Designing appropriate SDD measures

2 Overview

At the heart of regulatory and institutional anti-money laundering and counter-terrorist financing measures are a set of obligations known as "Customer Due Diligence" (CDD) measures.

FATF's standard CDD requirements include the following.

The FATF standards on CDD

"The CDD measures to be taken are as follows:

(a) Identifying the customer and verifying that customer's identity using reliable, independent source documents, data or information.

(b) Identifying the beneficial owner, and taking reasonable measures to verify the identity of the beneficial owner, such that the financial institution is satisfied that it knows who the beneficial owner is. For legal persons and arrangements this should include financial institutions understanding the ownership and control structure of the customer.

(c) Understanding and, as appropriate, obtaining information on the purpose and intended nature of the business relationship.

(d) Conducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the institution's knowledge of the customer, their business and risk profile, including, where necessary, the source of funds.

Financial institutions should be required to apply each of the CDD measures under (a) to (d) above, but should determine the extent of such measures using a risk-based approach (RBA) in accordance with the Interpretive Notes to this Recommendation and to Recommendation 1."

(Extracts from Recommendation 10)

FATF *International standards on the combating of money laundering and the financing of terrorism & proliferation* (2012 -)

Enhanced CDD measures are required where risks are higher while countries are allowed to support simplified due diligence (SDD) measures where AML/CFT risks are assessed as lower. In cases of proven low risk, appropriate exemptions from general AML/CFT obligations may be considered.

CDD measures can be expensive and may create service cost barriers for persons who are financially excluded. It may also create absolute barriers, e.g. by requiring identity verification documents or data that cannot readily be provided by financially excluded persons. Many financial-excluded persons pose a lower money laundering and terrorist financing risk and their access to financial services can be supported by SDD measures that remove or lower such barriers.

Importantly, the FATF standards identify as lower risk product, service, transaction or delivery channel situations "Financial products or services that provide appropriately defined and limited services to certain types of customers, so as to increase access for financial inclusion purposes".

4 Enabling the implementation of simplified due diligence

From an institutional risk-based perspective SDD is appropriate where inherent risks are lower:

- If inherent risks are lower, residual risks will also be lower even if AML/CFT controls are simplified.
- If inherent risk are higher, residual risk may be lower, if stronger AML/CFT controls are applied.

These two possibilities are explored below.

Possibility 1: Operate in a lower risk environment

Countries do not all have the same ML/FT/PF risk levels. The national risk level of a country may therefore be lower than that of a neighbouring country. Similarly not all regions in the country may have the same ML/FT/PF risk profile. ML/PF risks may for example be much lower in a remote regional area than in urban areas while TF risk may be higher in one particular city or region of a country. Not all population segments have the same ML/FT/PF risk levels either. A product or service offered in a lower risk region or offered to a lower risk population segment (e.g. retirees on government pensions) may not require more than SDD to mitigate any ML/FT/PF risk adequately.

For guidance on finding information about risk levels and the profile of financially-excluded persons, see **below:**

Collecting information and evidence about risk and financial inclusion

Risk mitigation measures should respond to assessed risks.

1. The latest national risk assessment is an important starting point:
    - What are the major crime types of concern? Consider whether and how these may be relevant to customers using financial inclusion products.
    - Does it identify any relevant aspects regarding the customer groups, products and services as higher risk?
    - Does it identify low value transactions as higher risk?
    - If it identifies cross-border transactions as higher risk, does it identify all corridors and all types of transactions as equally risky?
    - Does it identify the cash and informal economy as elements of concern? If so, that may justify SDD to support financial inclusion and formalisation

2. Often the national risk assessment may not be particularly helpful and further risk-related data and information may be sought from authorities :
    - The financial intelligence unit may have data on the average values of transactions reported to it and the profiles of customers featuring in such reports.
    - Law enforcement agencies may have national and regional data on reported crimes and convictions relating to identity fraud, offences generating significant proceeds of crime (drug trafficking, smuggling, corruption, fraud, etc) and financing of terrorism. Data in this regard is important as anecdotal information is often biased.

To support financial inclusion SDD design must also respond to the needs of customers of financial inclusion products and services, and the inclusion barriers they face. Regulatory bodies or local and international bodies and databases such as 2021 version of the World Bank's Global Findex database may hold relevant data, including:

- What is the profile of financially-excluded persons (age, gender, location, sources of income) ?
- What types of products would meet their needs ?
- When sending or receiving funds or making payments, what are the average amounts involved?
- How regularly would they engage in transactions ?
- If they have cash to save, how much would be saved in a financial inclusion product ?
- What documents or data would be available to verify their identity ?

Possibility 2: Operate in a higher risk environment with appropriate product and service controls

When the product is offered in a standard or higher risk environment, appropriate product or service restrictions and conditions will have to be considered to combine with SDD to result in a lower residual risk. In some cases a single restriction may suffice while, in higher risk environments, more than one may need to be combined to achieve the desired result.

5 Imposing appropriate restrictions and conditions, where required

In a low risk environment no restrictions or limitations may be required but in a higher risk environment appropriate restrictions and limitations may lower risk levels sufficiently to allow for SDD.

- User-related restrictions;
- Functionality restrictions;
- Value restrictions; and
- Business model restrictions.

5.1 User-related restrictions

User-related restriction	Motivation
Restricting the product or service to citizens and residents	When crime risk is higher in neighbouring countries or among tourists; or when law enforcement agencies have proved more able to investigate domestic criminals rather than foreign criminals
Restricting the number of such products a user may hold	This limits the level of abuse should the product or service be abused; may also be required to protect any value restrictions imposed.
Restricting it to a group of users with a lower crime risk (according to criminal justice data of the country)	Restricting a product to women or to pensioners may lower the risk if data reflects that those groups are less prone to commit crime.

Restricting product functionality, e.g. to be only used within the borders of the country	Preventing cross-border functionality can lower risks where criminals primarily require cross-border funds movement to laundering money or finance terrorism

5.2 Functionality restrictions

Functionality restriction	Motivation
Limiting the product to use within the borders of the country	Preventing cross-border functionality can lower risks where criminals primarily require cross-border funds movement to laundering money or finance terrorism
Allowing the product to be used to send remittances within specified lower risk corridors only	Limiting cross-border functionality to regulator-approved corridors where risks are lower and regulatory and law enforcement collaboration is good, lowers risks of abuse.
Allowing the product to be used for certain lower risk payments only, e.g. P2G payments	Where the context and the users are higher risk in nature it is possible to lower risk by restricting the product to lower risk government payments, e.g. for tax and government services such as water and lights bills, education, etc.

5.3 Value restrictions

Value restrictions	Motivation
No transaction in excess of a stated amount may be transacted; i.e. no transaction above $200 is allowed	A product with appropriate capped transaction value lessens the attractiveness of its abuse by criminals while retaining its usefulness for low income users
Product-related transactions are capped to a stated amount within a time cycle, i.e. weekly or monthly	Cycle-based caps allows for more discretionary use by the users (e.g., they may engage in an occasional transaction of more than $100 provided that their other transactions remain below the overall limit) but still limits the attractiveness of the product to criminals.
Value storage can be capped to a stated amount	Value storage caps lessen the potential for money laundering abuse, especially when combined with appropriate caps on transactions

5.4 Business model restrictions

Business model restrictions	Motivation
Restricting the approved lower risk products to banks and/or specific non-bank providers	The regulator may hold an evidence-based view that the providers allowed to offer the products

	are the only types of providers that have the capacity to ensure that the restrictions are observed.
Requiring the use of eKYC linked to the national identity register	The regulator may hold an evidence-based view that eKYC provides a higher level of identity verification assurance
Only allowing in-person account opening	The regulator may have an evidence-based view that in-person processes provide higher levels of identity verification assurance than remote account opening. If considered, this may be best imposed in a tier-based CDD processes in relation to the highest level, if there is a sound risk mitigation reason to prefer in-person account opening rather than secure, eKYC-supported remote account opening.
Not allowing agents to perform any aspect of CDD	The regulator may hold an evidence-based view that no agents can be trusted with any aspect of CDD.
Allowing agents to collect documents and information and to forward it to the Agent Network Operator or main compliance function to decide whether an account should be opened.	The regulator may have evidence-based reasons why agents should not be entrusted with account opening decisions
Not allowing outsourcing of any CDD element	The regulator may have evidence-based reasons why no service providers can entrust any CDD element to third parties

Additional Considerations:

1. User restrictions

User restrictions are only effective if they do not allow for easy evasion and are combined with measures to detect evasion, when it occurs, i.e.:

- Restricting customers to holding one limited product with one institution may not be an effective general control measure if there are multiple institutions offering similar products, enabling clients to multiply their individual products across multiple institutions.
- Restricting access to a lower risk group may not be effective if they, after securing the product, can allow others outside the group to transact via that product.

Such risks of evasion can be limited by additional CDD design elements, e.g.:

- **Monitoring product use for anomalies**. Persons abusing accounts for criminal purposes across multiple institutions and those who abuse accounts of others will often have transaction patterns that differ from those of the regular users. Monitoring for transactional patterns that are outliers compared to the normal transaction and use patterns of other users will help to identify such abuse.
- **Requesting users to declare when securing a product that they do not hold a similar product with another provider**. This may not limit criminal abuse but it will raise the probability that multiple account holding is criminal in nature when detected via product monitoring.

- Where possible, **gain supervisory visibility of registered users across institutions** to determine whether a significant number of users may have similar lower risk products with more than use provider. Directive (EU) 2018/843 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, the so-called "5th Anti-Money Laundering Directive", requires EU Member States to set up centralised automated mechanisms allowing the identification of holders of bank and payment accounts.
- **Educate users never to share their product access credentials** with others, to prevent abuse of accounts by third parties.

2. Value Restrictions:

The FATF standards apply value caps in a handful of cases, e.g.:

- USD/EUR 15,000 is the applicable designated threshold that triggers CDD in relation to occasional transactions;
- Life insurance policies where the premium is low (e.g. an annual premium of less than USD/EUR 1,000 or a single premium of less than USD/EUR 2,500), are used as examples of lower risk products; and
- USD/EUR 1,000) is used as the minimum threshold for cross-border wire transfers.

To inform decisions about regulatory caps regulators will need to draw on their national risk assessments and may need to collect additional information to determine caps that ensure lower risk, whether in isolation or in combination with other control measures, while still supporting financial inclusion. Additional data and information may be collected from the financial intelligence unit and law enforcement agencies, e.g.:

- What is the average value of transactions reported as suspicious to the financial intelligence center? How many transactions were reported in the past year that were below 20% of the average value?
- What is threshold value of a transaction reported as suspicious that is likely to be investigated by law enforcement? What are threshold value of single transactions that would generally be too low to trigger investigative resources?

Statistics regarding potential money laundering should be separate from statistics regarding terrorist financing. Given the nature of terrorist financing authorities may give attention to lower value transactions that may often be disregarded for money laundering purposes.

3. Other Conditions:

In addition to restrictions, conditions may also lower the risk level of products. Such conditions may include the use of eKYC or digital identity rather than document-based identity verification. See for example the FATF's views on the impact of digital identity to lower risk below**.**

The FATF on risk levels of appropriate digital identification

"Given the evolution of digital ID technology, architecture, processes, and the emergence of consensus-based open-source digital ID technical standards, it is important to clarify that non-face-to-face customer-identification and transactions that rely on reliable, independent digital ID systems with appropriate risk mitigation measures in place, may present a standard level of risk, and may even be lower-risk where higher assurance levels are implemented and/or appropriate

ML/TF risk control measures, such as product functionality limits and other measures discussed in INR10 and FATF Guidance on Financial Inclusion, are present … " (par 89)

FATF Digital Identity (2020)

6 Designing appropriate SDD measures

When the risk levels are lower, either because inherent risk is lower or because restrictions and limitations lowered the risk level sufficiently, thought can be given to the design of the SDD measures.

The FATF classifies as SDD a CDD scheme where one or more of the elements are simplified, even though others (like transaction monitoring) may be enhanced. Monitoring allows intervention and interdiction of any illicit funds that may be involved, and can provide valuable criminal intelligence to secure convictions, thereby limiting the risk of abuse. The potential of simplifying one or more CDD elements or of combining different control measures at different levels provide regulators and institutions with flexibility to design due diligence measures that lower residual risk levels sufficiently while enabling greater financial inclusion.

The FATF lists the following examples of possible SDD :

- Verifying the identity of the customer and the beneficial owner after the establishment of the business relationship (e.g. if account transactions rise above a defined monetary threshold).
- Reducing the frequency of customer identification updates.
- Reducing the degree of on-going monitoring and scrutinising transactions, based on a reasonable monetary threshold.
- Not collecting specific information or carrying out specific measures to understand the purpose and intended nature of the business relationship, but inferring the purpose and nature from the type of transactions or business relationship established.

Simplified CDD measures are not acceptable whenever there is a suspicion of money laundering or terrorist financing, or where specific higher-risk scenarios apply.

While there is no prescriptive standard regarding the elements of SDD it is useful for regulators and institutions that wish to advance financial inclusion to first consider whether any inclusion barriers may be lowered by the SDD design.

Where financially excluded persons have difficulty to meet identity verification requirements, thought can be first be given to whether these requirements may be simplified. Should simplification of identity verification be found to introduce risk, that risk may perhaps be mitigated by requiring enhanced transaction monitoring, as discussed above. Alternatively, the designers may elect to introduce appropriate digital identity requirements.

Tier-based CDD may also be considered. In tier-based CDD very limited functionality can be accessed with minimal SDD while product or service functionality increases when and as the customer meets increased CDD levels. The FATF described such a system in its 2020 digital identity guidance, drawing on material provided by the US Treasury. Importantly the example used a digital identity model but allowed the lowest level of functionality to be accessed without identity verification.

A FATF example of the use of digital ID in tiered and progressive CDD to support financial inclusion

"A financially excluded individual applies for a basic bank account, using a digital ID obtained without presenting identity evidence. The digital ID has a lower assurance level for identity proofing but an authentication assurance level that provides confidence that the claimant controls authenticator(s) bound to the identified individual.

The regulated entity onboards the customer and provides a low risk bank account, with a very low threshold for value, transaction volume, and velocity and no crossborder transactions (these risk mitigation measures are based on risk analysis). The customer uses this account to obtain a mobile phone under a contract and receives digital wage payments directly into the bank account among other activities.

The regulated entity uses data associated with the direct deposit of wages, social transfers or benefits, to verify employment, occupation, and source of funds, and regular payments from the account for mobile phone and utility services to establish a pattern of responsible financial behaviour. The regulated entity also collects other transaction and associated authentication information to verify the customer's address. Over time, the regulated entity uses the customer's consistent financial activities and behavioural patterns (e.g., transaction times, typical amounts, purposes/counterparties and geolocation) to strengthen authentication for account access and anti-fraud measures.

The jurisdiction's AML/CFT legal framework is principles-, performance-, and outcomes-based. Its customer identification/verification regulations require regulated entities to have a reasonable basis to believe they know who their customers are, but do not rigidly prescribe how they are to achieve this objective. The regulated entity treats the data generated by the customer's activities over time as identity evidence and uses it to build confidence that it knows who its customer is and the customer's risk profile. When that confidence satisfies the regulated entity that it has complied with its customer identification/verification obligations and satisfied its own risk appetite and risk management practices and procedures for other financial services, the regulated entity offers a standard bank account with higher thresholds and greater functionality and later, provides a small loan, which the customer uses to start a business.

This approach for digital ID mirrors the same process which is set out in the FATF's 2017 Guidance on CDD and Financial Inclusion, where persons without adequate identity documents can undergo tiered CDD and progressively expand their level of access to financial services, beginning from a restricted, low-risk form of account. Source: US Treasury"

FATF Digital Identity (2020) par 168

7 Reviewing proposed design of SDD measures

It is important to critically review the proposed design of SDD measures to ensure that it meets the objectives of mitigating risk and supporting financial inclusion.

Sometimes designers are pressured to increase transaction caps to provide access for users who may need higher caps occasionally, for example farmers when they sell their crops. Instead of lifting the caps on transactions of all customers all year round to accommodate farmers thought may be given to allowing a limited number of transactions above the general cap per year. Alternatively thought

may be given to creating separate products for individuals and for sole proprietors such as small traders and farmers.

It is possible that proposed caps may also be too low to serve the interests of financially excluded persons. If the evidence supports a lower cap thought can be given to an additional control measure, e.g. enhanced account monitoring, that may allow adjusting the cap higher to support financial inclusion and to combat financial integrity risks linked to the cash-based economy.

Test the control measures from a criminal abuse perspective. What are vulnerabilities that can reasonably be explored? How can a criminal successfully evade any product or service restrictions? Are there sufficient grounds for concern to increase the proposed control measures? When this exercise is conducted it is important to remember that the control measures are meant to lower the risk level and not to ensure a low level of risk or even an absence of risk of criminal abuse.

Ongoing review of products and their criminal abuse is required. Once implemented the lower risk classification may attract criminal attention. Products and services subject to SDD should therefore be monitored to detect when levels of abuse may require an upwards adjustment in SDD. Should there be no evidence of abuse of the relevant products that information may inform a more relaxed SDD approach or may even convince a regulator that a proven low risk exemption might be appropriate.