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 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 7 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 and adversely affect a DLT Provider's customers as well as the soundness, financial stability and reputational integrity of a DLT Provider.

In order for firms to safeguard themselves from potential attacks, it is important that as part of any countermeasure systems introduced, the following be considered:

- management of risks: Understanding the range of data held by the business and who has access to the most sensitive information. Regular reviews of access rights to data and proper data classification measures is good practice;
- keeping Systems Updated: Ensuring networks and systems are kept up to data and fully patched;
- 2FA: employing two-factor authentication for the most sensitive information; and
- disaster recovery: ensuring critical and sensitive systems and data are backed up adequately and any recovery processes tested regularly. This should include planning for worse case scenarios and ensuring that adequate Crisis Management Teams, Business Continuity Plans and Disaster Recovery Plans are maintained.

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 potential cyber threats as a result of the use of technology platforms within the business. Involvement at this level in understanding and engaging 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 good cyber risk management culture and practices;
- aligning of business strategic objectives with information and communications technology (ICT) objectives;
- having adequate cybersecurity budget and resourcing;
- management of the firm's cybersecurity controls and frameworks through adequate periodic testing and reporting; 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, with responsibility 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. Education of staff on security and cyber risk is important;
- the controls, processes and policies are understood and followed by all those involved in a DLT Provider's day to day business;
- appropriate user and device credentials are maintained. Strong passwords and keys should be used when logging into hardware or software platforms. The use of all high privileged credentials should be kept to a minimum and adequately logged; and
- appropriate Cyber Training and Cyber accreditation is obtained/achieved.

It is good practice to follow industry standards in cyber and security founded on the following:

- ISO 27001 Security Policies;
- the national Cyber Security Centre's website : www.ncsc.giv.uk/guidance/10-steps-cybersecurity; and
- Cyber Security Information Sharing Partnerships (CiSP): www.ncsc.gov.uk/cisp.

ICT Governance

A DLT Provider will be required to have adequate infrastructures (to industry standards), commensurate to its 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 cyber security;
- 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 crystallising and a Root Cause Analysis is carried out.

Satisfactory 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 the most recent security releases.

Using a formal IT governance framework ensures the alignment of an organisation's IT and business strategy. The international standard for the corporate governance of IT is ISO/IEC 38500:2015. This sets out principles, definitions and a high-level framework that organisations of all types and sizes can use to better align their IT with organisational decisions.

By following such a framework, firms can demonstrate measurable results against their broader strategies and goals, ensure they meet relevant legal and regulatory obligations, and assure stakeholders that they can have confidence in the use of IT.

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. Penetration tests should cover as a minimum the following:

- Whitebox testing - Full information about the target is shared with the testers. This type of testing confirms the efficiency of internal vulnerability assessment and management controls by identifying the existence of known software vulnerabilities and common misconfigurations in an organisation's systems; and, separately,
- Blackbox testing - No information is shared with the testers about the internals of the target. This type of testing is performed from an external perspective and is aimed at identifying ways to access an organisation's internal IT assets. This more accurately models the risk faced from attackers that are unknown or unaffiliated to the target organisation. However, the lack of information can also result in vulnerabilities remaining undiscovered in the time allocated for testing.

Cloud Computing

A number of cloud providers are available delivering a wide range of IT services. Each of these have associated risks and cyber implications, and therefore firms are expected to consider these when engaging with a provider.

A DLT Provider must ensure it follows the DLT Provider’s Corporate Governance Guidance Note “Outsourcing” section and GFSC outsourcing Guidance Note.

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