MFSA
MALTA FINANCIAL SERVICES AUTHORITY

FIAU
MALTA
FINANCIAL INTELLIGENCE ANALYSIS UNIT

Supervisory Guidance Paper

on ML and TF Institutional/Business Risk Assessment

Issued jointly by the Financial Intelligence Analysis Unit and the Malta Financial Services Authority

This Supervisory Guidance Paper is being issued by way of supervisory outreach as a follow up to the sector-specific training on the ML and TF institutional/business risk assessment, delivered between 22 January 2018 and 25 January 2018.

This Supervisory Guidance Paper is not binding. It provides high level guidance and is intended for information and to assist subject persons to better understand their obligation to carry out their ML and TF risk assessment.

The Financial Intelligence Analysis Unit is in the process of revising the binding Implementing Procedures which will contain detailed procedures on how the risk-based approach is to be applied. A consultation document will be issued later on this year.

This Guidance Paper makes reference to a number of compliance structures which may not always be present or relevant within a subject person's setup as a result of the nature and/or size of the activity. This may be the case where a subject person has a small setup or in the case of one person "self-employed" subject persons. In any such circumstances, the ML and TF business risk assessment would still have to be carried out by the subject person.

Introduction

In order to use a comprehensive and risk-based approach, it is necessary to first make an analysis of the money laundering and terrorism financing risk that your institution is exposed to. You have to make such a risk assessment because the risk of money laundering and terrorist financing is not the same in every case. The risk-based approach is not an unduly permissive option, but it involves the use of evidence-based decision-making. This provides for a more efficient approach to target the risks of money laundering and terrorist financing that financial institutions face.

Primarily, responsibility for the quality and execution of the ML/TF risk assessment lies with the first line. This is the business, as risks manifest themselves first there. The role of Compliance is process monitoring, facilitating and testing. Other departments such as Security and Audit can also provide the necessary input. The ultimate responsibility for the integrity risk analysis lies with the management board.

Legal basis

Article 8 EU Directive 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing

Obliged entities shall take appropriate steps to identify and assess the risks of money laundering and terrorist financing, taking into account risk factors including those relating to their customers, countries or geographic areas, products, services, transactions or delivery channels. Those steps shall be proportionate to the nature and size of the obliged entities. The risk assessments shall be documented, kept up-to-date and made available to the relevant competent authorities and self-regulatory bodies concerned. Competent authorities may decide that individual documented risk assessments are not required where the specific risks inherent in the sector are clear and understood.

Regulation 5(1) of the Prevention of Money Laundering and Funding of Terrorism (PMLFTR)

Every subject person shall take appropriate steps, proportionate to the nature and size of its business, to identify and assess the risks of money laundering and funding of terrorism that arise out of its activities or business, taking into account risk factors including those relating to customers, countries or geographical areas, products, services, transactions and delivery channels and shall furthermore take into consideration any national or supranational risk assessments relating to risks of money laundering and the funding of terrorism.

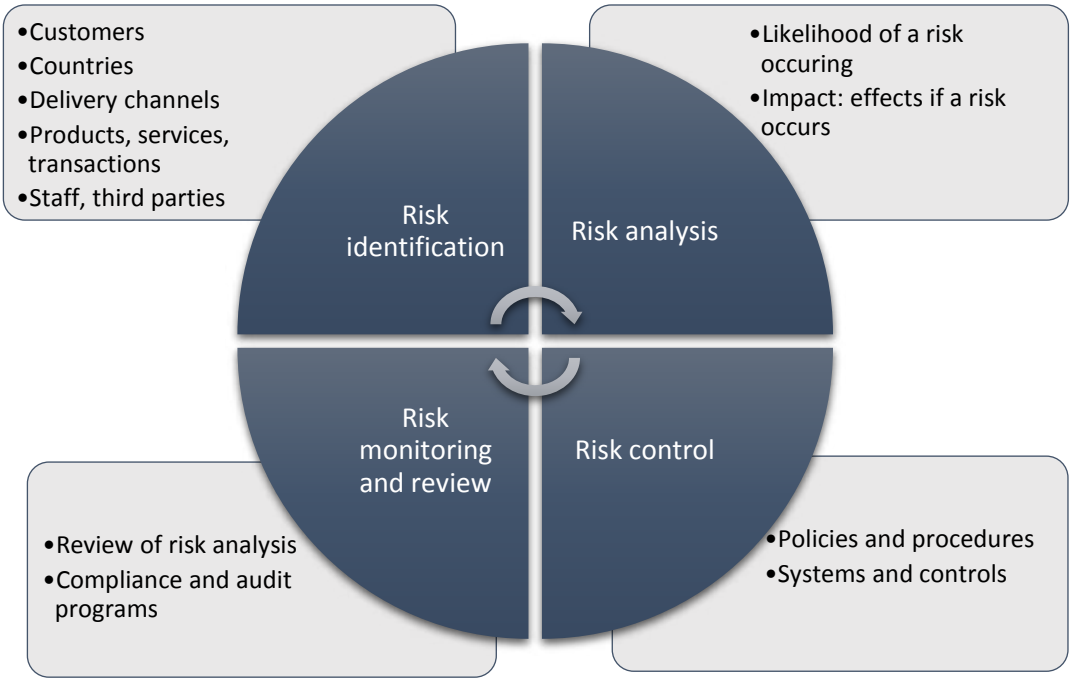
Methodology

A risk assessment starts with determining the inherent risks, i.e. the risks that exist if there are no control measures in place to mitigate them. Inherent risks consist of threats and vulnerabilities. Threats are caused by external factors such as clients or incoming payments, vulnerabilities exist because of products or delivery channels. Inherent risk is a function of likelihood and impact. Likelihood is the chance that a risk occurs; impact is the negative influence on the continuity of the company when a risk occurs.

To identify and assess the risks, it is necessary to examine the nature and size of the risks. First of all, the inherent risks need to be identified by analysing the nature and size of likely risk scenarios that could be related to factors such as clients, products, transactions, in combination with geographical factors and delivery channels. Second, the effectiveness of the control measures in place needs to be determined and offset against the inherent risks. The outcome of this process is the residual risk: the risk that remains after all procedures and measures have been implemented effectively. The institution will also have to determine to what extent the risks are acceptable and within the risk appetite.

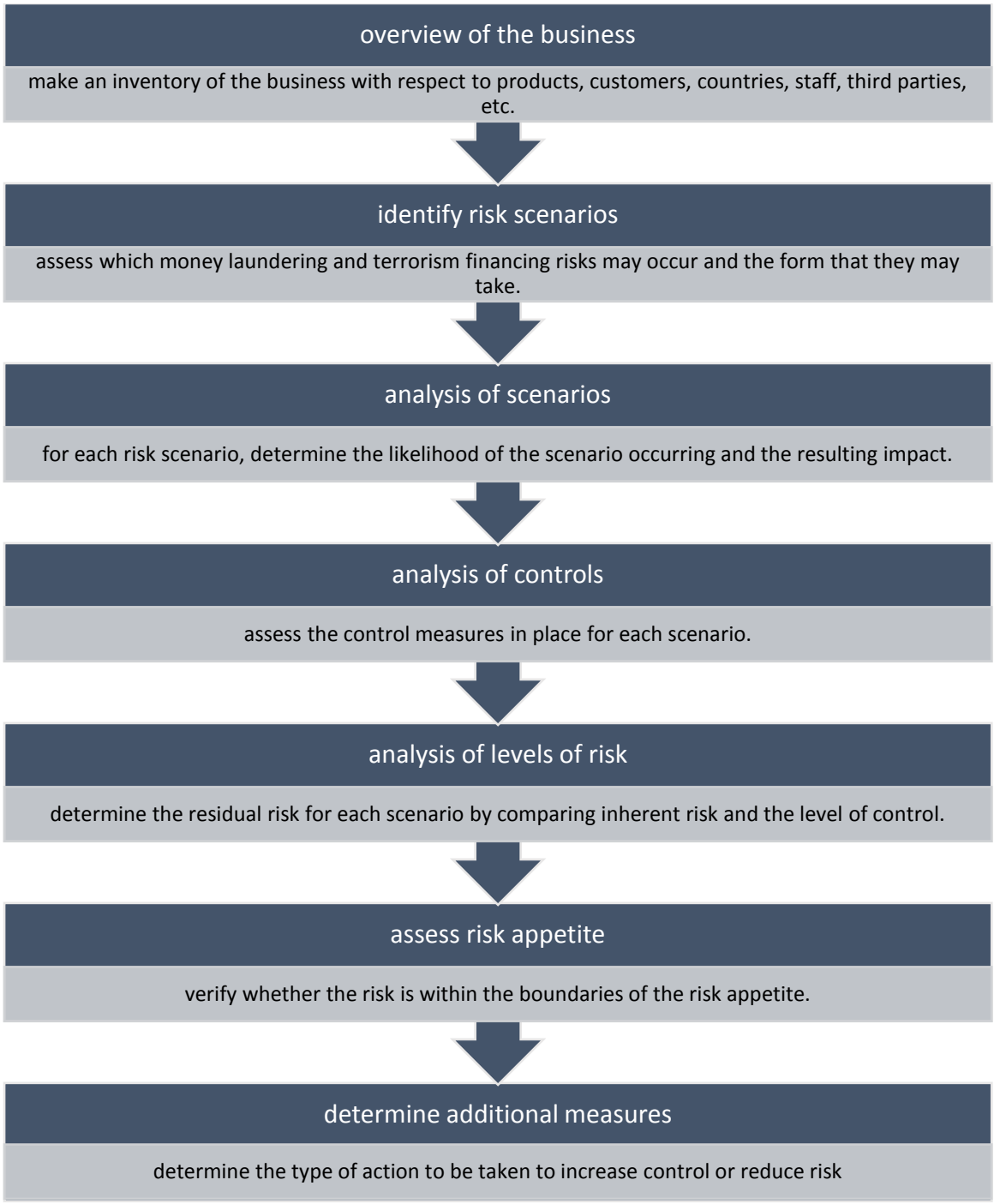
Cyclical process

The risk assessment is a cyclical process, which means that you are required to perform the whole cycle of identification, analysis and testing of the effectiveness of controls at regular intervals. This is because risks are not static. Risks to institutions may change as a result of both internal and external factors. Your institution's activities or products may for instance be expanded or changed, specific trends may emerge in the financial and economic world, or laws and regulations may be amended.



Steps

The steps below have to be taken to develop an ML and TF risk assessment.



1. Overview of the business: make an inventory of the business with respect to products, customers, countries, staff, third parties, etc.

In order to perform a risk assessment, you need an accurate picture of your organisation: a quantitative analysis of the size and nature of the institution. This means that you will have to map out the different areas of your institution where ML and TF risks may occur. This entails making an up-to-date description of the nature and size of the company and the markets in which it operates. Larger institutions should also analyse their units and business lines. Subsidiaries and branch offices should also map out their own activities.

In this first step, you make an overview of the number and type of customers, the products provided to these customers, countries where these customers are active, payments received, etc. These are the so-called risk factors; the factors that expose your organisation to risk:

- Customers
- Products
- Services
- Transactions
- Geography
- Employees
- Third parties
- Delivery channels

This organisation overview will provide you with an accurate picture of all factors exposing your organisation to risks.

2. Risk scenarios: assess which money laundering and terrorism financing risks may occur and the form that they may take.

Inherent risks are the risks that exist if there are no control measures in place to mitigate them. Inherent risks consist of threats and vulnerabilities. You need to know how both money laundering and terrorism financing can manifest themselves. In other words, the different forms that ML and TF can take. The inherent risk assessment focuses on the estimated intent and capability of criminals and terrorist financiers to exploit existing or new products and services for money laundering and for terrorism financing. The assessment specifies the methods that can be deployed to misuse your institution for money laundering or terrorism financing. It is an inventory of the threats that your organisation is exposed to. It is important to make an assessment for money laundering and one for terrorism financing.

3. Analysis of scenarios: for each risk scenario, determine the likelihood of the scenario occurring and the resulting impact.

The question to assess is what the likelihood is that your institution enables money laundering or terrorism financing and what the impact will be if a risk materialises. The risk scenarios that were developed in step 2 are scored for likelihood and impact. After your institution has outlined the possible scenarios and has determined how to assess likelihood and impact, you must now actually analyse the scenarios. Likelihood is the occasions per period, is something unlikely or likely to happen. Impact is damage or loss to the institution, or the short-term or long-term effects. This is ideally based on qualitative and quantitative input.

Likelihood and impact together constitute inherent risk. You could assess for each scenario whether these inherent risks are within the boundaries of your institution's risk appetite (see also step 6).

For likelihood, various system can be used, for instance:

1 - Low	• the scenario can occur less than once per year, very unlikely
2 - Medium	• the scenario can occur once per year, small chance
3 - High	• the scenario can occur a few times per year, reasonable chance
4 - Extreme	• the scenario can occur several times per year, very high chance

Also for impact, several systems can be used, for instance:

1 - Low	• negligible loss or damage, no measure from supervisor, no effect
2 - Medium	• limited loss or damage, simple measure from supervisor, short-term effect
3 - High	• large loss or damage; some measures from supervisor, medium-term effect
4 - Extreme	• severe loss or damage, heavy measures from supervisor, long-term effect

This results in the following inherent risk scores:

IMPACT / LIKELIHOOD	1	2	3	4
1	Low Risk	Low Risk	Moderate Risk	High Risk
2	Low Risk	Low Risk	Moderate Risk	High Risk
3	Moderate Risk	Moderate Risk	High Risk	Extreme risk
4	High risk	High Risk	Extreme risk	Extreme risk

4. Analysis of controls: assess the control measures in place for each scenario.

The next steps are to determine the effectiveness of the control measures that are taken to mitigate the inherent risks. In a risk assessment, the overview of the control measures ideally shows the implementation and effectiveness of the safeguards in place. It is very important that you assess the level of control realistically. If you want to create an accurate picture of possible large risks that are only partially controlled, it is no use making an overoptimistic assessment of control. Possible sources are reports on incidents, audit reports, compliance monitoring reports and supervisory findings.

You should analyse the control measures necessary for each scenario. This means for example that you should specify all processes and evaluate them on effectiveness. This is an obvious task for Compliance, Audit, and various other departments where control measures are performed. Compliance has a monitoring role and will therefore be aware of the level of risk control in the institution. Using the knowledge and insight from the business is, however, essential for this part of the analysis.

An assessment system that can be used is for instance:

1 - Strong	• There are several measures in place to control risk, fully operational and fully effective
2 - Effective	• Risk is managed adequately, could be improved in certain parts, but works adequately and is effective
3 - Ineffective	• Risk is not managed adequately, substantial improvement necessary, but has some effect
4 - Non-existent	• No controls, or controls have no effect

5. Determination of residual risks: determine the residual risk for each scenario by comparing inherent risk and the level of control.

Residual risk is determined by 'subtracting' the level of control from inherent risk. Residual risk is the inherent risk left once effective control measures are in place.

The residual risk assessment can be as follows:

Residual Risk	*Description*
Low	The risk is unlikely to cause damage.
Moderate	There is a slight chance of this risk causing some damage.
High	There is a considerable likelihood of this risk causing large damage.
Extreme	There is a certainty of this risk causing dramatic impact.

6. Risk appetite: verify whether the risk is within the boundaries of the risk appetite.

Risk appetite is a framework developed by senior management and the board prescribing the type and level of risk that the institution is prepared to accept. Risk appetite specifies the boundaries that staff have to respect when pursuing the institution's strategy. The risk appetite should for instance specify the shortcomings and violations that the institution does not want to be involved in. If risks fall outside your institution's risk appetite, you should consider not providing the services concerned, or no longer serving a particular type of customer.

After determining residual risk, you should verify whether this is within the boundaries of your institution's risk appetite. In other words, you should determine the level to which your institution is prepared to accept, mitigate, or avoid the remaining residual risk. If this residual risk is not within the boundaries of your institution's risk appetite, you should take additional control measures, reduce the risk in question, or avoid the risk by ending the activities. If reduction is impossible due to the nature of the risk (e.g. countries that customers receive payments from), you must of course make sure that additional control measures are taken. It will be impossible to reduce all risks to 'zero', residual risk may remain after additional measures have been put in place.

Risk appetite
Accept: mitigating measures are working
Reduce: reduce risk or improve controls
Avoid: end the activities

7. Determination of additional measures: determine the type of action to be taken to increase control or reduce risk

This part of the risk assessment, where deficiencies are found in the control of risks is particularly important for management to be aware of. Management will then have to act on the deficiencies identified in the analysis, as it will use the risk analysis as a guiding instrument. This is because the risk assessment highlights the risks that need more control and those that may be mitigated by means of less strict control.

In this final step, you need to determine what additional measures are necessary, for instance changes in policies and procedures, additional training and risk awareness raising, or improving IT systems.

Summary

The risk assessment should

- address ML and TF
- be comprehensive
- be up-to-date and updated regularly
- be based on qualitative and quantitative information
- have relevant risk scenarios and risk factors
- assess likelihood and impact in a substantiated, plausible way
- have a clear, realistic assessment of the control measures per scenario
- give an overview of residual risks, gaps
- set risks against the risk appetite
- determine follow up measures
- cover the entire business: all business lines, branches, departments, subsidiaries
- serve as a basis for the internal policies and procedures
- function as a steering document for management
- be communicated within the institution
- involve 1st line, Compliance, Audit, Risk and Management

Examples of risk factors

Clients	***Products/services/transactions***
PEPs	Trade finance transactions
High residual worth clients	Credit/prepaid cards with no or high limits
Non-resident clients	Services to non-account holders
IIP program client	Cash transactions
Cash intensive businesses	Domestic transactions
Online gaming operators	International transactions
Bitcoin exchanges	Investments in real estate, private equity, race horses, wines
SPV, Personal asset holding vehicles	Omnibus accounts
Charities, NGOs	Only providing business address (no other services)
Trusts, legal arrangements	Acting as nominee
	Setting up company with bearer shares
	Management of SPV
Quantitative information to consider for these risk factors:	**Quantitative information to consider for these risk factors:**
✓ Number of customers in each category	✓ Number of
✓ Number of customers per risk category	○ products/services/transactions
✓ Maturity of customer base	○ customers per product and service
✓ Volume of business	✓ Volumes related to each product or service
Geography	***Delivery channels***
UN and EU Sanctions	Direct
High-risk jurisdictions (FATF list)	Non face to face
Tax-related (EU list)	Introduced business
Corruption-related (TI-CPI)	Intermediaries
Terrorism-related	Agents
Offshore financial centres	Other channels
Quantitative information to consider for these risk factors:	**Quantitative information to consider for these risk factors:**
✓ Number of branches or subsidiaries	✓ Number of relationships started non face to face
✓ Number of customers, UBOs	✓ Number of introducers and intermediaries
✓ Number of transactions to or from	✓ Number of customers through introducers or intermediaries
✓ Trade finance facilities	
✓ Correspondent relationships	

Examples of risk scenarios

What is the likelihood that your institution enables money laundering or terrorism financing

- by serving clients with complex or opaque corporate structures
- by working with intermediaries or introducers
- because of clients or UBOs from high risk countries
- because of the institution's own international activities
- because of receiving large sums of funds from high risk countries
- because a client pays with cash
- because an unknown third party pays
- because the valuation report does not reflect the real value
- because an employee colludes with a third party
- because a SME client frequently deposits cash
- through your bitcoin exchange or gaming clients
- because you deal with nominee accounts
- et cetera

Step 1: preparation and identification

- Business inventory: make an inventory for each business unit/branch office/subsidiary of the organisation with respect to products, customers, countries, staff, third parties, et cetera.
- Scenarios: assess which risks may occur and the form that they may take.
- Scoring system: determine how to assess likelihood and impact

Step 2: analysis

- Gross risks: for each scenario, determine the likelihood of the scenario occurring and the resulting impact.
- Risk appetite: assess the gross risk and verify whether this is within the boundaries of your risk appetite.
- Controls: list and assess the control measures in place for each scenario.

Step 3: assessment and measures required

- Net risks: determine the net risk for each scenario by comparing gross risk and level of control.
- Risk Appetitie: determine whether net risk is within the boundaries of your risk appetite.
- Measures: determine the type of action to be taken, increase control or reduce risk.

IDENTIFICATION			**ANALYSIS**						**ASSESSMENT**			
Risk	Factor	Scenario	Likelihood	Impact	Gross Risk	Risk appetite	Control measures	Assessment of control	Net risk	Risk appetite	Gap	Measures required
Which integrity risks is the institution likely to face?	*Which factors play a role for each risk?*	*How is the risk likely to manifest itself?*	*What is the likelihood of a particular scenario occurring?*	*What will be the impact on the institution if the scenario materialises?*	*Determine the inherent risk by assessing its likelihood and impact*	*Is the inherent risk within the boundaries of the risk appetite?*	*Which control measures are in place for each risk scenario?*	*How effective are these control measures?*	*Determine net risk by assessing gross risk and the relevant control measures in place*	*Is the net risk within the boundaries of the risk appetite?*	*Are there any deficiencies where measures are concerned?*	*Which measures are required in order to control or avoid this particular risk?*
Money laundering	Customers											
	Transactions											
	Third parties											
	(…)											
Terrorist financing	Customers											
	Transactions											
	Third parties											
	(…)											
Circumvention of sanctions (PF)	Customers											
	Transactions											
	Branches											
	(…)											
(Corruption / bribery)	Staff											
	Third parties											
	(…)											