GIBRALTAR FINANCIAL
SERVICES COMMISSION

DLT Provider Guidance Notes

Systems and Security Access

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

The Regulatory Principle states that "***A DLT provider must ensure that all systems and security access protocols are maintained to appropriate high standards"*.**

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.

Cybersecurity and IT Vulnerabilities

Risks associated to cybersecurity and IT vulnerabilities could seriously impact and adversely affect a DLT Provider's customers as well as the soundness, financial stability and reputational integrity of a DLT Provider. In relation to DLT and its reliance on technology, it is more important that cyber related precautions are taken to protect the environment and mitigate these risks.

Board of Directors and/or Senior Management

A DLT Provider's board of directors and senior management need to be able to understand the firm's business and the cyber threats involved with the use of technology platforms within the business. Involvement at this level to understand and engage with potential cyber risk matters should be promoted and a security risk conscious regime should be adopted by the DLT Provider.

Directors and senior management responsibilities in relation to cybersecurity should include:

- ensuring ethical data and security governance is kept;
- having up to date cyber risk management culture;
- alignment of business strategic objectives with ICT objectives – a fast paced industry that requires quick changes but not at the risk of cyber mitigation and planning;
- having adequate cybersecurity budget and resourcing;
- management of the firm's cybersecurity controls and frameworks through adequate periodic reports; and
- ensuring all cyber controls are disseminated throughout all areas servicing the firm's operational model.

Information Security

A DLT Provider should appoint an individual with sufficient authority, responsible for overseeing and implementing the DLT Provider’s information and cybersecurity policies, programmes and initiatives.

The implementation of all security measures within a DLT Provider’s network infrastructures should be to current industry standard requirements, ensuring these include segregated levels of authoritative controls and adequate administrator segregation to avoid any potential cyber risks.

The nominated person should ensure that:

- users are adequately kept informed about potential cyber risks and threats;
- the controls, processes and policies are understood and followed by all those involved in a DLT Provider’s day to day business.

ICT Governance

A DLT Provider will be required to have adequate infrastructures (to industry standards), commensurate to their business needs and complexity, in order to safeguard the integrity of its data/information, clients and assets.

These should comply with ICT requirements, ensuring that the relevant cyber requirements are embedded in its security protocols, including:

- strong IT governance allowing the management of IT risks with adequate process to adjust these as and when required;
- adequate procedures and policies to mitigate potential cyber or security attacks or leaks with these being updated regularly to accommodate the ever changing landscape evolving around cybersecurity;
- clearly defined roles and responsibilities around ICT infrastructures with clearly demarcated segregation and adequate levels of access around all areas of systems; and
- integration of processes and procedures into the risk framework methodology.

Incident handling should form part of the integrated processes ensuring mitigation steps are implemented around any risk or incident identified root causes.

Adequate patch management at all infrastructure levels should be maintained and not delayed. DLT requires online access to areas that could adversely affect the security of systems and create vulnerabilities if these systems are not kept up to date with most recent security releases.

Independent Assessments and Tests

A DLT Provider should perform independent external tests (Penetration Tests) by an accredited third party and ensure the security and mitigation are adequate and in accordance to the set objectives.

Published by:

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

www.gfsc.gi