GUYANA'S RISK-BASED APPROACH TO ANTI-MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM IN THE GAMING SECTOR

Published January 2022

GUYANA GAMING AUTHORITY
COMPLIANCE AND ENFORCEMENT DEPARTMENT
252 SOUTH ROAD, BOURDA, GEORGETOWN,DEMERARA, GUYANA, SOUTH AMERICA
225-4446/9

PREPARED BY: **TRACY SHAMSUDEEN**
REVIEWED BY: **LLOYD MOORE**
&
VICTOR HERBERT

Contents

1. GUYANA GAMING AUTHORITY

The Guyana Gaming Authority (GGA) is the supervisory body for casinos, betting shops and lotteries with regard to the Anti-money Laundering and Terrorist Financing legal framework applicable in Guyana. The GGA derives its authority from the ***Anti-money Laundering and Countering the Financing of Terrorism Act No. 13 of 2009 (AML/CFT Act Cap 10:11),*** its later amendments and Regulations.

Section 22 of the ***AML/CFT Act Cap 10:11*** sets out the role of the supervisory authority and a brief segment of the section states as follows:

Section 22(2)

'In accordance with this Act, the supervisory authority shall-:

(a) ***examine*** *and* ***supervise*** *the reporting entity, and* ***regulate*** *and* ***oversee effective compliance*** *with the obligations set out in sections 15, 16, 18, 19 and 20 and any other preventative measures in relation to combating money laundering and terrorist financing;*

(b) ***issue instructions, guidelines or recommendations*** *and* ***provide training to reporting entities*** *on their obligations and requirements under the Act and to make the reporting entities aware of any amendments to the laws relating to money laundering, terrorist financing or proceeds of crime; …'*

Regulations No. 4 of 2010 related to the AML/CFT Act Cap 10:11

Regulation 13

'A ***supervisory authority*** *shall* ***examine, supervise, regulate*** *and* ***issue Guidelines*** *to each reporting entity for compliance with the obligations set out in sections 15, 16, 18, 19 and 20 of the Act and the applicable provisions of these Regulations.'*

2. EXECUTIVE SUMMARY

This is a comprehensive document intended to be used as a guide for reporting entities to understand the importance and to adapt a methodology for conducting an internal risk-based approach to assessing risks related to *money laundering and the financing of terrorism* in the Gaming sector. The context of this document derives the source of its information from **forty plus nine of the *Financial Action Task Force (FATF) Recommendations but more specifically Recommendation one (1)*** and all guidance notes published by FATF relating to a Risk Based Approach to AML/CFT.

An overriding objective of the **Guyana Gaming Authority (GGA)** as the AML/CFT supervisory body for Casinos, Betting Shops and Lotteries, is to require that our reporting entities, in so far as our domestic legislation allows, abide by the FATF Recommendations (see legal requirement contained in ***Regulations No. 4 of 2010. Regulation 5(3)***). The contents of FATF recommendation one (1) and guidance related to recommendation one (1) are captured in Guyana's domestic legislation, in the ***Anti-money Laundering and Countering the Financing of Terrorism (AML/CFT) Act No. 13 of 2009***, its later amendments and applicable regulations.

In furtherance of the effort to combat money laundering and terrorist financing the GGA has published these guidance notes to ascertain that our reporting entities receive the requisite knowledge when conducting their '***Risk Based Assessment'*** for the products and services they offer. Additionally, these guidance notes will assist reporting entities in the gaming sector to strengthen and maintain their internal compliance program.

A general overview of these guidance notes is that it lays out the basic concepts for adapting a methodogy for a risk-based approach to conducting a risk assessment for developing a robust AML/CFT compliance program. Furthermore, these guidance notes highlight some of the impacts that money laundering and terrorist financing in the gaming sector could have on the local economy and society at large. Further, these notes give a brief history into the development of international cooperative measures to tackling money laundering and terrorist financing.

The section of the AML/CFT Act Cap 10:11 which states the requirement to assess risks of products and sercive is stated section ***19(e)*** of the ***AML/CFT Act Cap 10:11***. The GGA took the initiative to develop these guidance notes to assist our reporting entities operating in the gaming sector who have the obligation in law to conduct risk assessments for their products and services prior to introducing these products and services to the public.

3. RISK BASED APPROACH TO MONEY LAUNDERING AND TERRORIST FINANCING IN GUYANA'S GAMING SECTOR

3.1. Money laundering as a Crime

The infiltration of dirty money is a crucial problem for the economy in Guyana. The purchase of shares, of real estate, the establishment of illicit investment funds and the use of land-based gaming entities (reporting entities) for embedding of such resources is a danger to the credibility of the country as a whole, and in particular to the security of the financial and banking system. Understanding the adverse effects of money laundering in our economy will help institutions in taking effective steps to manage the problem.

Money launderers and terrorist financiers exploit both the complexity inherent in the gaming industry as well as the national AML/CFT regime. These launderers and financiers are especially attracted to entities with weak or ineffective controls where they can more easily play their funds into the system and receive winnings without detection.

3.2. What is the connection with society at large?

The social and political costs of money laundering, if left unchecked or dealt with ineffectively, are serious. Organised crime can infiltrate financial institutions, acquire control of large sectors of the economy through investment, or offer bribes to public officials and indeed governments.

The economic and political influence of criminal organisations can weaken the social fabric, collective ethical standards, and ultimately the democratic institutions of society. Most fundamentally, money laundering is inextricably linked to the underlying criminal activity that generated it. Laundering enables criminal activity to continue.

Gaming Entities are by definition designated non-financial business institutions. As part of their operation gaming entities offer gambling for entertainment, but also undertake various financial activities that are similar to financial institutions, which put them at risk of money laundering. Some gaming entities accept money deposits; give credits, conduct money exchange; money transfers; foreign currency exchange; debit card; cashing facilities, cheque cashing.

Gaming Entities (Reporting entities) are by nature a cash intensive business and the majority of transactions are cash based.

During a single visit to a casino, betting shop or lottery a customer may undertake one or many cash or electronic transactions, at either the *'buy in'* stage, during play, or at the *'cash out'* stage.

It is the variety, frequency and volume of transactions that makes the gaming sector particularly vulnerable to money laundering.

3.3. International efforts to combat Money Laundering

3.3.1. The Financial Action Task Force (FATF), established by the G-7 countries in 1989. FATF is an intergovernmental body, comprising 34 member jurisdictions and two regional organizations, and whose purpose is to develop and promote policies to combat money laundering and terrorist financing. FATF has set out 40+9 recommendations that outline the basic framework for anti-money laundering and terrorist financing efforts.

Regarding the Gaming industry, The Financial Action Task Force (FATF), issue two important reports

(2008) Risk Based approach guidance for Casinos

(2009) Vulnerabilities of Casinos and Gaming Sector

3.3.2. Egmonton Group: In 1995, a group of Financial Intelligence Units (FIUs) met at the Arenberg Palace in Brussels and decided to establish an informal group whose goal would be to facilitate international cooperation. Now known as the Egmont Group of Financial Intelligence Units, these FIUs meet regularly to find ways to cooperate, especially in the areas of information exchange, training and the sharing of expertise.

3.3.3. Money laundering definition.

Based on the International Compliance Association definition, "Money laundering is the generic term used to describe the process by which criminals disguise the original ownership and control of the proceeds of criminal conduct by making such proceeds appear to have derived from a legitimate source."

The definition of Money Laundering is contained in **section 3** of the ***AML/CFT Act No. 13 of 2009***.

There are three widely recognized stages in the money laundering process

Placement, the stage at which criminally derived funds are introduced in the financial system.

Layering, the substantive stage of the process in which the property is 'washed' and its ownership and source is disguised.

Integration, the final stage at which the 'laundered' property is re-introduced into the legitimate economy.

These three staged definitions of money laundering are highly simplistic. The reality is that the so-called stages often overlap and, in some cases, for example in cases of financial crimes, there is no requirement for the proceeds of crime to be 'placed'.

3.4. The need for Gaming Sector-specific risk assessments

Preventing Gambling from being a source of crime is the main goal of any **AML** prevention program. By using a Risk Based approach framework, it encompasses all the standards the **FATF** (The Financial Action Task Force) adopted, a set of guidance papers on the application of the RBA for different business sectors including the gaming industry.

3.4.1. What is risk?

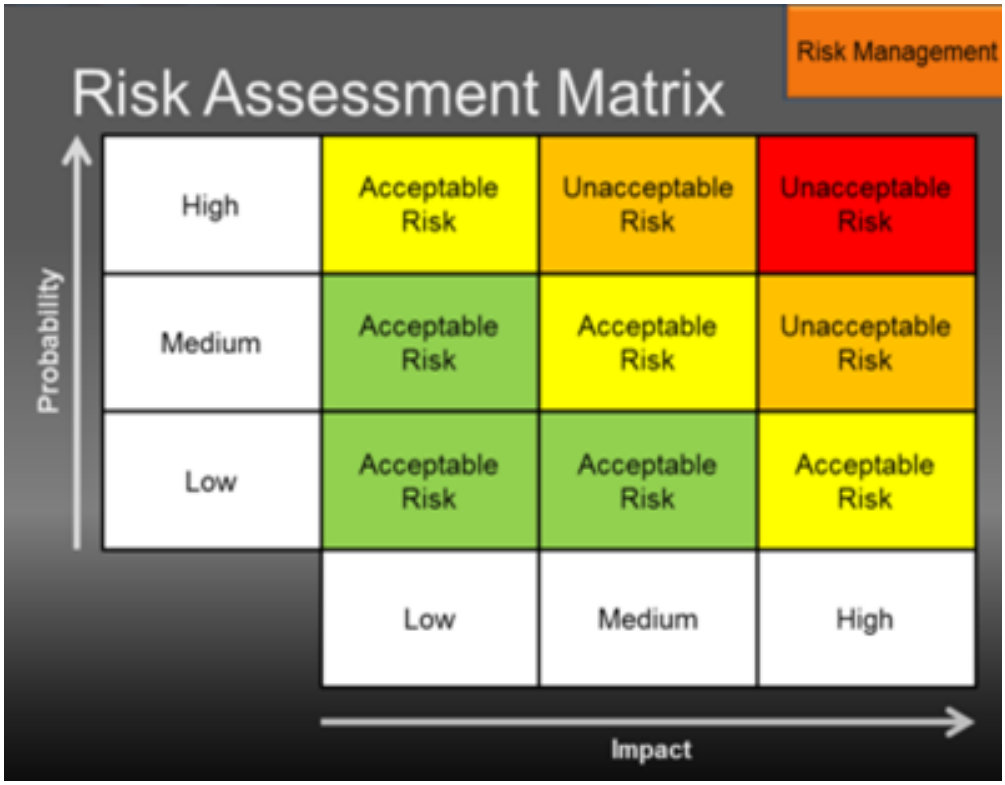
Risk can be defined as the likelihood of an event, the consequences derived from, and the degree of damage or loss that may result from such an occurrence. In the context of money laundering/terrorist financing (ML/TF), risk means:

Threats: this could be a person (or group), object that could cause harm. In the ML/TF context, a threat could be criminals, facilitators, their funds or even terrorist groups.

Vulnerabilities: elements of a business that could be exploited by the identified threat. In the ML/TF context, vulnerabilities could be weak controls within a reporting entity, offering high risk products or services, etc.

Probability = likelihood of occurrence

Impact: this refers to the seriousness of the damage that would occur if the ML/TF risk materializes (i.e., threats and vulnerabilities)



3.5. What is risk management?

It is the process that includes the recognition of ML/TF risks, the assessment of these risks, and the development of methods to manage and mitigate the risks that have been identified.

3.5.1. What are inherent and residual risks?

When assessing risk, it is important to distinguish between inherent risk and residual risk.

Inherent risk is the intrinsic risk of an event or circumstance that exists before the application of controls or mitigation measures.

On the other hand, **residual risk** is the level of risk that remains after the implementation of mitigation measures and controls regarding business, activities and clients.

3.6. What is a risk-based approach?

In the context of ML/TF, a risk-based approach is a process that encompasses the following:

A. **The risk assessment of gaming business activities** using certain prescribed elements;
Products, services and delivery channels;
Geography;
Clients and business relationships;
Other relevant factors.

B. **The mitigation of risks** through the implementation of controls and measures tailored to the identified risks;

C. **Keeping your *'know your customer'* (KYC) identification** and, if required, **beneficial ownership** and business relationship information up to date in accordance with the assessed level of risk;

D. **The ongoing monitoring of transactions in accordance with the assessed level of risk.**
Assessing and mitigating the risk of ML and TF is not a static exercise. The risks that have been identified may change or evolve over time as new products or new threats in the industry emerges. Consequently, the risk-based approach should be re-evaluated and updated when the risk factors change.

3.6.1. Benefits of a risk assessment approach

Providing effective reporting to executive management and identifying unmitigated risks that require immediate action. An effective risk-based approach will allow gaming entities to exercise reasonable business judgement with respect to customers.

With a risk-based framework the compliance costs can be reduced, and mitigate the economic, reputational, operational, legal and regulatory risks.

A risk-based approach focuses its efforts on high-risk variables and their impact, and mitigation responses. This is because regulatory compliance activities do not always entail effective risk management.

A risk-based approach allows a reporting entity to develop a tailored AML/CFT risk management strategy and programme that specifically reflects that reporting entity's operations, environment, customers, products, services and technology.

A risk-based approach is less prescriptive and more responsive to changes in risks, which is particularly important when managing the risks of money laundering and terrorism financing activities.

A risk-based approach relies on correctly identifying how the potential risk of money laundering and terrorist financing impacts the specific operations of the reporting entity.

3.6.2. Challenges to overcome in a risk-based approach

There are no universally accepted methodologies that prescribe the nature and extent of a risk-based approach. However, an effective risk-based approach does involve ***identifying and categorising money laundering and terrorist financing risks*** and ***establishing reasonable controls based on risks identified*.**

A properly applied risk-based approach does not necessarily mean a reduced burden, although it should result in a more cost-effective use of resources**.**

Risk Based Approach/ Potential Benefits and Challenges

Potential Benefits

- **Better management of risks**
- **Efficient use and allocation of resources**
- **Focus on real and identified threats**
- **Flexibility to adapt to risks that change over time**

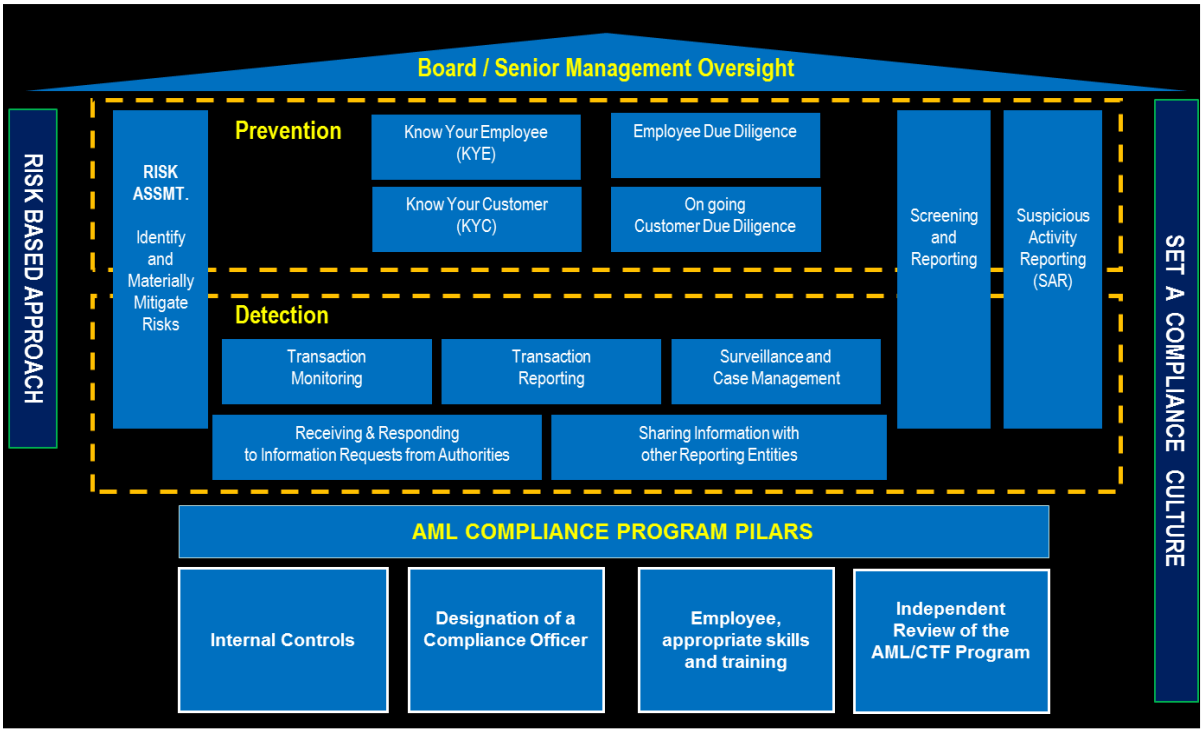
Potential Challenge is given

- **Identifying appropriate information to conduct a sound risk Based analysis**
- **Addressing short term transitional costs**
- **Greater need for more expert staff capable of making sound judgments**
- **Regulatory response to potential diversity of practice**

4. RISK BASED APPROACH FRAMEWORK AND STEPS

1. **Risk assessment: Identify and mitigate Risks**
2. **Develop a KYC (Know your customer) identification and record keeping policy**
3. **KYE (Know your employee) screening policy.**
4. **Ongoing monitoring of transactions and reporting**
5. **Internal controls**
6. **Compliance officer designation**
7. **Ongoing compliance training program (for employees or other individuals authorized to act on your behalf). The training program has to be written and maintained overtime**
8. **Independent audit review to evaluate AML Program**
9. **Develop a compliance culture with the tone at the top.**

Risk based approach framework



4.1. Risk assessment: Identify and mitigate Risks

Risk categories factors may be described as those which affect customer risk and are not intended to be prescriptive or comprehensive. They will not apply universally to all gaming entities, and even when these factors are present there may be different risk outcomes for different gaming entities and operators depending upon a host of other factors.

AML/CFT ACT CAP 10:11 Section 19 (1)(e)

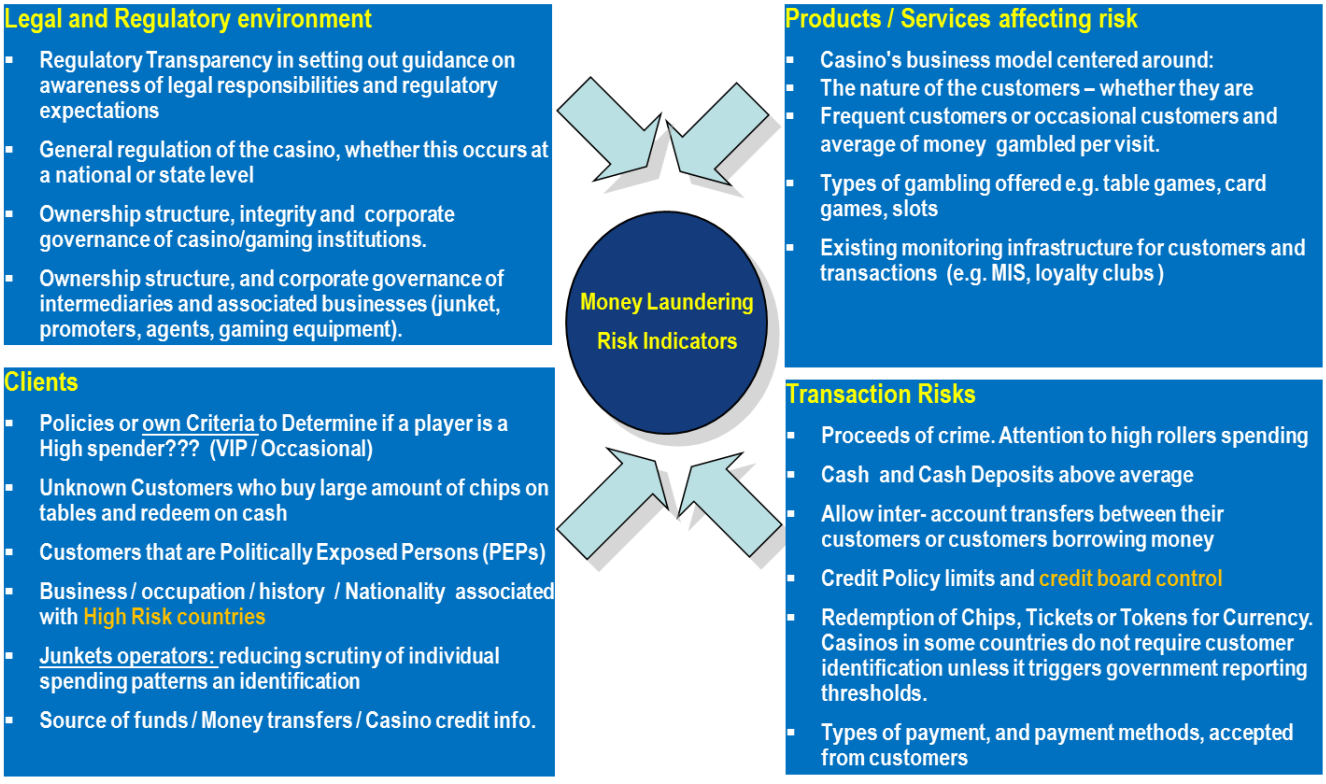
'A reporting entity shall-

(e) identify and assess the money laundering or terrorist financing risks and take appropriate measures to manage and mitigate those risks which may arise in relation to-

(i) the development of new products and new business practices including new delivery mechanisms; and

(ii) the use of new developing technologies for both new and pre-existing products, and ***this risk assessment shall take place prior to the launch of the new products, business practices or the use of new or developing technologies****.'*

RISK CATEGORIES Based on FATF recommendations



We remark the **legal / regulatory environment** where transparency rules and guidance provide certainty to business and authority for effective implementation to achieve the objectives of the compliance framework. It should be necessary to implement in ways that minimise compliance costs on industry to the extent feasible.

No matter what individual procedure is adopted, the guiding principle will be that there is an awareness of legal responsibilities of each gaming operator as directly responsible for complying with their legal obligations.

In the absence of this transparency the authority may be perceived as unpredictable which may undermine even the most effective application of the risk-based approach by the **gaming entity herein also referred to as a reporting entity.**

4.1.1. Risk tolerance

It is an important component of effective risk management. When considering threats, the concept of risk tolerance will allow you to determine the level of exposure (e.g. number of high-risk clients, inherently high-risk products, etc.) that you consider tolerable.

To do so, you may want to consider the following risk categories that could affect your business:

- Regulatory risk
- Reputational risk
- Legal risk
- Financial risk

4.1.2. Adverse risks of non-compliance:

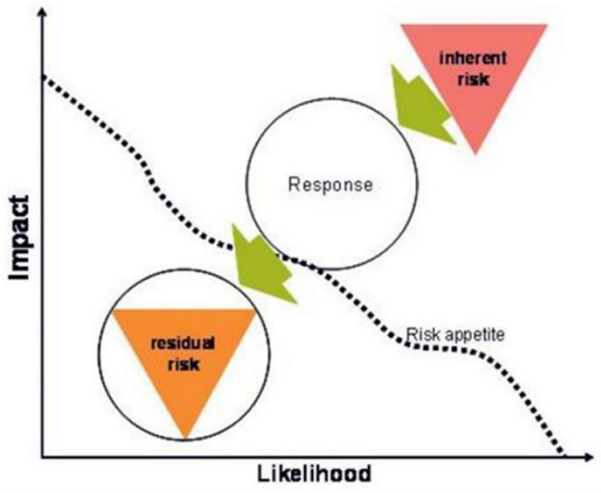
- Sanctions from relevant government agencies
- The impact on customers who do not want to play in gaming on the public radar
- Industry machine Vendors aware of the sanctions to the gaming entity will not sell anymore
- Suspension of business activities due to operational and financial impact of sanctions
- Loss of gaming license
- Bad reputation in the industry due to sanctions

Your **risk tolerance** will have a direct impact on the following step: creating risk-reduction measures and key controls, your policies and procedures, and training.

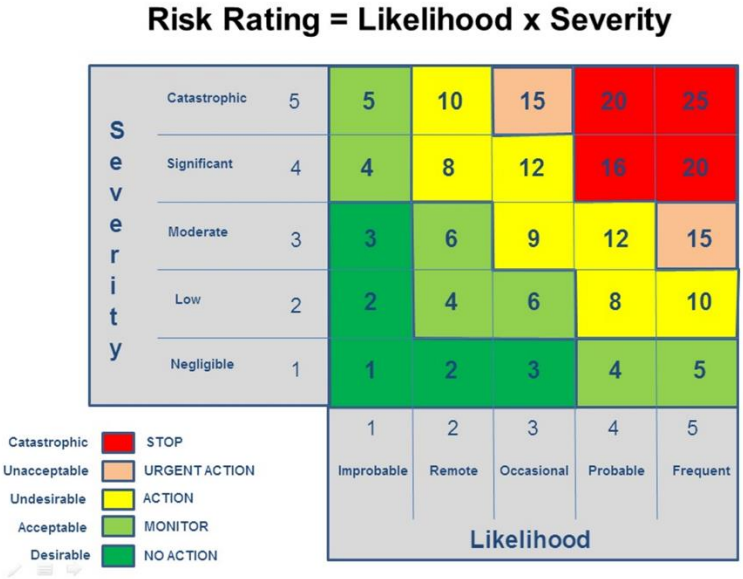
4.1.3. Inherent and Residual Risks

Inherent risk is the risk to an entity in the absence of any actions management might take to mitigate either the risk's likelihood or impact.

Residual risk is the risk remaining after management's response to the risk.



A risk map is a graphic representation of likelihood and impact of one or more risks. Risk maps may plot quantitative or qualitative estimates of risk likelihood and impact. Often, risk maps are referred to as "heat maps" since they present risk levels by color, where red represents high risk, yellow moderate risk, and green low risk



Identifying the inherent risks will require you to look at the vulnerabilities to ML/TF.

4.1.4. What Are the Four Risk Responses?

Avoidance is a response where you exit the activities that cause the risk. Some examples of avoidance are exiting product line, selling a division, or deciding against expansion.

Reduction is a response where action is taken to mitigate the risk likelihood and impact.

Sharing is a response that reduces the risk likelihood and impact by sharing a portion of the risk. An extremely common sharing response is insurance.

Acceptance is a response where no action is taken to affect the risk likelihood or impact.

4.2. Develop a KYC (Know your customer) identification and record keeping policy

4.2.1. Customer Due Diligence

"Gaming Entities also known as Reporting Entities should apply CDD to all customers when they engage in financial transactions in a casino, betting shop or lottery.

AML/CFT ACT CAP 10:11 Section 15 (2)

'Reporting Entities shall establish the identity and verify the identity of any customer of the reporting entity by requiring the applicant to produce an identification record or such other reliable, independent source documents as the Financial Intelligence Unit may request'

Regulations No. 4 of 2010 related to the AML/CFT Act Cap 10:11

Regulation 4
'Identification procedures in relation to new and continuing business relationships'

Examples of financial transactions include the purchase or cashing in of casino chips, tickets or tokens, the opening of accounts, wire transfers, and currency or value exchange.

This applies to either a single transaction, or to several transactions that appear to be linked.

The CDD procedures should include:

- Identify and verify the identity of each customer.
- Identify any beneficial owner (i.e., the natural person(s) who ultimately owns or controls a customer and/or the person on whose behalf a transaction is being conducted.
- Customers that are Politically Exposed Persons (PEPs).
- Obtain appropriate additional information to understand the customer's circumstances and business.

AML/CFT Act Cap 10:11 Section 16

The Section sets out the basic record keeping requirements for reporting entities to obtain when establishing a relationship with a customer.

Regulations No. 4 of 2010 related to the AML/CFT Act Cap 10:11

Regulation 6
'Where a reporting entity is required under these Regulations to verify the identity of a person, it shall establish and maintain a record which –

(a) Indicates the nature of the evidence obtained; and
(b) Comprises a copy of the evidence or, where this is not reasonably practicable, contains such information as would enable a copy of the evidence to be obtained.'

4.2.2. KYE (Know your employee) screening policy.

4.2.2.1. Employee screening

- New and existing staff Personal and/or Professional background
- will likely go further than just senior staff, and into anyone involved or with access to financial transactions and compliance information

4.2.2.2. Does your recruitment process already include this?

- speak to your HR team
- develop (or share) a management framework
- carefully consider privacy implications
- who has access to information?
- who needs access to information?
- Update your recruitment guidelines - for both new staff and changes of role

4.2.2.3. Red Flags regarding employee behavior changes

- Sudden and significant changes in their standard of living.
- Lifestyle and spending habits that aren't consistent with their salary, financial position or level of indebtedness.
- If employee refuses to take time off for no apparent reason.
- Employees who don't allow other colleagues to assist certain customers.
- If employee suspiciously receives gifts or gratuities on a regular basis.
- Employees who are reluctant to accept any promotions or changes in their activities.
- Employees who stay at the office after working hours or that go to the office at odd times for no reasonable explanation.

4.3. Ongoing monitoring of transactions and reporting

Monitoring customers and their gambling is essential to ensure effective application of AML/CFT policies, procedures, internal controls and automated systems. It always must be done in an ongoing basis.
There is a need for greater vigilance of patterns of transactions and play, unusual transactions and possible indicators of suspicious transactions.

Suspected money laundering in casinos, betting shops and lotteries is detected in two main ways:

- Through surveillance on-site
- Through financial intelligence with information systems in place

Regulations No. 4 of 2010 related to the AML/CFT Act Cap 10:11

Regulation 7
'Where a reporting entity is required under these Regulations to verify the identity of a person, it shall maintain a record of all transactions carried out by or on behalf of that person such as records sufficient to identify the source and recipient of payments from which investigating authorities will be able to compile an audit trail for suspected money laundering or terrorist financing.'

4.3.1. Transaction monitoring

A reporting entity must put in place a transaction monitoring program

AML/CFT ACT CAP 10:11 Section 18 (3)

*'A reporting entity shall monitor its business relationships and the transactions undertaken throughout the course of the relationship to ensure that its obligations under **section 15** are met that the transactions conducted are consistent with the information that the reporting entity has of its customer, of the customer's business and risk profile and source of funds, where necessary'*

The extent to which transactions should be monitored, is to be determined, on a risk basis, having regard to the customer's risk classification and the risk factors set out in the Rules

Management should periodically evaluate the appropriateness of **filtering criteria and thresholds**

- Managing Alerts
- Have policies & procedures in place for detecting unusual activity from customers.
- Establish a clear & defined escalation process from the point of initial detection to conclusion of the investigation.
- System alert framework is needed to avoid discretion from staff criteria

4.3.2. Managing Alerts

When multiple departments are responsible for researching unusual activities, lines of communication must remain open.

- Allows multiple departments to gain efficiencies by:
- Sharing information
- Reducing redundancies
- Ensuring all suspicious activity is identified, evaluated, & reported

The ***FATF Recommendations*** require gaming entities to keep records for five years. Such records must be sufficient to permit reconstruction of individual transactions (including the amounts and types of currency involved, if any) so as to provide, if necessary, evidence to criminal activity. Casinos and gaming entities are likely to keep sufficient records of transactions for other reasons, e.g., marketing and promotions.

With regard to Internet services offered by gaming entities, checks may be made on the location of the computer used when gaming accounts are opened, or during gambling, including IP checks. IP addresses provide information about the country where the computer being used is located.

Note that:

Regulations No. 4 of 2010 related to the AML/CFT Act Cap 10:11

Regulation 8(1)
'A reporting entity shall maintain the records required by regulation 6 and 7 for at least seven years from the date-

(a) when all activities relating to one-off transactions or a series of linked transactions were completed;
(b) when the business relationship was formally ended: - or
(c) where the business relationship was not formally ended when the last transaction was carried out.'

Regulation 9(1)
'A reporting entity shall ensure that any records required to be maintained under these Regulations are capable of retrieval in legible form without undue delay.'

4.3.3. Transaction reporting

Decision maker should have the authority to make the final **SAR** (Suspicious Activity Report) filing decision, based on:

- An established decision-making process
- The company has followed existing policies, procedures, & processes
- Document SAR decisions, including the specific reason for filing or not filing a SAR
- Thorough documentation provides record of SAR decision-making process, including final decisions not to file a SAR

Section 18 of the ***AML/CFT Act Cap 10:11*** sets out the criteria for reporting of suspicious business transactions as well as the FIU published guidelines which can be found on www.fiu.gov.gy .

Regulations No. 4 of 2010 related to the AML/CFT Act Cap 10:11

> ***Regulation 11***
> *'Establishment of procedure for recognising and reporting suspicious transactions.'*
>
> The regulation goes on to state the reason and the process whereby a reporting entity shall document and conduct its internal reporting procedures.

4.4. Internal controls

Internal controls should mitigate the inherent risk of any high-risk account, customer, product, or service as well as transactions to or from a high-risk country that could be misused for money laundering or terrorist financing.

AML/CFT ACT CAP 10:11 Section 16 (6)

> *'Where there are higher risk categories of customers, reporting entities shall conduct enhanced customer due diligence measures, consistent with the risks identified and shall increase the degree and nature of monitoring of the customer or business relationship in order to determine whether those transactions or activities appear unusual or suspicious.'*

Gaming Entity's internal controls should be commensurate with:

- Complexity, organisation, and relative size of the business;
- Risks posed by the types of gambling and financial services offered as well as the volume of business;
- Risks posed by the types of customers and their geographical location

Internal controls should cover all related activities and programs such as:

- Suspicious activity reporting regarding the threshold set by the supervisory or regulatory authority (in Guyana the Financial Intelligence Unit)
- Currency transaction reporting (where required),
- Customer and patron identification
- Policies and procedures in place when dealing with high-risk situations (e.g. for politically exposed persons (PEP).
- Policies about proper staff training
- Establishment of a compliance department
- Recordkeeping, and compliance
- Account opening and documentation procedures,
- Management information systems adequate to detect and report suspicious activity in a timely manner

4.5. Compliance officer designation

A reporting entity (gaming entity) must designate an 'AML/CFT Compliance Officer' at management level according to AML/CFT Act Cap 10:11 and its Regulations. The position ensures the Board of Directors, management and employees are in compliance with the rules and regulations of regulatory agencies, that company policies and procedures are being followed, and that behavior in the organization meets the company's Standards of Conduct.

AML/CFT Act Cap 10:11 Section 19

The Section alludes to the requirement to appoint a compliance officer and the responsibility of the compliance officer.

Section 19(1)(a)
'A reporting entity shall-

(a) Appoint a compliance officer who shall be responsible for ensuring the reporting entity's compliance with the requirements of the Act; …'

Regulations No. 4 of 2010 related to the AML/CFT Act Cap 10:11

Regulation 14(1)
'A reporting entity shall appoint a Compliance Officer at the management level with appropriate and adequate authority and responsibility to implement these Regulations.'

Regulation 14(2)
'The Compliance Officer shall-

(a) be a senior officer with relevant qualifications and experience to enable him to respond sufficiently well to enquiries relating to the reporting entity and the conduct of its business; …'

4.5.1. Compliance officer main duties

- Develop and implement control policies and an AML program to prevent illegal, unethical or improper conduct.
- Cooperation with other departments (e.g., finance, Internal Audit, human resources, etc.) to evaluate effectiveness of compliance policies and procedures in place.
- Act as the liaison personnel between the Guyana Gaming Authority and the company.

- Company problems resulting from non-compliance activities can include misunderstandings of policy or current legislation, technical reporting issues or non-adequate staff training. In this instance, Compliance Officers require abilities in dealing with others in situations of non-compliance in order to correct non-compliant conducts or rules.

- Acts as an independent review to ensure that compliance Issues/concerns within the organization are being appropriately evaluated, investigated and resolved.

- Reports on a regular basis, and as directed or requested, to keep the supervisory authority (in this case the Financial Intelligence Unit/ Guyana Gaming Authority) and the Board of directors informed of the compliance efforts.

- Manage the compliance chain of reporting for employees and customers.

4.6. Ongoing compliance staff training program

4.6.1. Training staff objetives

- their obligations under the AML/CTF Act Cap 10:11, Regulations and Guidelines
- the consequences of non-compliance
- the nature and consequences of ML/TF risk they may reasonably face
- the processes and procedures in the AML/CFT program that are relevant to their role.
- Suggested compliance course content
- Trends in the prevention of money laundering
- Guyana's domestic legal framework and regulations
- Client Identification Program
- Know Your Customer Program
- Customer's Risk Profile
- Decentralized Monitoring of Transactions
- Unusual/Suspicious Transactions Report
- Money laundering and Terrorist Financing Methodologies

AML/CFT Act Cap 10:11

Section 19(1)

'A reporting entity shall-

(b) establish and maintain internal policies, procedures, controls and systems to-…

(v) make its officers and employees aware of the law relating to combating money laundering and terrorist financing;

(vi) make its officers and employees aware of the procedures and policies adopted by it to deter money laundering and terrorist financing; and…

(d) train on an on-going basis its officers, employees and agents to…'

Regulations No. 4 of 2010 related to the AML/CFT Act Cap 10:11

Regulation 16(1)
'A reporting entity shall provide education and training for all directors or, as the case may be, partners, all other persons involved in its management and all key staff to ensure that they are aware of - …'

Regulation 16(2)
'A reporting entity shall, in addition, provide training in accordance with the requirements of this regulation to all new key staff as soon as practicable after their appointment.'

Regulation 17
'A reporting entity shall also provide education and training appropriate to particular categories of staff in-

(a) its policies and procedures to prevent money laundering or terrorist financing;
(b) its customer identification, record keeping and other procedures; and
(c) the recognition and handling of suspicious transactions.

Regulation 18
'A reporting entity shall, at least once in every year, make arrangements for refresher training to remind key staff of their responsibilities and to make them aware of any changes in the laws relating to money laundering or terrorist financing and the internal procedures of the reporting entity.'

4.7. Independent audit review to evaluate AML Program

A gaming entity (reporting entity) must ensure that its AML/CFT Program, including each of its components, is subject to regular independent review.
This review of of an AML/CFT program must be carried out on a regular basis by an internal or external party determined by the reporting entity (for example, an internal or external auditor). It should be conducted in accordance with good review and audit practices. The review should be carried out by a competent individual who is free from bias and conflict of interest.

AML/CFT Act Cap 10:11 Section 19(1)

'A reporting entity shall-

(c) establish and maintain an independent Audit function with adequate resources to test, including sample testing its anti-money laundering and combating of terrorist financing procedures and systems; and …'

The purpose of the review should be to:

- Test the effectiveness of the AML/CFT Program having regard to the AML/CFT risks faced by the reporting entity
- Ensure that the AML/CTF Program complies with these Rules
- Ensure that the AML/CTF Program has been effectively implemented
- Ensure that the reporting entity has complied with its AML/CFT Program
- Continuous improvement in control, procedures and processes
- The extent and effectiveness of the staff AML/CFT awareness training
- The completion of appointments of staff to AML/CFT roles
- The performance of staff in AML/CFT activities
- The completion of AML/CFT compliance reporting

The recommendations include, but are not limited to:

- Corrective actions to address compliance failures
- Changes to improve the AML/CFT program
- Changes to both compliance and operational processes to improve the management of:
    - ML/TF business risks
    - ML/TF regulatory risks

4.8. Develop a compliance culture with the tone at the top.

The 'culture' of a business comprises the experiences, attitudes, beliefs and values of the organisation. These control the way people interact with each other and with stakeholders outside the organisation such as customers, suppliers and regulators.

Organisations that are successful in embedding a compliance culture often follow a similar process. A useful first step is to learn the extent of the compliance culture and indicate some of the things that may need doing is to complete a compliance risk-based assessment.

"A strong ethical culture, including clear expectations for acceptable conduct within the organization and with third parties, is essential for good governance.

Ethical behavior, however, involves much more than a code of ethics. The audit committee plays a critical role in ensuring that an organization's culture aligns with its code of conduct, that behaviors are consistent from top to bottom, and that corporate values resonate throughout the organization. But getting a true understanding of an organization's ethical culture can be difficult when the people in the audit function rely on most information about the organization from senior management and these are the people who, ultimately, must be held most accountable."