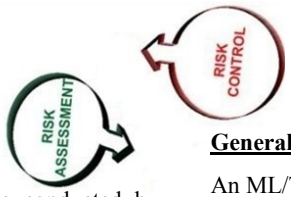
ST. KITTS BRANCH
Financial SERVICES
Regulatory Commission

NewsLetter

October 2018
Issue No. 54

Enterprise Risk Assessment: *What Are Your Risks and How Can You Address Them?*

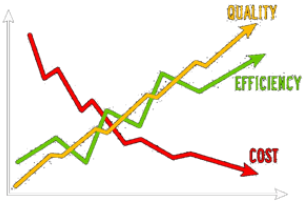


Introduction

There are several types of risk assessments that should be conducted by Regulated Entities. These include:

- Enterprise Risk Assessment – to assess the overall risk of the business;
- Products/Services Risk Assessment – to assess the risks associated with services/products offered; and
- Customer Risk Assessment – to identify the risk associated with a customer.

This month's newsletter will focus on Enterprise Risk Assessment. The purpose of conducting an enterprise-wide risk assessment is to assess the size and magnitude of risks, both individually and collectively, in order to focus management's attention on the most vital threats and opportunities. The assessment process allows management to measure and prioritize risks to ensure that they are appropriately managed within the entity's tolerance thresholds.



The Benefits

A well-developed risk assessment process can:

- Assist in managing and understanding the entity's risk exposure;
- Establish an organization's risk appetite;
- Assist management in making informed risk-based decisions;
- Identify weaknesses in an organization's internal controls; and
- Assist management to efficiently allocate resources and understand risk/ benefit trade-offs.

Conducting A Risk Assessment

There are no specific rules to conduct an enterprise-wide risk assessment; it is basically a matter of judgment. The Board of Directors/Senior Management should decide the appropriate method or format, based on the organization's particular risk profile. The format used for the risk assessment should be relevant and easily understood by all appropriate parties. The risk assessment should provide a comprehensive analysis of the money laundering and terrorist financing (ML/TF) risks in a concise and organized model. It is important to be self-critical during this exercise. Your risk assessment should list the steps taken to mitigate the ML/TF risks and clearly reference your policies, controls and procedures.

General Principles

An ML/TF risk assessment should meet the following minimum requirements:

- Identify and assess the ML/TF risks that may be associated with the entity's unique combination of products and services, customers, geographic locations, delivery channels and other factors.
- Analyze all necessary data to assess risks identified (e.g. transactions, media articles, sanction lists, etc).
- Evaluate the entity's AML/CFT compliance program.
- Establish the residual risk for the risk categories identified.
- Use appropriate weights and scoring (whether numerically or categorically).
- Commensurate with the nature and size of the business.
- Be documented and available to relevant persons.
- Be subjected to internal review and approval by the Board and Management.
- Be enumerated in a policy document.
- Keep up-to-date with local legislation and international standards.

Definitions

Inherent Risk— the risk that exists before controls are applied.

Residual Risk—is the risk that remains after controls are applied to the inherent risk.

Topics Discussed:

Identifying Internal Controls

When conducting a risk assessment, you must evaluate the existing internal controls you have in place to mitigate risk. Are these controls effective? Are there any weaknesses? These controls include:

- Policies and Procedures;
- Customer Screening;
- Employee Screening;
- Monitoring Systems/Software;
- Compliance Reviews by the Compliance Officer/Department; and
- Independent/Internal Audit.

Risk Categories

When conducting a risk assessment, the risk categories unique to the business operations must be assessed to achieve the most accurate risk rating. Types of risks include:

- Credit;
- Market;
- Operational;
- Strategic;
- Reputational;
- Concentration;
- Geographical;
- Money Laundering/Terrorist Financing; and
- Product.

Involvement of the Board of Directors

All Board members should understand the nature of threats and vulnerabilities the business faces. The Board should ensure that the business adopts a risk based approach to managing ML/TF risks. The responsibilities of the Board in relation to ML/TF risk assessment include:

1. Approve and oversee the development of a documented framework to conduct ML/TF risk assessment.
2. Review outcome of the risk assessment process.
3. Understand the ML/TF risk profile of the entity.
4. Allocate adequate resources to undertake the process.
5. Approve strategic decisions proposed by management after the assessment.
6. Ensure all relevant departments/functions are involved in the process.

How often Should a Risk Assessment be Conducted

Risk assessment is not a one time activity! Risk assessments should be conducted on a regular basis to reflect a business current risk profile. How often should you reassess?

- Annually;
- When a new product or service is introduced;
- When there is a change in the product or services offered;
- When there is an increase in market share.

Developing a Risk Response

Risk response is the process of developing strategic actions to take advantage of opportunities and reduce threats to the business. For each risk assessment conducted, a risk response should follow. This includes developing a formal action plan and risk measures to deal with risks falling outside the acceptable tolerance levels. The table below summarizes risk strategies.

For Threats	For Opportunities
Avoid. Risk can be avoided by removing the cause of the risk or executing the business activity in a different way while still aiming to achieve the objectives.	***Exploit***. The aim is to ensure that the opportunity is realized. Exploit is an aggressive response strategy, best reserved for those "golden opportunities" having high probability and impacts.
Transfer. Transferring risk involves finding another party who is willing to take responsibility and who will bear the liability of the risk should it occur.	***Share***. Allocate risk ownership of an opportunity to another party who is best able to maximize its probability of occurrence and increase the potential benefits if it does occur.
Mitigate. Risk mitigation reduces the probability and/or impact of an adverse risk event to an acceptable threshold. Taking early action to reduce the probability and/or impact of a risk is often more effective than trying to repair the damage after the risk has occurred.	***Enhance***. This response aims to modify the "size" of the positive risk. The opportunity is enhanced by increasing its probability and/or impact, thereby maximizing benefits realized for the project.
Acceptance. This strategy is adopted when it is not possible or practical to respond to the risk by the other strategies, or a response is not warranted by the importance of the risk.	

Legal Requirements

The Financial Action Task Force (FATF) requires countries to ensure that financial institutions and designated non-financial businesses and professions (DNFBPs) identify, assess and take effective action to mitigate their ML/TF risks. As such, risk assessment provisions were outlined in Anti-Money Laundering Regulations, No. 46 of 2011, Anti-Terrorism (Prevention of Terrorist Financing) Regulations, No. 47 of 2011 and Financial Services (Implementation of Industry Standards) Regulations, No. 51 of 2011.

Regulated Entities should note that you are required to conduct risk assessments in accordance with international standards and regulations. Regulated Entities will soon be required to submit business risk assessments on an annual basis to the FSRC. Kindly contact our office for any questions or assistance in conducting an Enterprise Risk Assessment.

Reference:

- *The FATF Recommendation*
- *Financial Services (Implementation of Industry Standards) Regulations, No. 51 of 2011*
- *Anti-Money Laundering Regulations, No. 46 of 2011*
- *Anti-Terrorism Regulations, No. 47 of 2011*
- *The FSRC Risk Based Supervisory Framework*

South Independence Square Street, P.O.Box 898, Basseterre, St. Kitts
Tel: (869) 466-5048 | 467-1019/1591 Fax: (869) 466-5317
Website: www.fsrc.kn | Email: info@fsrc.kn