GIBRALTAR FINANCIAL SERVICES COMMISSION

DLT Provider Guidance Notes

Risk Management

Introduction

The purpose of this guidance note is to provide a DLT Provider, as defined in the Financial Services (Distributed Ledger Technology Providers) Regulations 2020 (the DLT Regulations), with guidance as to the operational, technical and organisational standards expected and in some circumstances required by the GFSC.

This guidance note is specifically in respect of regulatory principle 4 of the DLT Regulations (the Regulatory Principle).

The Regulatory Principle states that "***A DLT Provider must manage and control its business effectively, and conduct its business with due skill, care and diligence; including having proper regard to risks to its business and customers".***

This document should be read as an interpretative guidance for a DLT Provider and the examples contained in this document should be noted as indicative of good practice by a DLT Provider in connection with the Regulatory Principle.

A DLT Provider should note that the GFSC will take this document into account when reviewing a DLT Provider's practices. The operational standards expected and required by the GFSC of a DLT Provider will vary depending on the size, particular nature, scale or complexity of the DLT Provider's business.

Overall Responsibility for Risk Management

A DLT Provider will be expected to apply good, forward-looking risk management practices. This will help provide assurance to all stakeholders that the core processes and systems are effectively controlled, are fit for purpose and that risks are being managed in the right way.

A DLT Provider's board will ultimately be responsible for ensuring the effectiveness of the risk management framework, setting the risk appetite and overall risk tolerance limits as well as approving the main risk management strategies and policies.

There will be an expectation that, as far as possible, the risk management activities are integrated into the day-to-day business processes and form part of the overall culture of the firm.

A DLT Provider will be expected to consider risks to its customers and the reputation of Gibraltar in addition to risks to its own business.

Risk Management Framework

A DLT Provider will be expected to develop risk management strategies into a cohesive enterprise-wide risk management framework with appropriate processes, procedures and policies. This should set out the methods that will be applied for the identification, assessment and management of risks, establish governance arrangements, assurance mechanisms and set the standard and expectations for risk management across the organisation.

A DLT Provider's risk management framework will need to define clear accountability for risk management, aligning risk management to performance management as well as the organisation's wider business strategy and objectives.

Adoption of an effective risk management framework will enable a DLT Provider and its management to meet its objectives as evidenced through the following outcomes:

- the board and senior management (together with other key stakeholders) will have assurance that the core processes and systems are effectively controlled, are fit for purpose and that risk is being managed in the right way;
- it will help the board and senior management to think strategically about how to manage the effects on the firm and its clients of volatility and uncertainty, helping the firm meet its strategic objectives and identify good business opportunities;
- management and staff will be better equipped to make risk based decisions and take action on risks and controls in a timely manner, supporting operational efficiency and effectiveness;
- continuous evaluation of a firms external and internal environment and evolving risk profiles will enable the DLT Provider to become more forward-looking and proactive, reducing the likelihood of significant risks emerging that have not already been identified; and
- it will help embed ownership and accountability for managing risk.

There are many known risk management frameworks and standards. It is the responsibility of each DLT Provider to adopt or develop a framework that reflects its activities and specific needs and that takes into account its size, risk and complexity. Although not an exhaustive list, a DLT Provider's risk management framework should include the following key areas.

Risk Identification and Assessment

A key aspect of a DLT Provider's risk management framework should be its risk assessment methodology. This should be designed to ensure a consistent approach to the identification and assessment of every kind of risk to which it is exposed.

A DLT Provider is expected to continuously assess and evaluate risks. It should take into account the changing external environment in which it operates and the impact this could have on its business, including its customers and the reputation of Gibraltar.

Risks should also be categorised in order to aid management and staff in identifying key risks across their areas of responsibility.

All risks to which a DLT Provider is exposed should be assessed and scored by applying the same methodology and criteria. When assessing risk, it is necessary to consider the consequences of the risk

materialising (impact), and the probability of the risk occurring, including a consideration of the frequency with which this may arise (likelihood).

A DLT Provider should develop strategies to manage all risks that it faces.

A DLT Provider is expected to have adequate measures in place to capture, assess, report and escalate risks that have crystallised.

Crystallised risks that have a material impact on a firm's business plan or an adverse effect on its customers and/or the reputation of Gibraltar must be communicated to the GFSC in a timely manner. For example, the GFSC would expect a DLT Provider to notify it of any event that results in:

- theft of customer virtual or fiat assets held by the DLT Provider;
- disruption in service offered to a client;
- customers not being able to access their monies/assets;
- legal or regulatory action being taken against the firm or any of its counterparts;
- resignation of key member of staff;
- significant operational losses;
- breach in capital requirements;
- systematic failure of a DLT Provider's IT systems;
- leak or theft of sensitive information; and
- negative press or a surge in complaints regarding the DLT Provider which could adversely affect the reputation of Gibraltar.

Risk Register

A DLT Provider is expected to maintain a central registry for the capture of all identified risks to which it is exposed, in the form of a risk register. All risks should be recorded on the risk register, categorised and assigned a risk owner. Risks and their respective controls should be assessed and managed appropriately and the risk register should be updated in a timely manner to reflect any changes to their assessed impact and likelihood.

Examples of the type of information that a DLT Provider should capture on its risk register include:

- risk description;
- risk classification;
- inherent risk score (taking account of both impact and likelihood);
- residual or current risk score (taking account of both impact and likelihood);
- risk controls;
- risk owner; and
- mitigation plans.

In order to ensure there is appropriate oversight, the individual(s) responsible for risk management within the DLT Provider should hold periodic meetings with risk owners to review their risks and follow up on any management actions.

Risk Reporting and Management Information Systems

A DLT Provider is expected to have appropriate management information systems, and assess key performance and risk indicators to allow it to monitor and adhere to its business plan, contributing positively to effective decision making. Where key performance indicators are not met, a DLT Provider should assess why they were not met and what remedial action needs to be taken.

As a minimum, the following risk information should be reported to the DLT Provider's board, senior management and internal risk committee at agreed intervals:

- material risk exposures and trends;
- new and emerging risks and issues;
- update on management actions to rectify issues and bring risks within appetite and tolerance levels;
- overdue management actions; and
- key risk and performance Indicators.

A DLT Provider will also need to comply with any ongoing reporting requirements as directed by the GFSC. The type and frequency of the reporting will be determined by the nature, size and complexity of a DLT Provider's operations.

Risk Policies and Standards

A DLT Provider should establish risk policies setting out the minimum standards that the DLT Provider expects to be followed. This will help provide assurance that all areas of risk are managed in line with agreed tolerance levels.

A DLT Provider should establish its own risk policy, appoint an accountable executive and policy owner, and develop guidelines establishing the manner in which non-compliance with, or breaches of, its risk policy should be reported and escalated. Mitigating actions to address breaches should be agreed and tracked through to completion.

Risk Appetite and Tolerance

A DLT Provider is expected to have a clearly defined risk appetite set and agreed by the board. This is fundamental to ensuring that a DLT Provider's activities are aligned with its strategic priorities by providing a mechanism through which risks can be prioritised, key stakeholders can be engaged, operations sustained and controls adjusted according to the nature and extent of risk.

A clearly defined risk appetite helps the decision-makers within the DLT Provider make risk-based decisions and ensures that risks to objectives are being managed within agreed levels.

While risk appetite is about the risks that the DLT Provider is willing to accept, risk tolerance is a measurable expression of sensitivity to different risk exposures and the ability to bear risk, practically applied through operational tolerances, which may be adjusted as appetite changes.

A DLT Provider's board should consider the relative importance of its objectives, align risk tolerance with risk appetite and set thresholds that can be monitored, and which guide day-to-day operations and decision-making.

Risk Culture

In order to ensure that effective risk management is truly embedded within a DLT Provider and that risk management activities are integrated into day-to-day business processes, a DLT Provider should ensure that it establishes a culture that encourages good risk behaviours at all levels of the organisation.

The board and senior management of a DLT Provider should lead by example and set clear expectations for managing risks.

In order to ensure that a DLT Provider establishes a risk culture that encourages risk management across all roles, relevant role profiles and job descriptions should capture relevant risk and control responsibilities. Good and proactive risk behaviours should be encouraged, recognised and rewarded.

Control Environment

A DLT Provider's control environment should consist of the governance and management functions, as well as the attitudes, awareness and actions of management about the internal controls.

A strong control environment is key to managing and controlling a business effectively as well as conducting business with due skill, care and diligence. The key aim is to integrate business risks with a DLT Provider's day-to-day operations. A DLT Provider should have controls that are relevant to specific business processes or areas and it should have a system in place to monitor controls and ensure these are operating as expected (e.g. internal audit or equivalent). Where any deficiencies are identified, these should be remediated.

The GFSC would expect a DLT Provider to assess its business risks and establish appropriate controls. This should include:

- communication and enforcement of integrity and ethical values;
- commitment to competence;
- participation by those charged with governance;
- communication of management's philosophy and operating style;
- having a suitable organisational structure for the size and nature of the business;
- assignment of authority and responsibility;
- human resources policies and practices;
- having the relevant review functions in place;
- implementation of segregation of duties;
- controls with respect to the financial reporting process;
- physical safeguards; and
- IT security measures.

This should extend to ensuring that a DLT Provider's internal audit is performed to ensure systems, controls and processes are suitable and the information being relied upon to make governance decisions is accurate.

GIBRALTAR FINANCIAL SERVICES COMMISSION

Published by:
Gibraltar Financial Services Commission
PO Box 940
Suite 3, Ground Floor
Atlantic Suites
Europort Avenue
Gibraltar

www.gfsc.gi