GIBRALTAR FINANCIAL SERVICES COMMISSION

DLT Provider Guidance Notes

Resilience

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 9 of Schedule 2 of the DLT Regulations (the Regulatory Principle).

The Regulatory Principle states that "***A DLT Provider must be resilient and must develop contingency plans for the orderly and solvent wind down of its business".***

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.

Resilience

A DLT Provider will need to develop, test and maintain adequate business continuity, disaster recovery and crisis management plans which are embedded into its risk management policies and procedures.

Preparedness for any potential threat or loss should form part of the disaster recovery plans as well as a well-managed and structured business continuity management process. Testing of the plans and its processes should form part of the business model.

Business Continuity

A DLT Provider should have a documented business continuity plan (BCP) which includes roles, responsibilities and actions to ensure business continuity following any disruptions and/or interruptions to critical functions. A BCP includes disaster recovery planning.

In the event of a significant or substantial disrupted service (that, for example, causes pending transactions to be aborted) a DLT Provider is required to implement procedures to protect consumers in a way that is compliant with the DLT Principles and fair to all those affected. The procedures should be readily available.

Backup and recovery procedures should be in place to ensure appropriate data and information (e.g. logs and financial information) are backed up on a regular basis and can be restored in the event of a disaster. Backup and disaster recovery responsibilities between software providers and operators should be clearly defined.

Information required for the fair resolution of an incomplete transaction should be recoverable by the system.

Recorded transaction information involving a customer's value, should be recoverable by the system in the event of a failure or malfunction.

Disaster Recovery

There should be a suitably documented incident handling procedure that allows a DLT Provider to smoothly transition from incident detection/trigger to resolution.

IT back-ups and contingencies should be enabled to cover for a number of areas such as:

- internet connectivity;
- servers;
- IT physical assets;
- cyber security threats;
- anti-virus software; and
- duplicate sites.

Testing

Comprehensive functional and security testing should be carried out before systems are made operational and subsequently performed at suitable intervals proportionate to the size and structure of a DLT Provider's operations. This should include physical security, IT security and cybersecurity.

Records

A list of all counterparties/service providers should be maintained on a real-time basis, including key contractual information in order to understand what the risks of each counterparty/service provider are.

A list of systems and services should be appropriately maintained on a real-time basis in order to understand what is subject to security risks and what are the most relied upon systems.

A DLT Provider should ensure that it has access to all relevant records, and can provide access to the GFSC on demand, at all times and have arrangements in place in the event of failure of primary record storage systems.

Key Person

Dependence on key individuals is a significant risk that a DLT Provider should consider and manage in line with its risk management framework.

Winding Down Process

A DLT Provider should have processes and controls in place which will inform them of the need to trigger the winding down of the business operations.

Should these triggers be prevalent, a DLT Provider should communicate and inform the GFSC in writing on a timely basis and enter into discussions about potential solutions and recovery options.

If a decision to wind-down is made, suitable and timely communication should be made to all customers and creditors.

A DLT Provider should consider how it could close down its regulated business in an orderly manner, including under stressed conditions and with minimum disruption to its customers.

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