through sample testing and the review of exception reports if the 1LoD have adequately addressed the ML/TF/PF risks and concerns; and
  - The Internal Audit unit in third Line of Defence (3LoD) would typically be responsible for independently evaluating the AML/CFT risk management framework, including adequacy and effectiveness of controls.
- Details of the key controls required to effectively assess and manage the ML/TF/PF risks arising from the bank receiving customer referrals from CSPs. Banks should leverage on the recommendations in this paper to better understand CSPs and assess the associated ML/TF/PF risks of receiving customer referrals from them (see Recommendations 2 to 5)

iii. Governance

Senior management should exercise oversight of the governance and implementation of effective controls over CSPs as part of the risk management framework. This risk management framework should be formalized within the bank.

As part of the governance process, there should be actionable reporting that provide insights on the ML/TF/PF risks, such as:

- ML/TF/PF risks associated with CSPs and their referred customers at the portfolio-level; and
- Specific ML/TF/PF risks at the CSP-level e.g., pattern of suspicious transaction reports (STRs) linked to a particular CSP, weak AML/CFT compliance by CSPs, supervisory/enforcement actions taken against a particular CSP, etc.

Case study for CSP risk management framework

A bank ("Bank A") established a CSP risk management framework, which included a CSP risk appetite statement, to guide onboarding decisioning of CSP-referred customers. The framework and risk appetite statement are reviewed periodically and when there are material changes to the bank's risks associated with receiving referrals from CSPs.

Bank A was approached by a CSP ("CSP B") for empanelment. Bank A noted that CSP B is located in a high-risk jurisdiction and hence outside of its risk appetite. However, Bank A's relationship managers remain keen to empanel CSP B. A formal empanelment request, together with mitigating measures, was then tabled at the business unit AML forum. The forum comprises of senior representatives from the business unit and Compliance. Following in-depth discussion, the forum proceeded with the empanelment of CSP B, subject to enhanced due diligence processes **of obtaining and assessing the CSP's AML policies and procedures and a site visit to observe the controls in place at the CSP.**

This case study demonstrates the importance of banks having a well-defined CSP risk management framework and relevant escalation procedures, guided by their overall risk appetite.

Operationalisation considerations

Operationalisation starts with formalising guidance for the management of CSP-related risks. Banks should be mindful that the setting up of such a framework is intended to drive better risk understanding and management, rather than restricting certain categories of CSPs or referred customers wholesale.

3.2. Recommendation 2: CSP empanelment

Banks should consider the introduction of a formal CSP empanelment process, and maintaining a panel of CSPs that have been assessed to be within the bank's acceptable risk appetite as established under ***Recommendation 1***. With this, banks will primarily be receiving customer referrals from empanelled CSPs, with due diligence and assessment already conducted upfront prior to empanelment, hence allowing subsequent customer referrals to proceed instead of conducting due diligence on the CSP repeatedly on each of the CSP's customer referrals. Notwithstanding a customer referral originating from a panel CSP, banks are reminded that they remain responsible for the performance of their AML/CFT requirements under relevant MAS Notices and cannot rely on a CSP to perform the required CDD measures.

The empanelment process is not a one-off exercise, but rather, includes ongoing reviews as well as a feedback loop to dis-empanel CSPs that no longer fall within the bank's risk appetite.

A robust CSP empanelling process should provide guidance on:

i. Empanelment oversight and approval process
ii. Handling of referrals from non-panel CSPs
iii. Assessment of the level of ML/TF/PF risk arising from CSPs (***Recommendation 3***)
iv. Periodic and ongoing surveillance of CSPs (***Recommendation 4***)
v. CSP Dis-empanelment process (***Recommendation 5***)

i. Empanelment oversight and approval process

The empanelment process would typically sit within a 1LoD function that is expected to receive such referrals from CSPs. This is to ensure that the 1LoD senior management maintains oversight, and is accountable for, the customer referrals that it receives.

To ensure proper governance, final approval for empanelment should lie with a party that is independent from the proposer or introducer of the CSP. As a best practice, the bank should consider appointing a senior person to be the independent party, as well as having multi-level approval process for CSP empanelment, for example by requiring senior management approval for CSPs assessed to be higher risk (see ***Recommendation 3*** for recommended assessment criteria). Refer to ***Recommendation 1*** - *Policies & procedures and clearly defined roles and responsibilities* for more details on the expected responsibilities within the approval process.

A standard practice is also to introduce the element of independent oversight. This includes conducting quality assurance activities on the CSP empanelment process and reviewing if the CSPs are onboarded onto the panel in accordance with the established risk appetite and procedures. For example, the second line of defence could include in its quality assurance checks whether the CSP meets the bank's risk appetite and fulfills the empanelment due diligence procedures, including on an ongoing basis.

ii. Handling of referrals from non-panel CSPs

It is envisaged that banks would still receive referrals from non-panel CSPs[8], and that some banks would not receive sufficient recurring customer referrals from CSPs to justify an empanelment process. Banks should ensure that the criteria to accept referrals from non-panel CSPs are clearly set out, along with risk mitigating controls as relevant, and that such referrals remain aligned with its risk appetite. Criteria to accept customer referrals from non-panel CSPs could include consideration of the following:

a. CSP is regulated by ACRA (or equivalent foreign regulator to similar standards) for AML/CFT controls

[8] Currently, some banks do not accept referrals from non-panel CSPs.

b. CSP is not sanctioned, or had its registration suspended or cancelled, for AML/CFT breaches[9]

c. Background checks (e.g., open-source search, sanctions, and adverse news screening) reveal no adverse issues in relation to the CSP, its directors and UBOs,

d. The rationale for the CSP involvement can be clearly understood. For example, where the referred customer is a subsidiary of an existing customer that the bank has global relations with, and that the incorporation locally is to support the group's expansion

Where the bank notes recurring referrals, it should consider subjecting the CSP to the empanelment process.

iii. Operationalisation considerations

When introducing a CSP empanelment process, banks should monitor the number of CSPs on their empaneled list. This will ensure that the empanelment list remains useful and is a repository of only the most reliable and high quality CSPs. These decisions should be made based on the bank's capacity to manage ML/TF/PF risks posed by CSPs.

Case study for non-empanelled CSP

Bank A received a customer referral from non-empanelled CSP B. Based on background checks conducted through open source, the following were noted on CSP B:

- CSP B's customer testimonial appears to promote that BVI incorporated entities conducting trading activities do not pay corporate taxes
- CSP B's customer testimonial mentions that CSP B successfully managed to open bank account for entities that have failed to open accounts through other CSPs
- CSP B appears to be marketing a 100% company registration success rate

Taking into consideration the above red flags, Bank A was not comfortable with receiving referrals from CSP B and decided against including it in its list of empanelled CSPs. While the referred customer may still be onboarded based on its own merits, the identified red flags on CSP B, considered in totality with the risk factors of the referred customer, served as a trigger for enhanced monitoring to be applied on the referred customer.

3.3. Recommendation 3: Assessment of the level of ML/TF/PF risk arising from CSPs

As part of the empanelment process, banks should set out the key factors used to assess the level of ML/TF/PF risk arising from CSPs that they receive customer referrals from, and the appropriate due diligence required. This can include:

a. CSP risk exposure;

b. CSP due diligence requirements; and

c. Additional considerations for foreign CSPs.

Banks can use the outcome of this assessment to make an inference about the quality and legitimacy of customer-referrals from CSPs. Each of the key factors are elaborated below.

i. CSP risk exposure

Banks should consider the inherent risks relating to a CSP, for example the jurisdictions or type of customers it serves. Banks could also consider assessing the CSP's AML/CFT controls effectiveness to determine whether the CSP demonstrates a strong AML/CFT controls framework. The following aspects may be considered when conducting risk assessments on the CSPs:

[9] In Singapore, the names of Registered Filing Agents whose registration have been suspended or cancelled are published on BizFile+ (ACRA's business filing and information portal) and ACRA's website.

- **CSP inherent risk** – CSPs that potentially expose the bank to higher ML/TF/PF risks may include foreign CSPs which are subject to less stringent AML/CFT requirements, presence of adverse news against CSPs (including its directors and UBOs), etc
- **CSP control framework**[10] – understanding the strength of controls applied by the CSP
- **Business considerations** – Presence of contractual relationships between bank and CSP where CSPs are paid for customer referrals, CSPs' referral volumes, contribution to the banks' number of customers, AUM etc.

ii. CSP due diligence requirements

a. Standard risk due diligence requirements

The assessment to understand a CSP's risk exposure should be formalised and could be performed through the implementation of an AML questionnaire, to help the bank ascertain the overall effectiveness of the CSP in managing its ML/TF/PF risks.

As part of CSP due diligence, banks should also consider gathering information from independent company registries and other reliable sources of information to conduct background checks on the CSP. Name, sanctions, and adverse news screening of the CSP and its related parties should also be conducted. If available, the number of STRs filed on customers that were referred by the CSP can also form part of the due diligence.

CSP AML questionnaire

Examples of information to obtain include:

- For local CSPs, evidence that the CSP has been registered as a Filing Agent with ACRA and hence required to comply with AML/CFT requirements;
- Understanding the CSP's ownership and management structures;
- Type of services the CSP provides (e.g. pure incorporation, account opening with banks, ongoing company filing/administration, etc.);
- Primary jurisdictions where the CSP provides services;
- Types of customers the CSP maintains e.g., private customers and the use of complex structures, nominee shareholders and directors;
- Information that the CSP collects to determine their customers' beneficial owners and controlling parties;
- Understanding CSPs process in obtaining their underlying customer's source of funds (paid-up capital)
- Identification and assessment of the CSP's UBOs; and
- Understanding whether the CSP has processes to monitor their customer's activities/behavior and to report suspicious activity if there's any. If so, understand the CSP's process to meet the obligation.

The AML questionnaire could be administered over a meeting with the CSP prospect. For CSPs with a more material relationship e.g., large volumes of customer referrals expected, banks may consider conducting the questionnaire at the CSP's premises. Documenting key pieces of information via an AML questionnaire is useful in ensuring robust due diligence and allows banks to understand, assess and effectively manage the ML/TF/PF risks posed by customer referrals from CSPs.

b. Additional Due Diligence (ADD) requirements applicable to CSPs assessed to pose higher risk

For CSPs assessed to pose a higher risk to the bank (including foreign CSPs not regulated for AML/CFT controls), or where the bank has a greater risk exposure to a CSP (e.g., through higher referral volumes or formalized contractual relationship) ADD measures should be considered to mitigate and manage those

[10] Refer to Appendix for an overview of the key elements of a CSP's AML/CFT control framework.

risks. This can be in the form of: (1) obtaining and assessing the CSP's AML policies and procedures; (2) site visits to observe the controls in place at the CSP (where possible); (3) understanding issues identified in the CSP's audit or compliance assessment report or equivalent, if applicable[11]; as well as (4) identifying and assessing the controllers of the CSP.

Identifying and assessing the controllers of the CSP

For higher risk CSPs, banks' ADD could include the unwrapping of the CSP's corporate structure and the identification of its ultimate beneficiary owner (UBO) and conduct name screening on all identified parties. In performing this, banks should also consider the complexity of the CSP's structure, as well as the bank's risk appetite.

UBO unwrapping for CSPs with simple shareholding structures are generally straightforward. For complex structures, e.g., multi-jurisdictional or where more than two layers of unwrapping is required, banks may face challenges in unravelling the CSP to the UBO-level. This is due to challenges in obtaining reliable information on the CSP's structure and ownership. Banks will then have to consider:

- If there are legitimate business reasons for such complex structures;
- Whether the empanelment of such complex CSPs is within their risk appetite e.g., through the application of a risk-based approach to guide empanelment decision making;
- The materiality of the relationship e.g., CSPs with high volumes of referrals, CSPs with contractual relationship for referrals etc;
- Whether additional monitoring controls can be put on the CSP, or the customers referred to by such CSPs e.g., increasing frequency of periodic reviews, onsite visits to the CSPs' premises, enhanced due diligence on the underlying customer etc.

UBO information is a key input to identifying relationships between CSPs and their associated parties, and this would help when banks introduce other or have existing data analytics capabilities to complement periodic and ongoing surveillance of CSPs.

To alleviate the operational challenges around CSP unwrapping and considering that these are not customer relationships, banks can consider having CSPs disclose ultimate beneficial ownership. Such disclosure can be a requirement for CSP empanelment. Banks should leverage on existing UBO identification resources e.g., databases and capabilities to identify UBOs and verify the disclosure provided by the CSP.

iii. Additional considerations for foreign CSPs

Banks recognise that foreign CSPs could bring a higher level of ML/TF/PF risks relative to CSPs operating from and regulated in Singapore. Banks might consider introducing limitations on the empanelment of foreign CSPs. Examples include:

- Alignment with the bank's risk appetite and challenging the economic purpose of the referred customer (see case study in section 3.1);
- Requirement for foreign CSPs to be empanelled before customer referrals can be made i.e., one-off, or ad hoc customer referrals from foreign CSPs will not be accepted;
- Only empanelling CSPs belonging to certain jurisdictions including:
  - Countries with existing bank presence and where the foreign CSP in question is already empanelled. Reliance will be placed on country offices should additional information on the CSP be required. Notably, due diligence on the referred customer should still be performed by the Singapore office;
  - Alignment with the bank's internal country risk rating, including in relation to the jurisdiction the CSP's UBO(s) are from;

[11] ACRA Registered filing agents ("RFA") are required to comply with the AML and CFT requirements which are set out as terms and conditions in the ACRA (Filing Agents and Qualified Individuals) Regulations 2015. This includes internal audit and compliance management requirements. ACRA may also appoint Reviewers to perform compliance reviews on RFAs, where the RFAs will receive a compliance assessment report upon completion. For more details, refer to 'https://www.acra.gov.sg/corporate-service-providers/compliance-review'.

- Countries in compliance with FATF standards;
- Similarities between Singapore and jurisdiction in consideration, with regards to AML requirements and supervision for CSPs

When introducing enhanced requirements for foreign CSPs, banks should consider the need for a more holistic view on empanelment requirements. In imposing specific requirements on foreign CSPs, banks must ensure that their approach does not become overly prescriptive. For example, two CSPs domiciled in the same country may be beneficially owned by individuals from other jurisdictions. Depending on whether these jurisdictions are FATF-compliant (or applying the relevant FATF-Standards on the CSPs), the risk profile of these two foreign CSPs may differ vastly.

As such, banks should focus on a holistic assessment of the CSP's ML/TF/PF risks. Banks should avoid being fixated on the specific limitations and run the risk of these enhanced requirements becoming a box-ticking exercise that do not provide effective risk mitigation.

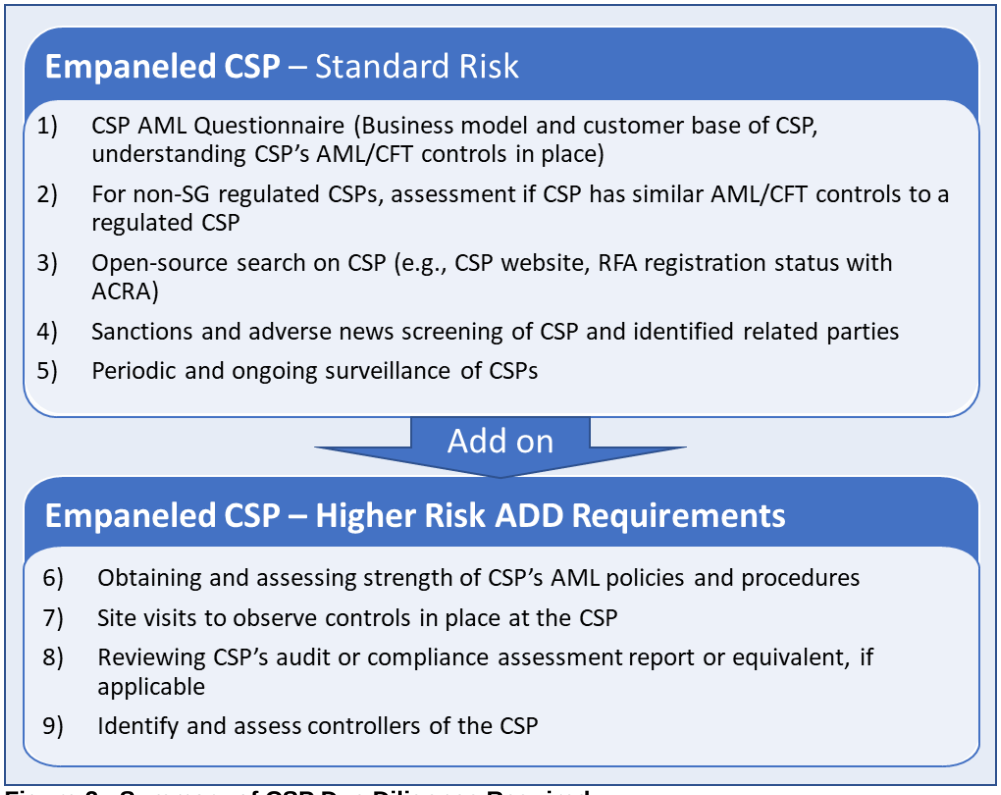


Figure 2 - Summary of CSP Due Diligence Required

3.4. Recommendation 4: Periodic and ongoing surveillance of CSPs

While the above recommendations primarily cover CSP risk assessment and empanelling, banks should also define periodic review and ongoing surveillance processes to manage these relationships.

Periodic reviews of empanelled CSPs[12] should include three elements

- A periodic review of the CSP to identify material changes of the CSP's ML/TF/PF risk exposure and assess whether CSPs are suitable for continued empanelment. The level of periodic review may cover CSP due diligence process or name screenings of the CSPs and its UBOs, etc depending on the bank's risk appetite. Higher risk CSPs should be subject to more frequent periodic review (e.g. on an annual basis).
- Trigger based reviews may be performed on a CSP where ML/TF/PF risk concerns are identified (e.g. resulting from material adverse information on the CSPs, its directors and its UBOs

[12] CSPs referring customers on a one-off or ad hoc basis are not empaneled and will not be subjected to periodic reviews (see section 3.2)

- CSP quality assessment, informed by the bank's customer controls. The main indicators of CSP quality are (a) the pattern of STRs filed on customers referred to the bank by a particular CSP, (b) prospective customers rejected at onboarding, customer exits or associated with a given CSP (due to ML/TF/PF concerns), and (c) data analytics findings[13]. Should a CSP be found to be associated with significant patterns of customer referrals who are eventually associated with STRs and customer exits, banks will have to consider whether the CSP remains of sufficient quality for continued empanelment. Please see Recommendation 5 for the dis-empanelment process. Banks can also consider other stages of the CSP lifecycle[14] as a starting point for its CSP quality assessment, including the following triggers:
  - Material adverse information on customers and its nominee directors (from CSP).
  - Confirmed sanction hits on customers and its nominee directors (from CSP).
  - Activity by the customer that is inconsistent with due diligence information.
  - Material or unexplained changes in volume and value of transactions by customers.
  - CSP is suspected to have guided the referred customer on how to circumvent CDD questions.

i. Operationalisation considerations

Close coordination between different teams within the bank is necessary to ensure the CSP quality assessment is conducted effectively. A clear line of communication between the relationship manager and the CSP empanelment monitoring teams is required. This ensures that customer control outcomes are provided as inputs to CSP quality assessment in a timely manner.

ii. Use of data analytics and external data

Banks could consider the feasibility of leveraging on existing data analytics tools that they may have been put in place for other purposes in the identification and management of CSP-related risks and could form a component of the bank's ongoing surveillance of risk arising from CSPs. Examples include:

- Identifying previously unknown CSPs or customer connected to CSPs
  - Trigger is a suspicion against a customer e.g., STRs filed, adverse new hits etc
  - Trigger is a concentration of customers linked to common identifiers, such as registered address, director, or common close associate or UBO
- Understanding the network of known CSPs within the bank's portfolio
- Identifying transaction patterns within the bank's network of CSPs and customers

For these use cases, banks should understand and identify risks within the networks by looking at internal data on the ownership structure of corporate customers. CSPs commonly arrange for their employees or associated individuals to act as a director of a company, to help foreign customers meet Singapore legal requirements for companies to have a resident director[15]. The Bank may also consider using external databases (where feasible) such as those maintained by market infrastructure information providers, commercial data providers and open source e.g., Bureau van Dijk. These external sources are useful for identifying direct matches of CSPs and bank customers which may be potential shell companies likely to be used to facilitate illicit activity. The establishment of a CSP network can be supported by robust primary analytics models. The outputs from these models are good starting points for banks to identify suspicious parties and transactions within networks of CSPs and customers. These may include analytics models on tax evasion, trade finance money laundering and most pertinently, shell analytics. Examples of shell model inputs and red flags included in its outputs are as follows:

[13] Refer to section 'Use of data analytics and external data' on how data analytics can be applied in managing CSP risk. The findings of such data analytics, e.g., uncovering of shell/front networks created by one or multiple CSPs, should contribute to the determination of a CSP's quality.

[14] CSP lifecycle starts from the empanelment of the CSP or acceptance of referral, goes through periodic reviews (for empaneled CSPs) and trigger event reviews, and ends with the exit or blacklisting of the CSP.

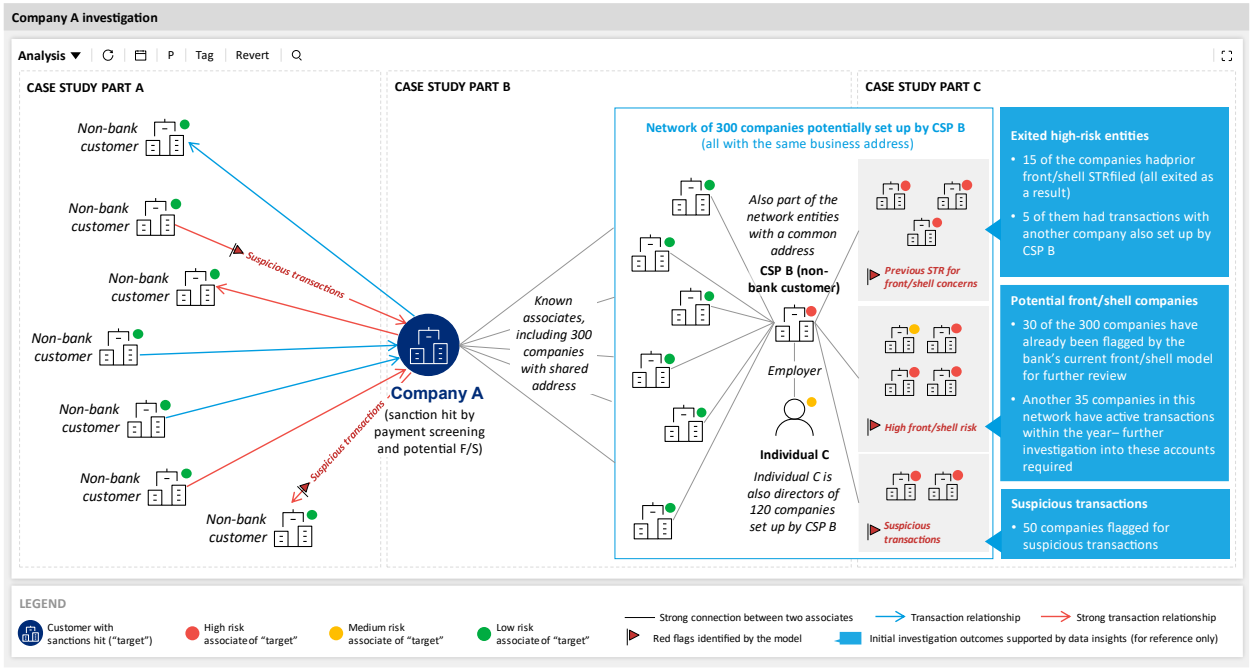
[15] Requirement under Section 145(1) of the Companies Act.

Shell model inputs	Example red flags included in model outputs
• Closed or dormant accounts • Number of STRs filed • Number of STRs filed • Percentage change in transaction volume, both in and outward • Percentage change in transaction amount	• Transaction with high-risk or tax haven jurisdictions • Connections with known shell companies e.g., common director, shared address • Passthrough, circular or “U-turn” transactions • Frequent transactions indicative of layering typologies • Transactions with known adverse news hits

Network Linked Analysis (NLA) and advanced pattern recognition could be useful tools for identifying and managing risks associated with CSPs. These capabilities allow banks to identify a network of potential relationships between CSPs and their associated parties. The network is based on a multitude of factors including transaction amount, frequency, and pattern, as well as demographic information e.g., directorships and credit scores. NLA and pattern recognition models identify suspicious networks to a significantly higher degree of accuracy as compared to traditional approaches.

Case study for the use of data analytics

The following is an illustrative case study of how NLA and advanced pattern recognition tools, supported by the relevant data sources and primary analytics models, can help banks identify CSP-related risks across the use cases highlighted at the top of this section.



Case study part A: Investigation triggered by suspicion against a customer

The investigation process starts with the bank's sanctions analytics model. A sanction hit from payment screening identified red flags from two set of suspicious transaction performed by the customer ("Company A"). These red flags included "U-turn" transactions, passthrough transactions, and structuring of transactions, indicating signs of ML activities.

Case study part B: Concentration of customers linked to a common address, associate or UBO

Looking further into Company A, the bank uncovered two insights. Firstly, existing records showed that Company A was flagged by the bank's analytics model as a potential front/shell company. Secondly, common address analysis showed that Company A shares the same registered address as 300 other companies, some of which are existing bank customers. One of the 300 identified companies within the shared address cluster was a CSP with no existing relationship with the bank ("CSP B").

Subsequent internal bank database deep dive showed that 120 of the 300 companies were also associated with an existing bank customer ("Individual C"). Individual C is named as a director in these companies. Furthermore, relying on external databases, Individual C was found to be employed by CSP B. This confirms suspicion that the rest of the 300 entities were potentially incorporated by CSP B under the same registered address.

Case study part C: Understanding the network of known CSPs

Having identified CSP B, the bank's data analytics models were also able to provide insights into its associated network of incorporated companies. The bank found that many of the 300 companies incorporated by CSP B were flagged for potential ML/TF concerns. These include customer exits, high front/shell risks and suspicious transactions.

- Exits: 15 of these companies had previously been exited by the bank as a result of front/shell STRs being filed against these entities. Five of the 15 were also found to have transacted with other companies incorporated by CSP B
- Front/shell: 30 of the 300 companies were already identified by the bank's existing front/shell model for review, with another 35 flagged for active transactions warranting further investigations. These

companies are part of a network of 100 companies incorporated by CSP B that were deemed potential front/shell companies

- Suspicious transactions: 50 of the 300 companies incorporated by CSP B were also flagged by the bank's analytics model for suspicious transactions
- Mitigating actions taken: All of the customer relationship identified to be incorporated by CSP B were reviewed and exited where suspicious transactions were found that could not be explained satisfactorily.

The above case study provides an example of how data analytics capabilities can help banks identify and mitigate risks posed by CSPs and their customer referrals, regardless of whether these relationships were of prior knowledge to the bank. Relevant mitigation action, including a review of relevant customer relationships and STR filings should be conducted by the bank, arising from such findings.

iii. Operationalisation considerations

Management of risks associated with CSPs may not justify the significant cost outlay associated with sophisticated analytics capabilities. This is especially so for banks with low volumes of empanelled CSPs and customer referrals. As such, the use of analytics in mitigating such risks should be a specific use case within the bank's broader AML analytics journey.

To build analytics capabilities, banks need to put in place the relevant data and technology infrastructure. Furthermore, banks will have to build the required teams and capabilities to perform data analytics and operationalise model outputs. These operational considerations are highly dependent on the maturity and broader data analytics strategy of the bank. Broader collaboration and information sharing between banks and relevant law enforcement authorities will also be helpful in uplifting the industry's AML capabilities.

3.5. Recommendation 5: CSP Dis-empanelment process

As part of the CSP lifecycle, where significant adverse issues are identified in relation to an existing association with a CSP, banks should cease further association. This should be supported by a formal dis-empanelment process, which includes an assessment and justification for dis-empanelment, and controls to monitor or prevent future referrals.

Banks should define requirements to support a structured assessment for dis-empanelment and include the following considerations:

- Trigger for dis-empanelment[16]
- Plausible CSP knowledge of ML/TF/PF activities by its customers (both actual knowledge and wilful blindness)
- Potential weakness in CSP's controls leading to dis-empanelment trigger

[16] Such triggers may include, where material ML/TF/PF concerns are noted during periodic review and ongoing surveillance of CSPs, material adverse news or sanctions hits, STR volume on customers linked to CSP, etc.

Case studies: Triggers for CSP dis-empanelment

Scenario 1: Material adverse news found on a CSP

The bank found news reports that an employee of a CSP was charged and found guilty of negligence in the carrying out of nominee director duties. The bank noted that this was not the first time that this particular CSP was reported in the news for similar offences by its employees and assessed that it was probable that the CSP has weak internal AML/CFT controls. As a result, the bank decided to dis-empanel the CSP.

Scenario 2: CSP quality assessment

In consultation with the customer control team, the CSP empanelment monitoring team noted that there were a significant number of exits for customers referred by a particular CSP ("CSP A"). These exits were due to various AML/CFT concerns. As such, the CSP empanelment team notified the relationship managers and proposed to remove CSP A from the bank's empanelment list. Upon review, the Business Head approved the proposal to dis-empanel the CSP.

Banks should also consider taking other actions upon dis-empanelment that may include the following:

- Handling of customer network linked to CSP (e.g., through trigger event reviews on bank's customers)
- Handling of future associations with the CSP (e.g., through blacklisting of CSP, shareholder and nominee directors)
- STR filing as appropriate
- Sharing information on the dis-empanelled/blacklisted CSP with ML/TF/PF concerns with the relevant authority where applicable

Further acceptance of referrals from the dis-empanelled CSP is then not appropriate. Dis-empanelled CSPs should be maintained on the bank's internal list as a "Do Not Engage" introducer for future reference.

It is recognized that while the bank may restrict customer referrals from a blacklisted CSP, it may not be feasible or reasonable to exit all customers associated with the CSP (e.g., through incorporation or nominee director services provided by the CSP). In general, such linkages with a blacklisted CSP would be treated as an adverse news on the bank's customer, in which the bank should then assess the relevance and materiality of the adverse issue on the bank's customer.

4. Conclusion

Banks should be cognisant of the ML/TF/PF risks they may be exposed to, when working with CSPs and receiving their customer referrals from CSPs. The recommendations in this paper set out best practices for banks to enhance their existing controls frameworks to manage risks associated with CSPs. This paper should also be read in conjunction with other relevant risk management literature, including publications by FATF. Over time, this will contribute to uplifting the banking industry's understanding and management of ML/TF/PF risks associated with CSPs. Although receiving customer referrals from CSPs can potentially introduce risks to banks, it should be noted that the root of such risk originates from the underlying customer. As such, **banks are reminded that all customers, CSP-referred or otherwise, must be subject to customer due diligence standards**, in line with the requirements set out in MAS 626 Notice, its associated Guidelines and the banks' internal policies and procedures.

5. Appendix

5.1. CSP's AML/CFT framework

This section provides a summary of FATF standards on AML/CFT frameworks that CSP may have in place for the bank to consider when assessing the CSP's control framework.

The FATF Standards require countries to impose AML/CFT requirements on CSPs. Hence, like banks, CSPs are AML obligated entities and play a vital gatekeeper role in mitigating ML/TF/PF risks. In its paper[17] "Guidance for a risk-based approach – Trust and Company Service Providers" (June 2019), the FATF listed critical AML/CFT controls that Trust and Company Service Providers are expected to impose (see summary table below).

Key elements of the AML/CFT control framework	Selected examples
Risk identification & assessment Identifying ML/TF/PF risks faced by firms, across risk categories of (1) customers, (2) services and (3) countries of operation, with reference to publicly available information regarding ML/TF/PF risks and typologies	Unexplained use of shell companies or legal entities with ownership through nominee shares or bearer shares
Risk management & mitigation Identifying and applying measures to effectively and efficiently mitigate and manage ML/TF/PF risks	Identifying and verifying the customer's identity using reliable and independent documents, data, and information
Ongoing Monitoring Putting in place policies, procedures, and information systems to monitor changes to ML/TF/PF risks	CSPs need to be alert to events or situations which are indicative of ML/TF/PF
Documentation Documenting risk assessments, strategies, policies, and procedures to monitor, manage and mitigate ML/TF/PF risks	CSPs must always understand their ML/TF/PF risk exposure. Risk assessment should be documented such that CSPs are able to demonstrate their exercise of due professional care and compelling professional judgement

[17] "Guidance for a risk-based approach – Trust and Company Service Providers" (June 2019); https://www.fatf-gafi.org/media/fatf/documents/reports/RBA-Trust-Company-Service-Providers.pdf

In Singapore, ACRA is the regulator and supervisor of CSPs[18]. ACRA has also published Singapore-specific AML/CFT Guidelines for CSPs[19], to help them understand and fulfil their AML/CFT requirements. AML/CFT requirements imposed by ACRA on CSPs are in line with the FATF Standards.

Other jurisdictions outside of Singapore may have different standards and regulatory requirements for CSPs.

In summary:

i. International standards, including those set out by the FATF, require that countries regulate and supervise the conduct of corporate services including CSPs compliance with AML/CFT requirements. This includes requirements for CSPs to set up internal AML/CFT policies and procedures which can form a basis for banks to assess a CSP's controls framework.

ii. Foreign CSPs may need to be subject to an additional assessment to determine if they are supervised by a foreign authority for compliance with AML/CFT requirements consistent with standards set by the FATF.

iii. CSPs assessed to pose a higher risk should be considered for additional due diligence measures ("ADD") as outlined in this paper.

In conclusion, a bank receiving referrals from Singapore regulated CSPs as compared to a foreign CSPs may be exposed to different level of risk due to the differing standards the CSPs would have conducted on the underlying customers. The bank should consider this risk in determining its risk appetite.

5.2. Glossary

Acronyms	Description
ACIP	Anti-Money Laundering and Countering the Financing of Terrorism Industry Partnership
ACRA	Accounting and Corporate Regulatory Authority
AML/CFT	Anti-money laundering and countering the financing of terrorism
CAD	Commercial Affairs Department
CDD	Customer due diligence
CSP	Corporate service providers
FATF	Financial Action Task Force
FI	Financial Institution
Legal Persons WG	Legal Persons Working Group
MAS	Monetary Authority of Singapore
ML/TF/PF	Money laundering/terrorism financing/proliferation financing
NLA	Network Linked Analysis
STR	Suspicious transaction report

[18] See footnote 5.

[19] "ANTI-MONEY LAUNDERING/ COUNTER FINANCING OF TERRORISM GUIDELINES FOR REGISTERED FILING AGENTS" (Jan 2023); https://www.acra.gov.sg/docs/default-source/default-document-library/corporate-service-providers/rfa-guidelines_v2-4_13-jan-2023.pdf

5.3. Legal persons working group members and other contributors

Firm		Representative
Banks	United Overseas Bank Limited	Melda Pravina Tandi
	United Overseas Bank Limited	Kevin Ho Lian Heng
	United Overseas Bank Limited	Leon Khoo
	OCBC	Gillian Huang
	OCBC	Kharan Coomaraswamy
	DBS	Eric Cheng Hian Luah
	DBS	Jean Gee Kian Tan
	DBS	Anning Xu
	SCB	Jennifer Koh
	SCB	Burzeen Tengra
	SCB	Tan Siew Gan
	Maybank	Chen Jee Meng
	Citibank	Low Serina Wei Qi
	HSBC	Margaret B Y Zhu
	HSBC	Kamilah Norghamar
	UBS	Ee Ping Lim
Professional Services	Oliver Wyman	Sean Kennedy, Partner
	Oliver Wyman	Jonas Heckmann, Principal
	Oliver Wyman	Charles Lewis, Manager
	Oliver Wyman	Brandon Ho, Consultant
Government	Monetary Authority of Singapore	
	Commercial Affairs Department	
	Accounting and Corporate Regulatory Authority	