EMERGING PAYMENTS ASSOCIATION

RISK ASSESSMENT GUIDANCE DOCUMENT THE EPA'S PROJECT FINANCIAL CRIME

January 2020

fscom

Expertise that adds value.

Contents

An introduction by the EPA

The Emerging Payments Association sets out to enable access to and trust in payments so people can pay and get paid more easily, quickly and securely.

This is only possible if the risks attached to any payment are assessed correctly. And what 'correctly' looks like is not clear, especially relating to the assessment of the risks of money-laundering.

So, our team of volunteers on Project Financial Crime, supported by our Benefactor Refinitiv, asked the experts at EPA member fscom to clarify this in this EPA Guide to Risk Assessment.

The guide describes an AML risk assessment and why is it necessary. It describes an 'Enterprise-Wide Risk Assessment (EWRA)' and a 'Customer Risk Assessment (CRA)'. It then makes the case for why and how often a risk assessment should be conducted.

Thank you to everyone involved with this project, and especially to fscom for helping us close this gap in knowledge in payments. Please pass this on to anyone involved with assessing risk in payments, anywhere in the world.

What is an AML risk assessment and why is it necessary?

A risk assessment for any business must be a combination of:

- Effective controls and systems;
- Proportionate to the size and nature of the business; and
- Robust enough to successfully mitigate the risk of Money Laundering and Terrorist Financing. (JMLSG part 1, 4.24 – 4.26)

According to the JMLSG (part 1, 4.6) It is the responsibility of senior management to manage the firm's affairs about the risks inherent in the business environment and jurisdictions the firm operates in.

The level of Money laundering and Terrorist financing throughout the world is believed to be on a much larger scale than originally documented through financial reporting, investigations and studies conducted by regulatory authorities. The mitigation and control of Money Laundering and Terrorist Financing is high on the agenda for both regulators and legislators globally.

A risk assessment is a business's way of identifying and understanding the level of risk (and types of risk) that the business is exposed to. It is the results from the risk assessment that allows for the risk appetite of the business to be formulated and the findings lead to the development of the necessary policies, procedures, systems, controls and training material the business requires to effectively control and mitigate the risk of ML/TF.

Each firm decides their own approach to the mitigation of ML/TF. This is called the risk-based approach. Each firm must document and rationalise their risk-based approach which should explain why they do what they do. The risk assessment also allows the business to focus their efforts and resources in the areas where risks are most prominent and in need of mitigation.

There are two parts to an effective risk assessment that firms should carry out as a matter of best practice prior to the establishment of a business relationship and before any transaction is authorised.

Enterprise Wide Risk Assessment (EWRA)

The EWRA identifies the risk of financial crime posed to a business on a whole firm scale. The customer risk assessment however is a secondary assessment which solely identifies the risks that each individual customer (private or corporate) pose to the business during onboarding and throughout the business relationship. Each customer poses their own unique risks to the business, and so must be assessed individually. Both the EWRA and the CRA are two pieces of the same puzzle and are intertwined to create the foundation for a strong and successful compliance program.

Example below:

Risk Number	Risk Type	Sub – Risk Type	Inherent Risk Type	Inherent Risk Rating	Controls effectiveness	Residual Risk Rating
RA1	Delivery Channel	A customer account us opened in fraudulent circumstance i.e. as part of impersonation fraud	The vast majority of the firms' customers are not dealt with face to face but through other delivery channels; for example, via the app or website The risk is that the firm allows a prospective client to open an account in fraudulent circumstances for example, by using stolen or forged identity documents. A related risk is the potential for a person to falsely purport to act on behalf of a corporate entity and to open an institutional	High	Individual and institutional customers who pass electronic or manual verification will be enabled to use their account. In order to mitigate the impersonation risk posed by the individual customers., the firm requires that the e-wallet account is funded from an account in the customer's name with a UK or EU regulated credit institution, or an assessed low risk jurisdiction. As such all fiat funded deposits and withdrawals are only to a bank or e-money account in the same name as the customer. Further to this, where the client is identified as higher money laundering or fraud risk, they will also be requested to upload a photograph of their face which reviewed by selfie recognition against the picture of on the ID to verify likeness. As regards to corporate customers, the signatory giving instructions to the Firm on behalf of the entity should be verified in line with the verification requirements for personal customers and proof of power to act on behalf of the entity	Low

			account in fraudulent circumstances.		will be obtained for the individual in question.	
RA2	Customer Risk	A prospective or existing customer is designated on an applicable financial sanctions list	The risk is that a sanctioned individual or entity designated on an applicable sanctions list uses the firm's facilities to undertake sanctions evasion	Low	The Firm will take all reasonable steps to ensure that all customers with whom a business relationship is established are screened against relevant notices published by: • The Office of Foreign Assets Control (OFAC) • Her Majesty's Treasury Department – UK (HMT) • European Union Sanctions (EU); and • United Nations sanctions (UN) Individual clients are automatically screened at onboarding by the onboarding tool and then on a monthly basis. Where a potential match is identified as part of ongoing monitoring this is reviewed by an outsourced intragroup function who can discount if applicable. Where the match is confirmed as true matches this is escalated to the Firm's compliance team. Confirm the firm do not have any clients identified as direct or linked sanction matches from the above list as clients.	Low

RA3	Geographic Risk	Funds received from a payer located in an area known to have high levels of criminal and/or terrorist activity	The risk is that an account is funded from a person or entity which is popularly recognised as having implemented lesser money laundering controls or recognised as being more exposed to bribery and corruption.	Medium	Individual and institutional customers who pass electronic or manual verification will be enabled to use their account. The Firm requires that an e-wallet is funded from a bank or e-money account in the customer's name with a UK or EU regulated credit institution, or an assessed low risk jurisdiction. The firm transaction monitoring is conducted primarily via the propriety system. The system is responsible for identifying suspicious activity transactions linked to customer e-wallets. Alerts generated for the client e-wallet.	Medium
RA4	Transactional Risk	A number of existing customers send payments to the same individual and/or entity.	The risk is that that a number of customers send payments to the same beneficiary and that this is indicative of money laundering	Medium	The firm has implemented tools to detect suspicious activity in relating to funding; this includes where a number of otherwise non-linked customers send payments to the same beneficiary. Further, the limited functionality of the pre-paid card for making outbound payments makes it unlikely that it could be used for money laundering and/or terrorist financing purposes in relation to making payment to the same beneficiaries. The only access that a client will have to funds is through approved merchants IPOS and ATM both of	Low

					which have undergone significant due diligence by our partner before authorisation as merchants i.e. is accepted by a limited number of merchants or point of sale. Further, withdrawal can only be made to either the funding account in the customers name or an account in the customers name which has been verified by way of micro payment.	
RA5	Product Risk	A customer uses the firm to make a payment to a merchant dealing in goods and services that are associated with a high risk of financial crime.	The risk is that a customer uses their account to transact with a merchant who has been identified as operating in a high-risk industry.	Medium	The firm has implemented a control where customers will not be allowed to make transactions with certain merchants operating under particular merchant category codes (MCCs) Any attempted transaction at this category of merchants will be blocked based on the MCC.	Low
RA6	General	The firm internal policies and procedures are not adequately followed by the relevant employees	The risk is that the relevant employees do not fulfil their personal obligations under the regulations and the firm internal policies and procedures.	Low	All the firm staff undergo two sets of required AML training. The first set is the learning management system training and the second set is additional compliance training from a member of the compliance team. The training is conducted at employee onboarding and prior to any employee normal course of business activities and annually following this and completed by all staff across the group.	Low

The additional training has been designed in house by the compliance team and is presented face to face to all staff. The AML training covers the key areas of:

- Defining money laundering and terrorist financing;
- UK specific legislation;
- Placing, layering, and integration;
- Personal responsibilities, personal and business punishment;
- PEP and sanctions risk;
- Suspicions, SARs and tipping off;
- Customers due diligence and its importance;
- Role of transaction monitoring;
- Customer behaviour red flags.

Staff training on anti-money laundering and counter terrorist financing will be carried out annually for all staff, and details recorded. The MLRO is personally responsible for oversite of the firm's compliance and with its requirements.

Customer Risk assessment (CRA)

Regulation 18 of the MLRs states that all customers of a business must be assessed on a much larger ML/TF scale due to the inherent risks that they pose to the business.

A customer risk assessment is an essential component of the enterprise wide risk assessment as the customer risk assessment evaluates and identifies all the unique ML/TF risks that each individual customer (private individual or corporate) through the nature of their business and activities pose to the onboarding business.

JMLSG guidance (part 1, 4.41) states that a risk assessment should always be performed at the inception of the customer relationship. However, for some customers, a comprehensive risk assessment of their profile may only become evident after the customer has begun transacting through their account. This allows the business to gather a greater understanding of the customers transaction behaviours and understand the profile of the customer on a larger scale. The monitoring of transactions and on-going reviews are therefore a fundamental component of a reasonably designed risk-based approach. Should the customer begin transacting outside of their intended/ forecasted volume, transaction monitoring and ongoing monitoring should flag an alert and an investigation should be conducted into the matter. If the customer begins transacting outside of the scope of the intended nature and purpose of the business relationship, again this should be flagged, and an event triggered risk assessment rerun. The results of the risk assessment may lead to the risk rating of the customer increasing, or potentially the customer relationship may be terminated in the event where there is a failure to fully understand and verify the change in transaction activity. (JMLSG, part 1 4.40, MLRs 2017 regulation 31(1))

Application of risk categories to potential and existing customers can provide a strategy for managing potential risks by enabling firms to subject customers to proportionate controls and oversight. The key risk criteria for an effective customer risk assessment include;

- Customer type
- Geography
- Product
- Delivery channel
- Transaction method

When assessing the customer risk, the business should consider all relevant risk factors before determining what the overall risk category and the appropriate level of mitigation to apply should be. The weight given to these criteria (individually or in combination) in assessing the overall risk of

potential money laundering may vary from one institution to another, depending on their respective circumstances. Consequently, firms have to make their own determination as to the risk weights that they set for each as this is part of the risk-based approach. (JMLSG Part 1, 4.47)

An example of a customer risk assessment may look like this:

CUSTOMER RISK ASSESSMENT				
Risk category	Risk type	Inherent Risk	Mitigating controls	Residual risk
Product Prepaid card	Card is used to load illicit funds in one jurisdiction and withdrawn in another	High	CDD, transaction monitoring.	Medium
Geography	Customer conducts business with a high-risk jurisdiction	High	Sanctions screening of Payer/Beneficiary, EDD, block transaction to high risk jurisdiction	Low
Customer Corporate	Complex corporate structure could be used to disguise UBO	Medium	EDD for complex corporate customers and full ID&V of UBOs	Low
Delivery channel	Non-face-to-face onboarding presents risk of impersonation	High	Anti-imp	Medium
Transaction method	Cash, online	High	Cash limit set, Transaction monitoring alert for anything above limit, freeze payment until authorised by senior management	Low

The business needs to have appropriate means of assessing the effectiveness of its risk mitigation procedures and controls and to identify areas that require improvement. The businesses policies, controls and procedures will need to be kept under regular review in relation to the risk assessment of the business and its customers.

A firm may also have to adjust its risk assessment of a customer based on information received from a competent authority. The risk assessment for a customer should be re - run during:

- Periodic review;
- Event driven due to a change in circumstance, this may include an existing customer becoming a named PEP, if this occurs, the business should conduct EDD and rerun the risk assessment of the customer to increase the risk score to high; and/or
- Trigger review: due to an alert from a transaction monitoring report where the customer has begun transacting outside of their usual transaction pattern.

JMLSG guidance (part 1, 4.74) and regulation 18 (4) of the MLRs states that, 'Firms must document their risk assessments in order to effectively demonstrate their basis, keep these assessments up to date, and have appropriate mechanisms to provide appropriate risk assessment information to competent authorities'.

Why conduct a risk assessment?

A businesses risk management is a continuous process, carried out on a dynamic basis. A money laundering/terrorist financing risk assessment is not a one-time exercise. A business must therefore ensure that their risk management processes for managing money laundering and terrorist financing risks are kept under regular review and all updates to it, documented.

Regulation 18 of The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 states that each firm has a regulatory requirement to '*take appropriate steps to identify and assess the risks of money laundering and terrorist financing to which the business is subject*'.

A good risk assessment is used to identify the money laundering and terrorist financing risks faced by the company and to further identify all risks of criminal activity occurring to and within the business including customer, employee, third party fraud, tax evasion, identity fraud. It will also assess the risk of a financial sanctions breach.

The risk assessment will assess the prevalence of an identified risk factor and establish the impact on the business depending on the likelihood of the risk occurring. The firm will then assess the likelihood of the risk occurring as well as the impact that it would have on the company. This assessment will then form the basis of a review into our anti-money laundering (AML), counter terrorism and financial crime systems and controls to ensure that counter measures are risk based and ensuring appropriate measures are in place to mitigate the identified risk with the objective being risk reduction.

Regulation 19 of the MLRs states that the nature and extent of a businesses AML/CTF controls will depend on several factors;

- The nature, scale and complexity of the firm's business;
- The diversity of the firm's operations, including geographical diversity;

- The firm's customer, product and activity profile;
- The distribution channels used;
- The volume and size of transactions; and
- The extent to which the firm is dealing directly with the customer or is dealing through intermediaries, third parties, correspondents or non-face to face access.

How often should the Risk assessment be conducted?

As referenced in the JMLSG guidance (part 1, 4.82) a business should run the risk assessment on an annual basis at least during periodic review. Throughout a 12-month period, the risk assessment may be refreshed in circumstances such as a significant change to circumstances e.g. change to a customer's corporate structure, a customer adding a new beneficiary etc., the other event when the risk assessment may be re conducted is due to an event driven trigger. An event driven trigger may occur when there has been an alert on a customer's profile such as a change to the PEP list. In the event where a current customer becomes a PEP, the customer risk assessment would need to be rerun.

The business is however entitled to take a risk-based approach and can conduct the risk assessment on an ad hoc basis throughout the year, if it is fully conducted periodically.

The risk assessment of a business is an essential starting point on a broad spectrum of compliance and ML/TF risk mitigation. A good risk assessment contributes to a strong compliance monitoring programme which also includes ongoing monitoring and screening. The risk assessment lays out the risks, formulates policies and procedures, and finally identifies and allocates the systems and controls that are necessary to mitigate the risks. Together the risk assessment identifies the risks, yet the systems and controls must also be tested to ensure that a businesses whole firm risk mitigation policy is appropriate, proportionate, effective and robust.

Disclaimer

This information is for guidance purposes only and should not be regarded as a substitute for taking professional advice.

The Emerging Payments Association (EPA), established in 2008, connects the payments ecosystem, encourages innovation and drives profitable business growth for payments companies. Its goals are to strengthen and expand the payments industry to the benefit of all stakeholders.
It achieves this by delivering a comprehensive programme of activities for members with help from an independent Advisory Board, which addresses key issues impacting the industry. These activities include:

- 12-month event programme
- Annual Black-Tie award ceremony
- Leading industry change projects
- Lobbying activities
- Training and development
- Research, reports and white papers

The EPA has over 150 members and is growing at 30% annually. Its members come from across the payments value chain; including payments schemes, banks and issuers, merchant acquirers, PSPs, retailers, and more. These companies have come together, from across the UK and internationally, to join our association, collaborate, and speak with a unified voice.