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 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 9 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 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 that 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. Periodic testing of the plans and their processes, occurring once a year at a minimum, should form part of the firm's business model.

Business Continuity

A DLT Provider should have a documented Business Continuity Plan (BCP) that 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 to the DLT Providers Crisis Management Team (CMT).

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 firm's system.

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

A DLT Provider should have adequate arrangements in place to ensure appropriate coverage of its key functions and the continuity of services to its clients and be able to continue to meet its regulatory obligations in the event of an unforeseen interruption to internal or outsourced services. These should include but not be limited to:

- a Business Impact Assessment (BIA) considering the risks and likelihood of potential disruptions to the continuity of operations;
- the creation of a Crisis Management Team (CMT), Business Continuity Plan and Disaster Recovery Plan in accordance with industry standards (e.g. ISO 22301);
- having adequate documentation on the strategic approach to be taken in order to maintain the continuity of its operations in the event of a failure, inclusive of recovery operations to achieve this;
- having adequate internal and external Communications Strategies and Plans; and
- the regular testing of BCP and DR arrangements (at least bi-annually), including an adequate test run (at least annually). All tests need to be documented and logged with any findings.

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 a number of areas such as:

- Internet connectivity;
- Servers;
- IT physical assets;
- Cyber security threats;
- Anti-virus software; and
- Duplicate sites.

Industry standards, such as those contained in Business Continuity ISO 22301, are a good measure to be used when implementing CMT, BCP and DR.

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.

Change Management

Risks and potential security vulnerabilities can occur when changes are made to processes and procedures that might impact an organisation's operations. For this reason, we expect DLT Providers to have adequate change management processes in place taking into account the following;

- an impact assessment of any proposed changes;
- a migration or change plan;
- rollback processes;
- detailed plan on how the testing of any change is to be conducted; and
- a backup plan.

Records

A list of all counterparties/service providers should be maintained on a real-time basis. This should include key contractual information in order to understand what the risks related to 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 which systems a DLT Provider relies upon the most.

A DLT Provider should ensure that it has access to all relevant records at all times, have backup arrangements in place, and be able to provide access to the GFSC on demand, in the event of failure of its 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 to inform the board and senior management of the need to trigger the winding down of its business operations.

Should these triggers materialise, a DLT Provider should immediately notify the GFSC to discuss potential solutions and recovery options.

If a decision to wind down is made, suitable and timely communications 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