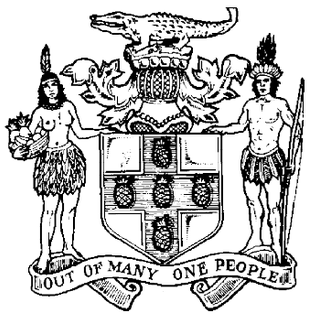

THE

JAMAICA GAZETTE

EXTRAORDINARY

1152D[1]

Vol. CXLV **MONDAY, AUGUST 15, 2022** **No. 265B**

The following Notification is, by command of His Excellency the Governor-General, published for general information.

CLAUDINE HEAVEN, JP (MRS.)
Governor-General's Secretary and
Clerk to the Privy Council.

GOVERNMENT NOTICE

MISCELLANEOUS

RCTS-GUI2022/06-0012

GUIDELINES:

RISK ASSESSMENT FOR SERVICE PROVIDERS

LEGISLATIVE REFERENCES : The Trust and Corporate Services Providers Act, 2017
Section 6(4)(d)

The Trust and Corporate Services Providers (Licensing and Operations) Regulations, 2022 — Regulation 5

1. PURPOSE

1.01 These guidelines are issued under section 46 of the Trust and Corporate Services Providers Act, 2017 (the "TCSP Act"). Licensees under the TCSP Act should have regard to section 46(5) of the TCSP Act which provides that:

> "*A person who fails to comply with any guidelines issued pursuant to this section, commits an offence and is liable to summary conviction in a Parish Court to a fine not exceeding one hundred thousand dollars or to imprisonment for a term not exceeding one month*."

1.02 These guidelines outline what is expected of trust and corporate services providers and their staff concerning their conduct of risk assessments in the particular circumstances of their businesses as a service provider, and its products, services, transactions, and customers. There may be general obligations on service providers to maintain appropriate records and systems of control more widely concerning their businesses. These guidelines are not intended to replace or interpret these wider obligations, if any.

1.03 Pursuant to paragraph 4 of the Second Schedule of the TCSP Act, licensees are to carry on their activities in a manner that will not tend to bring Jamaica's reputation into disrepute. In order to fulfil that obligation, paragraphs 2(3) and 4(2) of the Second Schedule to the TCSP Act require licensees to maintain adequate systems to assess the risks of their businesses and to develop and maintain policies and procedures pertaining to their statutory obligations regarding those business activities.

2. BACKGROUND

2.01 Assessing business risk is useful in helping a service provider understand the risks of its business and how those risks may change in response to the mitigating actions taken by the service provider over time.

2.02 The Financial Services Commission (the "FSC") therefore considers it prudent to provide guidance to applicants and persons who will be licensed under the TCSP Act regarding the risk assessment they are required to undertake.

3. LEGAL OBLIGATION

3.01 A core element of the prudent management of a licensee's business is an effective risk assessment that clearly demonstrates the corporate and/or trust service provider's (hereinafter referred to as service provider) understanding of the risks and vulnerabilities it may face during the course of conducting business.

3.02 A licensee under the TCSP Act is required to comply with applicable guidelines published by the FSC and other information provided in relation to this Act and associated regulations.

3.03 Service providers have several obligations concerning the ongoing assessment of their business risk. The obligations include:

(i) identifying all of the risks reasonably expected during the operation of the business;

(ii) documenting the risk assessment completed, determining the level of risk involved in relation to pertinent obligations under the TCSP Act, and keeping the risk assessment current by updating it on an on-going basis to take account of any identified deficiencies and other necessary changes; and

(iii) submitting an annual compliance report to the FSC as specified.

3.04 A service provider is expected to develop adequate and effective risk assessment methods that best suit its business taking into account its size, nature, and complexity. Senior management of a service provider consequently has a responsibility to ensure that the licensee's policies, controls, and procedures are appropriately designed and implemented, and are effectively operated to manage the risks of the business.

4. RISK MANAGEMENT POLICIES

4.01 The policy and procedures of a service provider should incorporate a statement of the service provider's policies regarding its key risk exposures, and the controls and procedures to implement the policy should set out how the service provider's senior management intends to discharge its responsibility for the management of those risks. This will provide a framework of direction for the service provider and its staff and should identify individuals and functions responsible for implementation.

4.02 The policy statement should be tailored to the circumstances of the service provider and include, but not be limited to, such matters as:

(i) *Guiding principles*

- an unequivocal statement of the values and culture that will be adopted and promulgated throughout the business towards the management of risk;

- a commitment to ensuring that staff are trained and made aware of the law and their obligations under it, and for establishing procedures to implement these requirements;
- recognition of the importance of internal and prompt reporting by the staff to senior management and the FSC;

(ii) *Risk mitigation approach*

- a summary of the service provider's approach to mitigating and managing effectively identified key risks;
- a summary of the service provider's controls and procedures for carrying out appropriate monitoring using a risk-based approach;
- a summary of the appropriate monitoring arrangements in place to ensure that policies and procedures are being carried out;
- allocation of responsibilities to specific persons and function.

4.03 It is important that a service provider's policies, procedures, and controls are communicated widely throughout the business to increase the effectiveness of their implementation.

5. STEP 1: IDENTIFYING PERTINENT RISKS

The following steps provide a general guide regarding the process entailed in conducting a risk assessment.

5.01 A service provider must understand all the ways that its business can be exposed to risks and develop and implement systems to deal with those risks. A risk assessment is pertained to how such risks are identified. Consequently, the identification of the inherent risks to which the business operation is vulnerable is an important element in conducting a risk assessment. Inherent risks are risks that are intrinsic to the services and products that are offered, and activities undertaken concerning those services and products and arise from uncertainty about and exposure to external threats.

5.02 Consideration must be given to all relevant factors, which include but are not limited to the following when identifying the vulnerability of a service provider's business:

- the nature, size, and complexity of the business;
- types of customers and transactions;
- products/services offered;
- IT infrastructure of the business.

5.02.1 *Nature, size, and complexity of the business*

(i) The size and complexity of a service provider's business play a key role in how attractive the business is for persons to use it for criminal purposes. The larger a business becomes the more likely it is for it to have customers that are not personally known by the service provider.

(ii) Business relationships with complex ownership or group structures, or with less transparency concerning beneficial ownership may pose different levels of risks than those with simpler legal/ownership structures or with greater transparency. Similarly, when a service provider conducts complex transactions, particularly across different countries, this could expose the business to greater risk in comparison to a business that is conducted entirely locally.

(iii) A service provider, therefore, needs to assess which parts of its business operations are vulnerable to risks and use all internal data it has such as the services/products that have been provided to customers, who those customers are, and where they are located to undertake the risk assessment.

5.02.2 *The* types *of customers and transactions*

(i) Some categories of customers pose a higher risk than others. The full range of circumstances associated with customers should be addressed when conducting a risk assessment of the business.

(ii) Consideration should be given to all relevant factors, such as whether client funds are being administered and the business model adopted.

5.02.3 *Products and services provided*

Many factors can contribute to the risk exposure of a corporate or trust service provider and it is the responsibility of a service provider to identify those factors associated with the services/products that are being offered. Consideration should be given to the conceptual, legal, operational, technological, and other complexities of a product or service, as those with greater complexity or dependencies on interactions between multiple systems and/or market participants may expose a service provider to different types and levels of risk than others with lower complexity or fewer dependencies on multiple systems and/or market participants.

5.02.4 *IT infrastructure of the business*

Consideration should be given by a service provider to how well its technical infrastructure, including data management and management information reporting capabilities, is suited to its risk-mitigation requirements.

6. STEP 2: ASSESSING RISK

6.01 Having identified all the risks faced by the business, a service provider must now assess each risk and determine the level of the risk, making allowance for different situations that currently arise in the business or are likely to arise soon. The assessment must be done without considering the extent to which the risks identified are mitigated by the business' risk management programme.

6.02 Assessing the level of inherent risk is based on judgement taking into account all relevant factors such as the impact of new services/products, types of customers, technology used, and the likelihood and consequence of a risk event occurring, and whether or not the risk has been compounded across multiple factors. While determining the impact of certain risk events may prove challenging a service provider could, among other things, consider the following factors:

- nature and size of the business (domestic and international);
- economic impact and financial outcomes;
- potential financial and reputational consequences;
- political impact;
- negative press.

6.03 It should also be noted that there are different ways to assess risk. Whichever method is used, the service provider must be able to explain and demonstrate its adequacy and effectiveness and ensure the method is proportionate and appropriate to the needs of the business. Regardless of the methodologies adopted, the risk assessment processes, the methodologies, and the related rationale are to be well-documented, approved by senior management, and communicated at the appropriate levels of the organization.

6.04 Inherent risks of the business are to be classified as low, moderate, above average, or high in keeping with the risk-based approach adopted by the FSC. Likewise, a service provider must be able to show how they arrived at the rating assigned to each risk identified (direct experience, domestic guidance, international guidance, case studies, etc.).

6.05 A service provider should also have regard to the implication of emerging and new technology as well as any material changes for the risk assessment that is conducted.

7. STEP 3: APPLICATION OF RISK ASSESSMENT

7.01 Senior managers must put in place appropriate controls, policies, and procedures to reflect the degree of risk associated with the business. The completed risk assessment must be used to prepare a comprehensive programme that will assist compliance with relevant statutory obligations. It should also be used to direct and prioritize resources such that greater focus is given to areas identified with greater risk.

7.02 The risk assessment will assist in planning and establishing the scenarios, red flags, and triggers that can form a part of its monitoring arrangements. Regard should be had to situations that by their nature, can result in an increased level of risk exposure and enhanced measures implemented to address them. Essentially then, the risk assessment should underpin the nature of the measures taken to manage the risk exposures of the business.

8. STEP 4: REVIEW AND AUDIT

8.01 A service provider must review the completed risk assessment at least annually to ensure it remains current at all times, identify any deficiencies, and make any necessary changes that are identified in the review process. The review may however be done more frequently as a result of the occurrence of a specified trigger event. A trigger event could be, for example, new services the business is authorized by the FSC to provide or the use of new technology.

8.02 Regular assessments of the risk monitoring and management systems (and internal controls) must be done to make sure they are working. A service provider is expected to demonstrate that a review was periodically done.

8.03 The completed risk assessments must be independently audited at least every two years, or at such time as requested by the FSC. A copy of the auditor's report is to be submitted to the FSC within 14 days of it being received by the board, general partners or other senior management as the case requires.

8.04 The annual report that a service provider is required to submit to the FSC must take account of the findings and implications of the independent audit. The annual report must also provide information on how the findings will be satisfactorily addressed.

Questions regarding these guidelines may be directed to the:

Registration, Corporate & Trust Services Division
The Financial Services Commission
39-43 Barbados Avenue
Kingston 5

Telephone: (876) 906-3010, (876) 818-0647

Facsimile (876) 906-3018

E-mail: Registration@)fscjamaica.org