2021

Anti-Money Laundering and Countering Finance of Terrorism Risks Assessment,2021

The United Republic of Tanzania

Ministry of Finance

THE UNITED REPUBLIC OF TANZANIA
FINANCIAL INTELLIGENCE UNITE

ANTI-MONEY LAUNDERING AND COUNTERING FINANCING OF TERRORISM RISK ASSESSMENT

GUIDE

SEPTEMBER, 2021

1.0 The objective of this guideline

1.1 This guideline is designed to help you conduct money laundering and terrorism financing risk assessment (Risk Assessment) under the Anti-Money Laundering Act (Cap. 423) and Prevention of Terrorism Act (Cap. 19).

1.2 You understand your business better than anyone else and therefore you are best placed to identify and determine the level of risks your business faces from money laundering (ML) and terrorism financing (TF), and to develop appropriate strategies to manage and control these risks.

1.3 A risk assessment is the first step that you must take before developing an AML/CFT programme (programme). It involves identifying and assessing the inherent risks your business reasonably expects to face from ML/TF. Once you complete a risk assessment, you can then put in place a programme that minimizes or mitigates these risks. Your programme must be based on the risk assessment. You should keep in mind that an effective AML/CFT regime is risk-based and the programme must manage and mitigate the ML/TF risks faced by your business. For instance, if you are a low-risk business you may only need a simple programme that is proportionate to your low risk.

1.4 Following this guideline is not mandatory. However, you must undertake a risk assessment and must establish a programme.

1.5 Your risk assessment and programme should reflect a risk-based approach that allows you some flexibility in the steps you take when meeting your AML/CFT obligations. A risk-based approach does not stop you from engaging in transactions/activities or establishing business relationships with higher-risk customers. Rather, it should help you to effectively manage and prioritize your response to ML/TF risks. The examples in this guideline are suggestions to help you meet your obligations under the Act. They are not exhaustive and are illustrative in nature.

1.6 This guideline is for information purposes only. It cannot be relied on as evidence of complying with the requirements of the Act. It does not constitute legal advice from any of the AML/CFT and cannot be relied upon as such. After reading this guideline, if you still do not understand any of your obligations you should contact your AML/CFT supervisor or seek independent professional advice.

1.7 You can access the AML/CFT guidance referenced in this guideline at the FIU website.

2.0 TERMS USED IN THIS GUIDELINE

For the purposes of this guideline, the following definitions apply.

"Material change" – ML/TF risk is not static and can change quickly. A material change is an event, activity or situation that you identify that could change the level of ML/TF risk you may encounter.

"Risk-based approach" refers to the proportionate AML/CFT measures that you implement in response to identified risks. An effective risk-based approach (sometimes called RBA) allows you to exercise informed judgement when meeting your AML/CFT obligations. Under a risk-based approach, there is no such thing as "zero risk".

"Inherent risk" is the assessed ML/TF risk before any AML/CFT controls and measures are in place.

"Residual risk" is the assessed ML/TF risk after AML/CFT controls and measures have been put in place.

"Gatekeepers" – The legal, accountancy, real estate, and trust and company service provider sectors are known as designated non-financial businesses and professions, or more commonly as "gatekeepers". Gatekeepers refers to the role they play in providing services and products that can be used to facilitate the entry of illicit funds into the legitimate financial system.

Suspicious Transaction Reports or the acronym (STRs) is used to denote both types of reporting for the purposes of this guideline.

PART I

3.0 THE OBJECTIVE OF AMLA AND POTA

The purposes of the AMLA and POTA are to:

(a) detect and deter money laundering (ML) and terrorism financing (TF);

(b) maintain and enhance the United Republic of Tanzania's international reputation by adopting, where appropriate in the United Republic of Tanzanian context, recommendations issued by the Financial Action Task Force (FATF);

(c) contribute to public confidence in the financial system.

3.1 WHAT YOU HAVE TO DO

The first things you should do as part of your obligations under the Act are:

(a) appoint an AML/CFT compliance officer (compliance officer);

(b) conduct a risk assessment to identify and determine the ML/TF risks you may encounter in the course of your business;

(c) develop and implement a programme containing the procedures, policies and controls used to manage and mitigate those risks.

3.2 RISK ASSESSMENT

3.2.1 A core element of your AML/CFT regime is an adequate and effective risk assessment. The risk assessment is the foundation of a proportionate risk-based AML/CFT framework. Your AML/CFT supervisor expects that you will have a clear understanding of the ML/TF risks and vulnerabilities you face during the course of business.

3.2.2 You must base your programme on your risk assessment. The risk assessment is the foundation document for your entire AML/CFT regime. This should be clearly explained in your risk assessment and programme documentation.

3.3 USING AML/CFT GUIDANCE

You must consider any applicable guidance material produced by your AML/CFT regulator or the Financial Intelligence Unit (FIU) and any other information provided in relation to the regulations. We strongly recommend that you are familiar with the following documents before you undertake your risk assessment.

(a) The National Risk Assessment (NRA);
(b) FIU guidance material accessible to reporting entities;
(c) Sector risk assessments (STRs) produced by the sector regulator;
(d) Industry-specific guidance (if any).

3.4 LEGAL OBLIGATION RELATING TO RISK ASSESSMENTS

3.4.1 As a reporting entity you have a number of obligations under the Act in relation to your risk assessment:

(a) Your risk assessment must identify the risk of ML/TF you may reasonably expect to face during your business;

(b) Your risk assessment must enable you to determine the level of risk involved in relation to relevant obligations under the Act. This includes the ML/TF risk presented by your customer, the products and services you offer and the countries you deal with;

(c) Your risk assessment must be in writing and include a description of how it will be kept up to date;

(d) Your risk assessment must have regard to guidance produced by the sector regulator and the FIU;

(e) You must use your risk assessment to develop your programme as set out in the Act;

(f) You must review your risk assessment to ensure it is up to date, identifies any deficiencies, and make any changes identified as necessary;

(g) Your risk assessment must be independently audited by an appropriately qualified person every two years or at any other time at the request of your sector regulator;

3.4.2 You must also prepare and submit an annual report to your Sector regulator. This must be submitted at a time appointed by the regulator.

3.4.3 When conducting your risk assessment, you do not have to follow the processes in this guideline. As long as you comply with your obligations under the Act and any other applicable laws or regulations, you can choose the method of risk assessment that best suits your business. For example, large financial institutions may have their own systems and methodology for conducting a risk assessment. However, you should be prepared to explain and demonstrate the adequacy and effectiveness of your procedures, policies and controls.

3.4.4 When evaluating your risk assessment (and your programme), the regulator and auditors will want to explore both adequacy and effectiveness. Adequacy is described as how compliant your risk assessment is with the various obligations of the Act. Effectiveness is described as how well the practical application of the risk assessment meets the obligations of the Act. This will be something you discuss with your regulator and auditor.

3.5 BACKGROUND ON MONEY LAUNDERING AND TERORISM FINANCE THREATS

3.5.1 Financial Action Task Force (FATF) recommendations - All countries are exposed to illicit international money flows. The global nature of ML/TF is reflected in the work of the FATF based on input from international experts. The FATF 40 Recommendations and 11 Immediate Outcomes represent a global standard of AML/CFT. Compliance with and demonstrated effective use of these standards are an important part of Tanzania's international reputation and ability to combat ML/TF. URT was evaluate in 2009 and 2020 on these standards and outcomes.

3.5.2 It is estimated that in Tanzania illicit funds typically originate from three sources: commercial tax evasion, trade mis invoicing and abusive transfer pricing; criminal activities, including the drug trade, human trafficking, illegal arms dealing, and smuggling of contraband; and bribery and theft by corrupt government officials. These estimates exclude transnational laundering of overseas proceeds of crime and laundering.

3.5.3 United Republic of Tanzania faces an unknown scale of ML generated from overseas proceeds of crime. The International Monetary Fund estimates that approximately 2–5% of global GDP (approximately US$2 trillion) is the proceeds of crime.

3.6 TERRORISM FINANCING

Although TF risk is assessed as low in Tanzania, it is prudent to provide guidance on the vulnerabilities and risks associated with the global issue of TF. Please refer to your relevant STR and the NRA for more information on the financing of terrorism.

3.7 STAGES OF MONEY LAUNDERING

3.7.1 It is worthwhile covering some of the basics of ML/TF before considering ML/TF risk. ML is generally considered to take place in three phases: placement, layering and integration. TF shares many of the characteristics of ML but may also involve legitimate funds and usually involves smaller amounts.

3.7.2 Placement occurs when criminals introduce proceeds of crime into the financial system. This can be done by breaking up large amounts of cash into smaller sums that are then deposited directly into an account, or by purchasing shares or by loading credit cards. In some offences, such as fraud or tax evasion, placement is likely to occur electronically and may be inherent in the offence.

3.7.3 Layering occurs once proceeds of crime are in the financial system. Layering involves a series of conversions or movements of funds in order to distance or disguise them from their criminal origin. The funds might be channeled through the purchase and sale of investment instruments or high-value goods or be wired through various accounts across the world. In some instances, the launderer might disguise the transfers as payments for goods or services, giving them an appearance of legitimacy.

3.7.4 Integration occurs once enough layers have been created to hide the criminal origin of funds. This stage is the ultimate objective of laundering: funds re-enter the legitimate economy, such as in real estate, high-value assets, or business ventures, allowing criminals to use the criminal proceeds of offending.

3.8 PREDICATE OFFENCES

Predicate offences are the crimes underlying ML/TF activity. It is important that you understand the various types of predicate offences. Please refer to AMLA, your relevant STR and the NRA for more information on predicate offending.

PART II

4.0 IDENTIFYING RISK

As part of assessing risk, you must address your "inherent risks". These are the ML/TF risks present before you apply controls and mitigations. You may wish to assess your "residual" risk (the risk after your controls and mitigations) as part of your risk assessment. However, your regulators will expect that your risk assessment deals with inherent risk. If your risk assessment covers residual risk, you will need to document and demonstrate how you arrived at your residual risk ratings.

When you identify how your business may be vulnerable to ML/TF risks, you must consider all of the following:

(a) the nature, size and complexity of your business;
(b) the products and services you offer;
(c) the way you deliver your products and services;
(d) the types of customers you deal with;
(e) the countries you deal with;
(f) the institutions you deal with.

4.1 THE NATURE, SIZE AND COMPLEXITY OF YOUR BUSINESS

4.1.1 The size and complexity of your business plays an important role in how attractive or susceptible it is for ML/TF. For example, because a large business is less likely to know its customers personally, it could offer a greater degree of anonymity than a small business. Likewise, a business that conducts complex transactions across international jurisdictions could offer greater opportunities to money launderers than a purely domestic business.

4.1.2 Use of corporate data will help you work out what parts of your business are vulnerable to ML/TF activity. For instance, you may have identified a higher-risk product, but without knowing how many of those products you have provided to 8 customers, and where they are domiciled, this will result in a flawed assessment of risk. Using your annual report data will help in this matter.

4.2 THE PRODUCTS AND SERVICES YOUR BUSINESS OFFERS.

4.2.1 Some products and services are vulnerable to ML/TF by their nature. When considering whether the products and services your business offers could be exploited for ML/TF purposes, we recommend you consider issues such as:

(a) Does the product/service allow for anonymity?
(b) Does the product/service disguise or conceal the beneficial owner of your customer?
(c) Does the product/service disguise or conceal the source of wealth or funds of your customer?
(d) Does the product/service allow payments to third parties?
(e) Does the product/service commonly involve receipt or payment in cash?
(f) Has the product/service been identified in the NRA, FIU guidance material or STRs as presenting a higher ML/TF risk?
(g) Does the product/service allow for the movement of funds across borders?

4.2.2 Many other factors can contribute to the ML/TF risk of your products and services. It will be your responsibility to identify those factors as part of your risk assessment. Domestic AML/CFT guidance material will help you in this exercise.

4.3 THE WAY YOUR BUSINESS DELIVERS ITS PRODUCTS AND SERVICES

The way your business on-boards your customers and delivers your products and services affects its vulnerability to ML/TF. For example:

(a) Does your business have non-face-to-face customers (via post, telephone, internet or via intermediaries)?
(b) Do you provide your products/services via the internet?
(c) Does your business have indirect relationships with customers (via intermediaries, pooled accounts, etc)?
(d) Do you provide your products/services via agents or intermediaries?
(e) Do you provide your products/services to overseas jurisdictions?

4.4 THE TYPES OF CUSTOMERS YOUR BUSINESS DEALS WITH

4.4.1 Some categories of customers pose a higher risk of ML/TF than others, especially when combined with higher-risk products/services and jurisdictions.

4.4.2 The legislation sets out circumstances where you must conduct enhanced customer due diligence (EDD) and where simplified customer due diligence (CDD) applies. These sets of circumstances are a useful reference point for the types of situations that may present a higher or lower risk of ML/TF.

4.4.3 Questions you will need to ask yourself about your customers, new and existing, include:

(a) Are they a trust or other legal person?
(b) Have you identified beneficial ownership?
(c) Are they specified in the Act as requiring EDD?
(d) Are they involved in occasional or one-off activities/transactions above a certain threshold?
(e) Do they use complex business structures that offer no apparent financial benefits?
(f) Are they a politically exposed person (PEP)?
(g) Are they a cash-intensive business?
(h) Are they involved in businesses associated with high levels of corruption?
(i) Do they have an unexplained or hard to verify source of wealth and/or source of funds?
(j) Do they conduct business through, or are they introduced by, gatekeepers such as accountants, lawyers, or other professionals? (Refer to your relevant STR for more information on gatekeepers.)
(k) Are they a non-profit organization?
(l) Have they been identified in the NRA, FIU guidance material or STRs as presenting a higher ML/TF risk?

4.4.4 This list is not exhaustive, and many other factors can contribute to customer ML/TF risk. As with your products and services it will be your responsibility to identify those factors as part of your risk assessment. Domestic and international guidance material will help you in this exercise.

4.5 THE COUNTRIES YOUR BUSINESS DEALS WITH

4.5.1 It is important to understand that the risks associated with a country are wider than having insufficient AML/CFT measures in place. It is also important to recognise the international operation of ML/TF and that Tanzania's reputation as a high-integrity, low-corruption jurisdiction makes it vulnerable to abuse. Country risk can result from:

(a) ineffective AML/CFT measures;
(b) ineffective rule of law and economic stability;
(c) high levels of organized crime;

(d) prevalence of bribery and corruption;
(e) association with TF
(f) conflict zones and their bordering countries;
(g) production and/or transnational shipment of illicit drugs.

4.5.2 To help you determine country risk, various information sources can help you in assessing country risk including:
(a) FATF list of high-risk and non-cooperative jurisdictions;
(b) FATF mutual evaluation reports;
(c) European Union AML and tax blacklists;
(d) Basel AML Index;
(e) United Nations Office on Drugs and Crime (UNODC)reports;
(f) Transparency International Corruption Perceptions Index;
(g) trusted and independent media sources.

4.5.3 While not directly associated with AML/CFT, you may want to consider checking if countries are subject to United Nations sanctions, embargoes or similar measures.

4.6 The institutions your business deals with

4.6.1 Some institutions present more ML/TF risk than others. This may be due to the nature of their industry or their association, or the types of business relationships that they have. For instance, financial institutions that are unregulated or shell companies and banks are high-risk institutions and are more likely to be used for ML/TF purposes or operated by criminals to disguise beneficial ownership.

4.6.2 Higher-risk entities such as banks, money remitters and gatekeepers are vulnerable to exploitation for ML/TF purposes and can represent risk to your business. We recommend that you refer to the NRA and your relevant STR for further information. Other factors to consider when identifying aspects of your business that may be susceptible to ML/TF

4.6.3 The Act also sets out special steps you must take in relation to PEPs, wire transfers, correspondent banking and new technologies. This information should help you to identify high-risk areas of your business.

4.6.4 The NRA and STRs are useful sources of information when identifying how your business could be used for ML/TF. You should also consider emerging trends that are signaled by the FIU in their guidance when identifying risks in your business. Information on current ML/TF methods is available on the FATF website.

PART III

5.0 ASSESSING RISK

Risk can be defined in many ways, and there is no one-size-fits-all assessment model for this process. Once you have identified the ML/TF risk that you face during business, you must determine the level of that risk. When assessing risk, you should consider:

(a) each element of risk you have identified;
(b) your business experience in relation to that risk;
(c) information and guidance published by the AML/CFT regulator and the FIU;
(d) information and guidance published by international organizations such as the FATF, ESAAMLG and UNODC, and AML agencies from FAST Regional Styled Bodies.

You should allow for the different situations that currently arise in your business or are likely to arise in the near future. For instance, your risk assessment should consider the impact of new products, services or customer types, as well as new technology. In addition, ML/TF risks will often operate together and represent higher risks in combination.

Potential ways to assess risk include but are not limited to:

(a) how likely an event is;
(b) how likely an event is and the consequence of that event;
(c) vulnerability, threat and impact;
(d) the effect of uncertainty on an event.

Some examples are provided later in this section, but whichever method you use you will need to explain and demonstrate its adequacy and effectiveness to your AML/CFT regulator and ensure it is appropriate and proportionate to your needs.

Your assessment of risk should be informed, logical and clearly recorded. For instance, if you have identified gatekeepers as presenting higher inherent risk in relation to the delivery of your product, your risk assessment should indicate how you arrived at this rating (domestic guidance, case studies, direct experience).

5.2 RISK ASSESSMENT (LOWER COMPLEXITY)

5.2.1 In line with the previous AML/CFT regulator's guidance, you may want to assess risk by only considering the likelihood of ML/TF activity. This assessment should involve considering each risk factor you have identified, combined with your business experience and information published by regulators and international organizations such as the FATF. Your likelihood rating could correspond to:

Very unlikely	There is very little chance of ML/FT occurring in this area of your business
Possible	There is a small chance of ML/FT occurring in this area of your business
Likely	There is a moderate chance of ML/FT occurring in this area of your business.
Very likely	There is a high chance of ML/FT occurring in this area of your business

5.2.2 For example, you may have identified that one of your products is vulnerable to ML/TF due to the potential for cross-border movement of funds. Your risk assessment highlights the product is easily accessible, that many customers are using it, and it is used in higher-risk jurisdictions. Combined with domestic and international guidance, you assess that the inherent risk rating of this product as likely.

5.2.3 Your programme should then address this likely risk with appropriate control measures. You will need to do this with each of your identified risks.

5.3. RISK ASSESSMENT (MEDIUM COMPLEXITY)

5.3.1 Another way to determine the level of risk is to work out how likely the risk is going to happen and cross-reference that with the consequence of that risk (see the example of a risk matrix below).

5.3.2 Using likelihood ratings and consequence ratings can provide you with a more comprehensive understanding of your risk and a robust framework to help you arrive at a final risk rating. These ratings, in combination with structured professional opinion and experience, will assist you in applying the appropriate risk management measures as detailed in your programme.

5.3.3 For example, you may have identified that one of your products is vulnerable to ML/TF and you assess that the likelihood of this product being used in ML/TF activity is highly probable. You judge the impact of the identified risk happening in terms of financial loss and assess the consequence as moderate.

5.3.4 Cross-referencing highly probable with moderate in the risk matrix below results in a final inherent risk rating of medium-high. Your programme should then address this medium-high risk with appropriate control measures. You will need to undertake this exercise with each of your identified risks. The risk matrix below is provided as an illustrative example only.

LIKELIHOOD SCALE						
	5 Almost certain	11	16	20	23	25
	4 Highly probable	7	12	17	21	24
	3 Possible	4	8	13	18	22
	2 Unlikely	2	5	9	14	19
	1.Improbable	1	3	6	10	15
		1 Minimal	2 Minor	3 Moderate	4Significant	5 Severe
Risk rating	CONSEQUENCE SCALE					
	LOW	Medium		Medium High		High

High Risk assessment (higher complexity)

5.3.5 More complicated and comprehensive assessments of risk may suit larger businesses with multiple products or services.

5.3.6 You could assess risk likelihood in terms of threat and vulnerability. For example, you may consider domestic tax evasion criminals as the threat, and your accounts dealing with cash payments as the vulnerability. Depending on the risk assessment method you use, this could result in an inherent risk rating of highly probable. You may then want to assess the impact of this event on your business and the wider environment.

5.3.7 Determining the impact of ML/TF activity can be challenging but can also help you focus your AML/CFT resources in a more effective and targeted manner. When determining impact, you may want to consider a number of factors, including:

(a) nature and size of your business (domestic and international)
(b) economic impact and financial repercussions;
(c) potential financial and reputational consequences;
(d) terrorism-related impacts;
(e) wider criminal activity and social harm;
(f) political impact;
(g) negative media.

5.3.8 You may want to give more weight to certain factors to provide a more nuanced understanding of your ML/TF risk.

5.3.9 In addition, you may want to consider how your risks can compound across the various risk factors. For example, you may identify that one of your products is high-risk and is being used in a high-risk jurisdiction that is directly involved in the production or transnational-shipment of illicit drugs. As such, you assess the compounded risk of this scenario as presenting an inherent risk rating of severe. You would be expected to prioritise and allocate your resources accordingly.

Part IV

6.0 APPLYING A RISK ASSESSMENT

Your risk assessment should help you rank and prioritise your risks and provide a framework of how you will manage those risks.

Your risk assessment must enable you to prepare a comprehensive programme. It should enable you to meet your relevant obligations under the Act and regulations, including your obligations to conduct CDD, monitor accounts and activities and report suspicious activity.

Your risk assessment should help in determining suspicion and consequently assist in the decision to submit an STR to the FIU. You must submit an STR to the FIU if you think activities or transactions are suspicious. For instance, you may consider unexpected international activity of a domestic-based customer unusual, especially if it involves a high-risk jurisdiction, and submit an STR.

You must conduct ongoing CDD. Your risk assessment will help you target and prioritize the resources needed for ongoing CDD. For instance, you may want to undertake ongoing CDD on your high-risk customers on a more regular basis than on your lower-risk customers.

You must undertake account monitoring. Your risk assessment will help you design the triggers, red flags and scenarios that can form part of your account monitoring. For instance, you may want the activity of a high-risk customer in a high-risk jurisdiction (as identified in your risk assessment) to be subject to more frequent and in-depth scrutiny.

6.1 NEW AND DEVELOPING TECHNOLOGIES AND PRODUCTS

New and developing technologies and products can present unknown ML/TF risks and vulnerabilities. In addition, new methods of delivery may be able to bypass existing AML/CFT measures to allow anonymity and disguise beneficial ownership. Your risk assessment should consider whether your business is, or may be, exposed to customers involved in new and developing technologies and products. Your programme should detail the procedures, policies and controls that you will implement for this type of customer and technology.

6.2 MATERIAL CHANGES AND RISK ASSESSMENT

6.2.1 Your risk assessment should adapt when there is a material change in the nature and purpose of your business or your relationship with a customer. A material change could present an increase, or decrease, in ML/TF risk.

6.2.2 Material change could include circumstances where you introduce new products or services or have customers (or their beneficial owner) based in new jurisdictions. Material change can include when you start using new methods of delivering your services or you have new corporate or organizational structures. It could result from you deciding to outsource CDD functions or changing your processes for dealing with PEPs. In these circumstances, you may need to refresh your risk assessment.

PART V

7.0 REVIEW AND AUDIT OF RISK ASSESSMENT REVIEWING A RISK ASSESSMENT

You must review your risk assessment to:

- ensure it remains current at all times;
- identify any deficiencies in its effectiveness;
- make any changes that are identified as being necessary in this process.

You may want to schedule this annually as part of your annual report process and/or as a result of a trigger event. A trigger event could be the emergence of new technology; a new customer base; new services or products; new ML/TF risks as determined by the FATF, AML/CFT supervisors or the FIU; or updated regulations. Version control of documents is useful to demonstrate this.

7.1 AUDITING A RISK ASSESSMENT

7.1.1 You must audit your programme (as well as your risk assessment) every two years, or at any other time. You must provide a copy of your audit to your regulator or FIU.

7.1.2 The auditor must be appropriately qualified – The Act requires that your auditor must be appropriately qualified to conduct the audit. This does not necessarily mean that the person must be a chartered accountant or qualified to undertake financial audits. It does mean that the person has to have relevant skills or experience to conduct the assessment. You should be able to justify how your auditor is appropriately qualified.

7.1.3 The audit must be conducted by an independent person – The law requires that your auditor must be independent, and not involved in the development of your risk assessment or the establishment, implementation or maintenance of your programme. The person/s appointed to undertake the audit may be a member of your staff (for instance, an internal audit team), provided they are adequately separated from the AML/CFT area of your business. You should be able to justify how your auditor is independent.

7.1.4 You may choose to appoint an external firm to undertake both the audit and review provided you are satisfied there are appropriate separation and conflict of interest arrangements. The annual AML/CFT report that you are required to provide to your regulator must consider results and implications of the audit.

8.0 Effective date

These Guidelines shall become effective on 28 September, 2021.

Fatma A. Simba
Commissioner
Financial Intelligence Unit