GBBC Digital Finance

Code of Conduct
Part VII

Principles for Security Token Offerings & Secondary Market Trading Platforms

These additional principles must be read in conjunction with the Overarching Principles and the GDF Taxonomy.

It is recognised that dependent on the underlying structure of a Security Token, principles outlined in other GDF codes of conduct will also apply, see here for current GDF codes. To avoid duplication these principles will not be covered in this document.

Terminology

Consistent with the regulatory regimes across the world, the categories and nomenclature of tokens should be based on the substance and economic realities of the token at issue – i.e. a substance over form approach[1]. Certain jurisdictions have established tests of (for instance) when a token will constitute a 'security' and therefore how to apply securities laws, and absent a specific regulatory regime one would expect jurisdictions to apply their existing laws if asked to determine what a token is and how it is characterised for the purposes of their laws[2]. Therefore, the categorisation of a token should start with a determination of what the token is or what it represents, and the functions and rights that a token provides.

In addition, issuers/arrangers may need to take a multi-jurisdiction approach to their analysis. For instance, if a token is interpreted to be a security in one jurisdiction, that may increase the chance that other jurisdictions also classify the token as a security, in order to promote cross-jurisdictional parity. Also, any classification as a 'security' or a Security Token may affect liquidity and tradability. For example, one or more trading venues may refuse to list or support tokens that are classified as securities, or there may be additional laws and regulations that apply to 'securities'.

The principles underlying the terms "Financial Asset Tokens," "Payment Tokens" and "Consumer Tokens", taken from the GDF Code of Conduct and Taxonomy for Cryptographic Assets, together with the discussion below on "Digital Securities", serve as an appropriate starting point to orient the reader on how "Security Tokens" fit within the greater picture.

Before deciding to issue a security token, the issuer must first determine the purpose the token will serve. Tokens may serve a variety of purposes, from representing assets that are financial in type ("Financial Asset Token"), a medium of exchange ("Payment Token") or used with a functional purpose on a set platform ("Consumer Token"). If the token is designed to serve one of these functions, designating the token as something else will not change how regulations will apply.

For example, simply designating a token as a "Consumer Token" in a token presale, when in reality it is an entitlement to dividends or interest payments, will still result in the token being classified as a security and will require appropriate licensing and registration, or an exemption therefrom.

Security Tokens

The GDF Code of Conduct and Taxonomy for Cryptographic Assets[3] refers to "financial asset tokens". For the purposes of this paper, 'Security Tokens' are a type of financial asset token, which are regulated as security and will be 'Security Tokens' for the purposes of this paper.

Security tokens are cryptoassets that have intrinsic features that are designed to represent assets typically of an underlying financial type, such as participations in companies or earnings streams, or an entitlement to dividends or interest payments. In terms of their economic function, these tokens are analogous to equities, bonds or derivatives (listed market instruments). In addition, so-called "alternative assets" (e.g. real estate, private equity, art etc) are increasingly being discussed as good candidates for being Security Tokens due to the increased process efficiency that could be brought to private placements and the ability to access global liquidity pools.

Although variations may exist, a typical Security Token would be issued by a business or entity in order to raise capital.

Examples of Security Tokens include, but are not limited to, tokens that represent:

- Shares or other equity securities in a company
- Bonds or other debt securities
- Fund interests

1 For instance, simply designating a token as a "utility token" will not be determinative and will not stop the token being categorised as something else for one or more legal and regulatory regimes.

2 Issuers/arrangers should also take into account that one or more features may be important or determinative in any analysis or categorisation of a token and should take legal advice accordingly.

3 GDF Taxonomy for Cryptographic Assets https://www.gdf.io/wp-content/uploads/2019/02/0010_GDF_Taxonomy-for-Cryptographic-Assets_Proof-V2-260719.pdf

- Other financial instruments or investment contracts
- A right to receive a certain percentage of operating revenues
- Fractional ownership of real estate or private equity assets
- A right to participate in governance (e.g. voting for decision-makers, business/product changes, or protocol changes)

The technology and smart contracts that facilitate financial instrument tokens are constantly improving. As of the date of publication, Security Tokens often include both "on-chain" and "off-chain" components. "On-chain" components refer to the part of the transfer or recordkeeping that occurs by way of a blockchain transaction. On the other hand, an "off-chain" component refers to the transfer or recordkeeping that occurs using legacy, traditional methods outside of blockchain (e.g. paper contracts). Where a platform has the technology to support it, financial instrument tokens may also be facilitated by a combination of 'private blockchains' and 'public blockchains' where the private blockchain serves the function of usually 'off-chain' components.

Digital Securities

Tokens may be structured and designed so that they explicitly are securities, albeit recorded and structured in a blockchain format ("Digital Securities"). For example, a token may be, or may directly represent, shares, bonds, depository receipt, fund interests (etc), or may be certificates representing those securities, etc.

This code of conduct applies to all regulated tokens (or Security Tokens) and therefore, if a token is treated as such, then it will be covered by this code.

Where a token is a Digital Security – i.e. it is explicitly a share, a bond, a fund interest, etc – then it seems highly likely to be a 'Security Token'. Digital Securities can include: "digitally native securities" where the security is issued or structured directly onto one or more blockchains, or "tokenised securities" where the security was not a digitally native security but has been subsequently converted into a digital security or where a cryptoasset or token is used to represent a security.

Introduction

The GDF Security Token Working Group is a group of industry community members and practitioners, specialising in Security Tokens. It has come together to develop a set of key principles and a code of conduct in order to showcase and legitimise blockchain technology as a platform for securities activities.

As there is no universal approach to regulating Security Tokens, the Working Group has analysed the common themes in the various regulators' statements, and based on the members' experience, have drafted key principles in order to provide a set of standards for best practice in the industry. This code of conduct only extends as far as Security Tokens and will not cover items such as stable coins or payment tokens.

This paper does not set out a full comprehensive view of the global approach to the regulatory treatment of Security Tokens, nor does it provide legal advice on regulatory compliance. It is up to readers to obtain their own legal advice.

1. Token Development and Issuance

This section covers important considerations and best practice for token development and issuance which is jurisdictionally agnostic. Best practices vary from jurisdiction to jurisdiction. Consider this section in compliance with existing laws as well as best practice articulated in the GDF Code of Conduct, Part II: Principles for Token Sales and Token Sale Service Providers.

a. Prior to issuing a Security Token, we will first determine what purpose the token will serve, and pay special attention to the function of the token, understanding that a token functioning as a Security Token will be treated as such, and that a token that represents or functions as a financial instrument (e.g. an equity, a bond, etc) will be treated as such. We will provide clear legal documentation that there is a legally enforceable right to something that is conferred by the Security Token;

b. Where we are an entity that is responsible for the technical design or implementation of the code or smart contracts relating to tokens:

   i. we will ensure the underlying code and smart contracts have been subject to adequate testing, and quality control (possibly including bounties);

   ii. we will use standard or open source protocols when possible and appropriate; and

   iii. we will ensure the appropriate audits have been undertaken.

c. We will take all reasonable steps to ensure that our Security Token offering(s) takes a form appropriate with its size, target market and surrounding regulatory considerations.

d. We will ensure that the mechanics for the usual shareholder / token holder interactions, such as notifications and voting, will be maintained if the Security Token confers ownership of a company.

e. To determine what regulations apply and / or whether an exemption can be utilised to circumvent some of these requirements, we will pay special attention to:

   i. the features and rights of the token;

   ii. the process in which the token will be distributed;

   iii. the classification of the issuer; and

   iv. the targeted investors in order.

f. In the event that a Security Token offering is only available to a limited circle of investors in a particular jurisdiction, and where it makes sense, we will take reasonable steps to:

   i. where a regulatory exemption or requirement requires minimum holding periods or lock up periods, limit the resale or onward transfer of tokens after a private offering until after such period(s);

   ii. limit the jurisdiction(s) from which an investor may purchase/seller may market the token, jurisdictions where: sanctions apply, the EU has designated it as a high risk third country; and legislation where no recognised legal / regulatory framework for Security Token applied;

   iii. where a regulatory exemption or requirement requires a limited number of transactions or a maximum number of holders, limit transactions or number of holders as appropriate; and

   iv. limit the sale to only investors that are qualified or accredited investors, whether self-authenticated or verified as required by law.

   Methods to enforce these limitations may be achieved by 'code' within the token or protocol itself, or via code within the token or protocol that refers to an external oracle or service provider, or via engaging the services of an investment platform or services provider, or by other mechanisms, as appropriate.

g. We acknowledge that tokens which serve as investment vehicles, structured financial products, or other regulated financial instruments or securities may have special considerations around:

   i. requirements for embedded AML / KYC;

   ii. requirements that service providers (e.g. arrangers, custodians, distributors, marketers, etc) are duly authorised and regulated in relevant jurisdictions;

   iii. offering restrictions (for instance prospectus requirements, etc);

   iv. restrictions on transfer (e.g. for regulatory imposed holding periods);

v. automated return of capital in the event of failure to meet a minimum raise hurdle; or

vi. other aborted issuance scenarios.

h. We acknowledge that where Security Tokens represent shares, bonds, fund interests, other financial instruments or investment contracts etc, it is highly likely that jurisdictions will treat these in the same way as they treat the relevant traditional security. For instance, where a token represents a share or a bond, it is highly likely that all the same laws, rules and regulations would apply as though it is a share or bond, as the case may be.

i. Where required by laws or regulations, or to satisfy any relevant exemptions, we will ensure that we have in place robust mechanisms to satisfy contractual, regulatory and compliance requirements, including but not limited to:

i. A "lock" to limit and control the jurisdictions that the Security Token can flow to.

ii. A whitelisting feature and related KYC and AML requirements.

iii. Mechanism for communication with investors. Communications may include tax forms, delivery of financial statements, voting etc.

iv. Cap table management.

v. Transfer restrictions including time-based and volume-based limitations to transfers.

vi. Ability to manage, pay and track dividend payments.

vii. Mechanism for the ability to unwind transactions.

viii. Other mechanisms to facilitate transfers for extraordinary events including transfers pursuant to divorce orders, wills, criminal seizures etc.

These mechanisms may (where feasible) be built into the smart contract of the Security Tokens, or may be monitored and enforced by third party service providers such as regulated issuance platforms.

j. If a token has the potential to change its regulatory status from a security to a non-security or vice-versa, we will provide a disclosure concerning the potential applicable triggers and consequences of this transformation.

2. Exemptions

a. We will seek legal advice to assess whether a prospectus or filing is required in the jurisdictions where the securities are being marketed or sold.

b. We acknowledge that severe legal consequences can arise if securities and financial promotion laws (or their equivalents in relevant jurisdictions) are not followed.

c. We will make ourselves aware of relevant exceptions that may exist, understanding that these vary between jurisdictions and that in certain jurisdictions offers may be exempt from prospectus requirements if:

i. the offer size is below any applicable thresholds below which a prospectus is not needed;

ii. the offer is a private placement offer made to a limited number of people; or

iii. the offer is made to institutional, professional, qualified, sophisticated or accredited investors only.

d. We acknowledge that disclosure requirements will depend on national law for offers that fall under the threshold for a prospectus.

3. Regulatory Permissions

Security Tokens

a. We acknowledge that different jurisdictions take different views on the laws, rules and regulations applicable to Security Tokens.

b. Understanding the laws, rules and regulations that apply to 'securities', (and the definition of a security itself) are not homogenous globally, we will assess whether a specific token constitutes

a security in those jurisdictions and take appropriate legal advice.

c. We will comply with all legal and regulatory requirements in every relevant jurisdiction if the nature of the token triggers the application of any respective securities regulation.

d. If we are providing services relating to Security Tokens – for instance (without limitation) arranging, custody, distribution, promotion, etc – we will:

   i. Seek legal advice to ensure that we have all appropriate licenses and approvals in relevant jurisdictions to carry out such activity and provide such services as:

      1. arranging or structuring the Security Tokens;
      2. marketing, arranging or facilitating investment into Security Tokens;
      3. custody or safe-keeping of Security Tokens;
      4. distribution of Security Tokens;
      5. promotion of Security Tokens;
      6. recordkeeping for Security Tokens; and
      7. administrative tasks relating to Security Tokens.

   ii. We acknowledge that it is highly likely that where an activity is a regulated activity (e.g. for shares or bonds), that such activity would be regulated activity for Security Tokens.

e. If we are a token issuer, we will undertake appropriate due diligence on our service providers to ensure that they are appropriately licensed, regulated (if appropriate) and qualified.

4. Token Arranging, Marketing, Offering & Selling

a. We will take care to ensure that in all jurisdictions where the offer occurs, all participants in the offering are appropriately authorised, regulated and/or licensed in those jurisdictions as appropriate:

   i. Issuer;
   ii. Arranger (including any issuance platform);
   iii. Underwriter;
   iv. Distributor or Placement agent;
   v. Broker-dealer;
   vi. Marketers; and
   vii. Trading platforms, alternative trading systems and exchanges.

b. Where we are an arranger or issuance platform for Security Tokens, we will:

   i. be clear in our marketing material whether we are authorised and regulated or not, and if we are authorised and regulated then what our regulatory permissions are;

   ii. be cautious about using terms such as "compliant" if we are not duly authorised and regulated. There is a risk that potential issuers and investors may misconstrue this term to mean that the arranger / platform is duly authorised and regulated; and

   iii. be mindful of and comply with laws, rules and regulations relating to financial promotion and other regulated activity.

c. We will conduct due diligence comparable with conventional capital raising, e.g. appropriate disclosures in line with regulatory requirements. We acknowledge that Security Tokens do not obviate the need for disclosure of relevant information.

d. We will ensure the suitability of investors to these tokens, whether this is a private or public sale or a pre-sale placement.

e. We will compare and endeavour to replicate where appropriate, the structure of Security Token offerings to traditional public and private securities offering models.

5. Secondary Markets & Trading Platforms

a. We will obtain appropriate regulatory permissions for our trading venue activities in the jurisdiction in which we operate.
    i. We will comply with the legal and regulatory requirements of the primary issuer for all instruments listed or traded on our venue.

b. We will ensure all systems and controls are effective and appropriate for the size and scale of the business.

c. We will carry out KYC and AML checks to establish the identity of the beneficial owner.
    i. We will undertake periodic refreshes of identity and additional documentation for certain accounts as required if they are frequently trading or engaged in large volumes of activity.

d. We will take appropriate measures to ensure that instruments admitted to trading provide enough publicly available information to enable our users to form an informed investment judgement.

e. We will deploy appropriate technology to promote the orderly price discovery of instruments listed on our venue.
    i. We will consider institutional targets around uptime, message trip speed and order acknowledgement.
    ii. We will consider what environment is optimal for the instruments we list or trade, considering the market depth/liquidity of the instrument and our users interested in trading it.
    iii. We will ensure our technology is fit for purpose and capable to settle trades post matching.
    iv. We will implement ongoing instrument lifecycle management, such as facilitating voting and dividend distributions.

f. We will ensure our trading venue is appropriately structured and staffed, with suitable experience and knowledge across the firm to operate a business in a maturing regulatory environment.

g. We will strive to maintain sufficient capital where appropriate, and the staff to implement the controls and processes on the venue.

h. We will employ suitable custody arrangements, as legally required, and consider if obtaining an insurance protection is appropriate.

i. We will subject all employees who have access to customer private keys to an initial and ongoing due diligence screenings.

j. We will implement a transparent policy establishing our venue's requirements for accepting instruments onto our venue for trading, including but not limited to:
    i. trading history of instrument created by issuer;
    ii. confirmation that the issuance event was lawful, and the issuance remains lawful at point of submission for trading on the venue;
    iii. law firm and service providers used by issuer on primary issuance; and
    iv. history of issuer, background of management and financial statements.
    v. if we are acting as a Security Token arranger and/or tokenisation / capital raising platform, we will be clear in our marketing material whether or not we are authorised and regulated.
        1. If we are not authorised and regulated, we will clearly disclose what our regulatory permissions include.
        2. If we are not duly authorised and regulated, we will refrain from using terms such as "compliant" or similar terminology which that potential issuers and investors could misconstrue to mean that we are duly authorised and regulated.

6. Market Integrity, Preventing Abuse and Insider Dealing

a. Where we are an issuer, we will implement effective arrangements, systems and procedures to prevent, detect and report market abuse.

b. Where we are a broker, we will disclose inside information as soon as possible and will maintain an insider list.

c. Where we are a broker, persons within our organisation who produce or disseminate investment recommendations will ensure that such information is objectively presented.

d. Where we are a trading venue, we will implement internal governance processes to ensure diligent management of shareholder interaction, including measures to deal with unauthorised Security Token creation.

e. If we are operating an alternative trading system, exchange or trading venue, we will comply with a clear set of rules, written in plain language and publicly available, in accordance with the principles set forth in the GDF Code of Conduct Part II - Principles for Token Trading Platforms.

f. If we are operating an alternative trading system, exchange or trading venue, we will employ appropriate market surveillance techniques.

   i. We will monitor trading activity and establish a benchmark of what represents normal and abnormal market activity.

   ii. We will employ systems to identify disruptions leading to a disorderly market.

   iii. We will identify and escalate breaches in a timely manner.

   iv. We will have processes in place to communicate potential market abuse, abnormal activity and financial crime to the appropriate organisations, as well as co-operate with them fully until resolved in the eyes of the relevant organisation.

7. Financial Crime Preventions and Know-Your-Customer

a. We will take appropriate steps to identify, assess and understand our money laundering and terrorism financing risks and develop and implement policies, procedures and controls to effectively manage and mitigate these risks.

b. We will comply with all relevant standards to undertake customer due diligence on all of our potential clients or investors, either on our own behalf or by engaging a properly authorised and regulated person to do so on our behalf in accordance with applicable laws, including:

   i. anti-Money Laundering checks;

   ii. know-Your-Customer and investor identity verification checks;

   iii. transaction monitoring, screening, and reporting suspicious transactions; and

   iv. record keeping, in accordance with best practice and relevant regulations.

c. We will perform enhanced measures where higher risks are identified, to effectively manage and mitigate those higher risks and monitor the implementation of those policies, procedures and controls, and enhance them if necessary.

d. Our KYC and AML checks will include applicable sanctions list checks and due-diligence. We will also carry out screening on ultimate beneficial owners.

e. When onboarding potential investors, we will aim to understand their business activity, the goods they are trading and the countries in which they are located to avoid facilitating sanctioned transactions and enable assessment of whether those activities implicate applicable sanctions laws.

f. We will not carry out or facilitate any transactions which would contravene applicable sanctions laws, or with any embargoed or sanctioned countries, or persons from those countries.

g. We will enact investor protections as appropriate, including but not limited to risk warnings.

h. We will apply a model that relies on a risk assessment of:
    i. The product/token use;
    ii. The prospect;
    iii. The target investors; and
    iv. Whether the enterprise is operating in a regulated sector or not.

8. Investor Disclosure

a. We will ensure a reasonable level of disclosure in order to minimise information asymmetry between issuers, promoters and investors.
    i. We will continue communicating with investors following a token offering and will post regular updates on progress.
    ii. We will avoid selective disclosure at all times and provide fair access and accurate information to all investors in a timely manner.
    iii. We will make obvious to investors potential risks.
b. Where we are issuing Security Tokens that are analogous to existing financial instruments, we will produce the required documents, such as a prospectus for the issuance of Security Tokens that are analogous to certain investment contracts.
c. Where a prospectus, investment memorandum or similar offering document is needed, we will ensure that it complies with all applicable laws and contain the necessary information material to an investor being adequately informed to make an assessment of:
    i. the financial condition of the issuer and of any guarantor,
    ii. the rights attaching to the securities and;
    iii. the reasons for the issuance and its impact on the issuer, including:
        1. detailed information on the issuer's venture;
        2. the features and rights attached to the securities being issued;
        3. the terms and conditions and expected timetable of the offer;
        4. the use of the proceeds of the offer; and
        5. the specific risks related to the underlying technology and any related contingency plans.
d. We will ensure that all disclosure documents and information is written and presented in an easily analysable and comprehensible form.
    i. We will communicate financial promotions for products and services, whether regulated or unregulated, in a way which is clear, fair and not misleading.
    ii. We will not overstate the potential return from the token.
e. In respect of financial promotions, we acknowledge that financial promotions such as communications to potential investors about the Security Token or the offering may be a regulated activity in one or more jurisdictions.
f. We will ensure that relevant potential investor communications are approved by an authorised person.
g. We will ensure that we take advice on financial promotion rules in all applicable jurisdictions.

9. Conflicts of Interest

a. We will be transparent about the use of promoters and broker dealers, who receive commission for inducing investors into buying Security Tokens, (e.g. celebrities, cybersecurity/privacy and disclosure the commission that such intermediaries receive.
b. We will ensure that we have appropriate processes and systems for minimising the risk of a cybersecurity breach.

10. Issuer Governance

a. Appropriate due diligence protocols will be followed during a capital raising exercise and we will implement due diligence protocols proportionate to the size and scale of the business.

b. We will review the process and legal requirements for Security Token asset services (such as corporate disclosure, proxy voting, payment of dividends or other distributions, stock splits) to be provided to all security holders.

c. We will commit to, where appropriate, treating traditional equity and digital equity pari passu.

d. We will comply with the applicable legal requirements for the corporate form chosen and we will designate a legal representative, where required.

e. We will take reasonable steps to safeguard investor and customer data, and where possible including features within the token design that promote data privacy.

f. We note that the issuance of Security Tokens may bring the product and activities around the product into a regulated space.

   i. We acknowledge that the required level of "systems, processes, controls, risk assessments and independent reviews" required to run such business(es) safely and responsibly are expected to be higher than in the non-regulated space.

   ii. We will apply similar considerations to any determination on "proportionality" in connection with the overarching principles and, as reflected in various international regulations where issuance size commonly provides for exemptions and opt-outs, the size of the offering will be an important factor to consider for operators in this market.

11.Funds

a. For information on funds, please see the GDF Principles for Funds and Fund Managers[4].

12. Secondary Market Considerations

a. We will have obtained the necessary regulatory status according to the law of the jurisdiction that we are operating in. This may be as:

   i. An intermediary (such as a broker), that facilitates the sale of securities by a client – which could be on an advised basis, an agency – or principal-basis, or as a pure arranger; or

   ii. As the operator of an organised trading platform, such as an alternative trading system or exchange – this would typically apply to firms that operate trading systems bringing together multiple buying and selling interests through an organised system for publicising, matching and executing such trades.

b. If we are operating a regulated intermediary, we will:

   i. establish appropriate terms of business with their clients and counterparties;

   ii. provide to clients appropriate information regarding the nature of the Security Token and/or ensure that the trade is suitable or otherwise appropriate for the client;

   iii. avoid and/or manage conflicts between the interests of our clients and those of ourselves and other clients;

   iv. provide appropriate information regarding the costs of execution of the transactions;

   v. subject to the basis on which legal title to the Security Token is held / recorded, establish suitable custody arrangements in respect of the tokens purchased or held for our clients. Where the Security Token is recorded on a blockchain-based ledger, we will understand clearly: how applicable law treats the establishment of title to the security represented by the token; whether typical custody structures for securities in a jurisdiction can be applied to a Security Token; and the implications for the client of the insolvency of the organisation or its custodian.

4 GDF Principles for Cryptoasset Funds and Fund Managers can be found here

c. If we are operating a regulated trading platform we will:
   i. establish a set of rules to govern the activities of market participants using the platform;
   ii. require participants to meet specific conditions in order to have access to the market;
   iii. monitor trading activity in order to identify breaches, disorderly trading or market abuse;
   iv. publish trades to the market, which may involve assessing the level of liquidity in a particular security in order to determine whether or not a trade must be published;
   v. report trades executed on the system to the regulatory authority;
   vi. ensure that the trading system is resilient, has adequate capacity to handle the volume of trades expected, and ensures business continuity in the event of severe disruption; and
   vii. ensure the orderly functioning of the market so that it does not pose a risk to participants or the financial system as a whole; and
   viii. apply appropriate AML / KYC / CDD considerations for Users / Participants, plus timely reporting to Authorities (e.g. SARs etc).
d. We will consider the legal requirements for recording the transfer of title to securities in their jurisdictions. If this requires trades to be registered by a licensed central securities depository (CSD), a transaction in a Security Token that is recorded using blockchain technology may also need to be registered on the books and records of a CSD. However, if this is not necessary, we acknowledge that this may result in a lower level of legal or regulatory protection for market participants that rely instead on recordkeeping via the blockchain only.
e. We will consider the impact of the insolvency of a participant in the transaction and acknowledge that certain national insolvency laws will provide rights to un-wind transactions that have already been executed.
f. If our system requires the creation of a new transaction to add a new "block" to the chain in order to un-wind a previous transaction we will carefully analyse the applicable insolvency laws in order to ensure that the legal implications of its operation can be clearly understood in scenarios where a participant is solvent and where it is insolvent.
g. We will be aware of arrangements for ensuring settlement finality. Some jurisdictions have laws designed to ensure settlement finality by protecting orders processed through a settlement system, even if a participant has become insolvent after (or shortly prior to) the entry of the order into the system. If an arrangement for the trading and settlement of Security Tokens is not subject to these laws, then participants may not have equivalent legal protection to that available for traditional securities.
h. We will have a clear understanding of whether we are able to benefit from the legal protections available to other financial market infrastructures (FMIs); and in any event, we will have a clear understanding of what the legal and practical implications of a disruptive event (such as a participant's insolvency) on the operation of our system and the settlement of the trades processed through it.