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 2017 (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 the regulatory principle under paragraph 4 of Schedule 2 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 risk is being managed in the right way.

Strong risk management practices will ensure that a DLT Provider is better equipped to act on risks and control in a timely manner, therefore reducing the likelihood of significant risks emerging that have not already been identified and managed effectively.

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

A DLT Provider should 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 polices and responsibilities. In order to do this, a DLT Provider should identify and assess its key current and potential risks for consolidation into the enterprise-wide risk management framework.

Further to setting the organisation's risk policy and defining risk roles and responsibilities, a DLT Provider should evaluate and assess its risks (both internal and external) and formalise them into a risk register where important elements of each risk can be documented and monitored. Furthermore, a DLT Provider is expected to analyse existing risk mitigation techniques in order to derive the organisation's residual (current) risk exposure and establish a programme of continuous improvement.

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.

The overarching aim of a DLT Provider's risk management framework is to create a robust, sustainable framework which delivers an effective and efficient approach to risk management and which contributes positively to effective risk based decision-making.

There will be an expectation that, as far as possible, the risk management activities are integrated into day-to-day business processes. A DLT Provider's risk management framework will be expected to define clear accountability for risk management, aligning risk management to performance management as well as the organisation's wider business strategy and objectives.

## 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 manage and control a business effectively as well as conduct 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 both entity level controls and controls relevant to specific business processes or areas. It should have a system in place to monitor controls and ensure they are operating as expected, and where any deficiencies are identified that these are remediated.

***Entity level controls***

Entity level controls apply across all areas of the organisation. The GFSC would expect a DLT Provider to assess their business risks and establish appropriate entity level controls. Types of entity level controls 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; and
- internal audit.

***Specific business process controls***

The GFSC would expect management to assess the risks in each specific business area and then implement relevant controls in order to mitigate risks associated to this area. Examples of business specific controls include:

- 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.

## Management Information Systems

A DLT Provider should have appropriate management information systems and key performance (and risk) indicators to allow it to monitor and adhere to its business plan, contributing positively to effective decision making. Furthermore, where key performance indicators are not met, a DLT Provider should assess why they were not met and what remedial actions need to be taken.

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

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