MFSA MALTA FINANCIAL SERVICES AUTHORITY

Feedback Statement

Feedback Statement to the Consultation Document on Security Token Offering

Ref No: 12-2019

Date: 25 February 2020

MFSA MALTA FINANCIAL SERVICES AUTHORITY

Feedback Statement

Introduction

On 19 July 2019, the Malta Financial Services Authority ('MFSA' or 'the Authority') issued the *'Consultation Document on Security Token Offering – Capital Markets Strategy'* (the Consultation Document') which was issued in line with Pillar II - 'Revising the Regulatory Framework' of the Authority's Capital Markets Strategy.

The Consultation Document aimed to pave the way to legal certainty for Security Token Offerings (STOs) in the Maltese financial markets by acknowledging *prima facie* challenges which STOs are facing within the current legal framework, particularly in relation to securities admitted to trading on trading venues, and to solicit feedback from industry participants in relation to how these challenges can be tackled in a manner that does not stifle innovation. The Authority focused, *inter alia*, on the implications of STOs within the framework of the following European Union ('EU') legislations:

- The Prospectus Regulation
- The Transparency Directive
- The Markets in Financial Instruments Directive II ('MiFID II')
- The Markets in Financial Instruments Regulation ('MiFIR')
- The Market Abuse Regulation ('MAR')
- The Central Securities Depositaries Regulation ('CSDR')
- The Settlement Finality Directive ('SFD')

Following an extension, the consultation period closed on 16 September 2019.

The Authority received feedback from 18 industry participants and interested parties which included national agencies, regulated firms, associations, technology providers, law firms and consultancy firms.

This Feedback Statement summarises the responses which the MFSA received and sets out the Authority's response and position thereto.

The Authority would like to thank all the participants who provided feedback on the Consultation Document.

1. Feedback Statement

1.1. Defining STOs

Question 1	Do you agree with the Authority's proposed categorisation of the different types of STOs?

1.1.1. Feedback Received

Most respondents generally disagreed with the Authority's proposed categorisation of the different types of STOs or had some reservations with respect to the legal certainty or clarity of the proposed categorisation. Most respondents were of the view that the concept of 'transferable securities' is a unified concept at EU law, and thus no distinction should be made based on whether the instrument is tokenised or not. A respondent who disagreed with the proposed categorisation highlighted that distinguishing between transferable securities could also create risks of structuring arbitrage.

One respondent was in favour of the creation of a new framework for traditional transferable securities which utilise distributed ledger technology ('DLT') but notes that the framework only addresses a set of financial instruments to be regulated, without addressing hybrid instruments (such as instruments akin to shares which grant profits without passing on ownership in the underlying company), as well as other traditional financial instruments such as units in collective investment schemes ('CIS').

Another respondent favoured a technology-agnostic approach and discouraged the creation of a new framework for STOs, maintaining that securities regulations should apply across the board for all securities, irrespective of the form which these take (i.e. whether they are tokenised or not). The respondent opined that the legislator should only intervene where the concerns being addressed relate directly to the tokenised form of the securities.

Another respondent supported this view and noted that hybrid forms of securities already exist in traditional markets wherein no legal distinction is made, thus tokenised transferable securities, which do not fully adhere to the characteristics of traditional shares or bonds, should not be subject to a separate regime.

Some respondents also raised a number of concerns with respect to how the proposed categorisation would function alongside the Financial Instrument Test ('FIT'). One of the respondents maintained that

if one were to follow the strict wording of the FIT, the category of 'Other STOs' as proposed by the Authority could potentially be classified as a Virtual Financial Asset ('VFA') as defined in the VFA Act[1]. One of the respondents suggested that if the proposed categorisation is enforced, a feature should be introduced within the FIT to enable the classification of Traditional and Other STOs.

Two respondents also highlighted the difficulty of distinguishing and defining what would fall within each category and noted that implementing a definition which is too narrow could create a loophole for securities that should fall under the current securities framework. Respondents generally expressed the view that it is unclear how the framework for Other STOs would work given that the same EU regulations will apply, irrespective of whether an STO is categorized as a Traditional or Other STO.

Feedback on the use of regulatory sandboxes within the context of STOs was also discussed by two respondents. One respondent was of the opinion that the creation of a sandbox environment could be the ideal means through which the Authority can test out the best regulatory requirements for the industry. On the other hand, another respondent noted that a fund-raising activity which is regulated under existing regulations should not be carried out through a sandbox since the latter is more ideal to innovative businesses models which may need licensing.

Two respondents proposed a wholly different categorisation from the one proposed by the Authority. One respondent proposed that Malta should adopt the taxonomy for crypto-assets proposed by the Blockchain Research Institute[2]. Another respondent maintained that the categorisation of STOs will depend on the level of impact of blockchain technology and the underlying infrastructure of a project, whereby a low impact of blockchain would generally entail the issue of a security in a traditional form and subsequent issue of token representing such security, while a high impact of blockchain technology would generally entail the issue of securities directly on the blockchain.

[1] Chapter 590 of the Laws of Malta, which defines a VFA as any form of digital medium recordation that is used as a digital medium of exchange, unit of account, or store of value and that is not
(a) electronic money;
(b) a financial instrument; or
(c) a virtual token.

[2] The Blockchain Research Institute created the following taxonomy for crypto-assets which generally expands beyond the taxonomy proposed by ESMA and the ECB. This taxonomy features seven categories of crypto-assets, namely: cryptocurrencies, platform tokens, utility tokens, security tokens, natural asset tokens, crypto collectibles, and crypto-fiat currencies and stable coins. For more information, refer to the following book: Don Tapscott and Alex Tapscott, 'Blockchain Revolution: how the Technology Behind Bitcoin and other Cryptocurrencies is changing the World' Reprint edition (June 12, 2018).

1.1.2. **MFSA's** Position

The Authority's initial rationale behind the proposed creation of a category of 'Other STOs' was to capture tokens[3] which, by principle, fall under the definition of a transferable security because they share some qualities with traditional transferable securities, but which do not fully conform with the traditional notions associated with such securities (e.g. tokens giving only the right to profits of certain investments of a business, yet which do not give ownership or voting rights to the token holder). The Authority wishes to avoid instances where tokens which fundamentally bear the characteristics of a security are not regulated under the applicable securities legislation merely because they do not fully conform to the traditional notions of shares, debt securities (including asset backed securities), derivatives, depositary receipts and securities offered by close-end investment funds. In line with the feedback received, the Authority acknowledges that, in principle, the category of 'transferable securities' is a unified legal concept within the ambit of EU legislation; thus, the proposed categorisation may create confusion within the industry.

From the MFSA's experience thus far with prospective STO Issuers as well as the advice issued by the European Securities and Markets Authority ('ESMA') on 9 January 2019[4], it has become evident that the advent of STOs has exacerbated the fact that the definition of transferable securities in Article 4 (1) (44) of MiFID is construed very broadly and is loosely defined at EU level[5], and in fact it is not harmonised within the laws of the Member States[6]. Although the EU legislator sheds some light on the concept of transferable securities through Commission Delegated Regulation (EU) 2017/59,[7] the general consensus from the feedback gathered from respondents is that the current resources on what the

[3]The terms 'token', 'DLT Asset' and 'crypto-asset' have been used interchangeably in this section and other parts of this document which broadly consider the nature of the asset being considered without prejudice to their legal definitions (if any) at law. Such references are thus to be construed broadly in their abstract sense.

[4] ESMA, 'Advice on ICOs and Crypto-Assets' (ESMA50-157-1391) 9 January 2019.

[5] Article 4 (1) (44) sets out that 'transferable securities' means those classes of securities which are negotiable on the capital market, with the exception of instruments of payment, such as:
(a) shares in companies and other securities equivalent to shares in companies, partnerships or other entities, and depositary receipts in respect of shares;
(b) bonds or other forms of securitised debt, including depositary receipts in respect of such securities; and
(c) any other securities giving the right to acquire or sell any such transferable securities or giving rise to a cash settlement determined by reference to transferable securities, currencies, interest rates or yields, commodities or other indices or measures.

[6] In a document entitled 'Annex 1 – Legal qualification of crypto-assets – survey to National Competent Authorities ('NCAs')' (ESMA50-157-1384), the NCAs provided feedback to ESMA wherein it was clarified that the transposition of 'transferable securities' within the legal framework of different member states was not harmonised, as set out in paragraph 8 of the aforementioned document.

[7] Commission Delegated Regulation (EU) 2017/568 of 24 May 2016, supplementing Directive 2014/65/EU of the European Parliament and of the Council with regard to regulatory technical standards for the admission of financial instruments to trading on regulated markets.

Authority deems to be a transferable security need to be clarified, particularly in view of the lack of harmonisation at EU level.

Where Issuers seek to issue a DLT Asset[8] which bears elements of a security, the Authority expects Issuers to be guided by the FIT, and in the case of borderline cases which cannot be easily classified through a *prima facie* analysis of the FIT, by independent legal advice demonstrating the legal reasoning behind the classification of a token as a transferable security in terms of MiFID. The Authority shall endeavour to issue further guidance in the future which may aid Issuers and legal advisors in the classification of DLT Assets where it is not clear that the proposed asset structure can be classified as transferable security, and thus a case-by-case and principles-based approach would be more apt. Where applicable, the Authority shall reserve the discretion to ask Issuers to explain how the proposed token structure complies with the requirements set out under our local Companies Act.[9]

As reiterated above, the definition of 'transferable securities' is only partially harmonised at EU level; thus there may be room for interpretation as to which instruments will qualify as such under this definition. To this extent, the Authority recognises the need to further explain its principles-based view of what constitutes a transferable security in line with the definition provided in Article 4 (44) of MiFID II as well as ESMA's '*Advice to ICOs and Crypto-Assets*' which provides significant insight as to how ESMA and other NCAs are interpreting the concept of a transferable security. It is important to note that this interpretation should not be construed as a legally binding definition, but only aims to give guidance to the industry.

Various scholars and regulators have identified three formal requirements which are needed for an instrument to qualify as a transferable security, namely [i] transferability, [ii] negotiability on the capital markets, and [iii] the creation of a class of securities.

i. Transferability

Transferability refers to the possibility that the token can be assigned to another person. The imposition of contractual restrictions on the transferability of an instrument does not necessarily preclude it from being considered transferable. In its Q&A on Prospectus-related topics, ESMA noted that it will analyse whether a security that is subject to such a restriction is transferable or not on a case-by-case basis.[10] If technical restrictions are coded into a token to preclude holders from effectively transferring ownership to third parties, a token will generally not satisfy the requirement of

[8] which are defined as (a) a virtual token; (b) a VFA; (c) electronic money; or (d) a financial instrument that is intrinsically dependent on, or utilises, DLT.

[9] Chapter 386 of the Laws of Malta.

[10] ESMA, 'Questions and Answers –Prospectuses 30th updated version –April 2019' (ESMA31-62-780).

transferability.[11] For transferability to subsist, the legal content or technical nature of the token should remain unchanged when it is transferred to another acquirer.[12]

ii. Negotiability on the Capital Markets

Negotiability is deemed to be a subset of the requirement of transferability since it refers to the ease with which ownership can be transferred through trading on the capital markets. The term 'capital markets' has not been expressly defined at EU level, but is generally construed as a broad term which captures but is not limited to regulated trading venues under the MiFID framework, namely regulated markets, multilateral trading facilities ('MTFs') and organised trading facilities ('OTFs').

Since the tokenisation of securities is still in its infancy, the number of MiFID-regulated trading venues which admit security tokens to trade on their platforms may be limited within the EU. However, the lack of availability, or specified market, for an instrument which bears the characteristic of a security will not preclude a token from being considered negotiable. It should also be clarified that since the categorisation of a token as a financial instrument is an objective one, the mere fact that a security token is being traded on an exchange which is not regulated under the MiFID framework should not be taken as an indication that the token is not or should not be regulated under the relevant securities laws.

Exchanges have a duty to ensure that prior to trading any instrument which bears characteristics akin to a financial instrument,[13] they attain the necessary licence since they would be operating within the remit of EU regulation. This requirement also emerges in terms of Maltese law, namely the VFA Act, which requires all VFA exchanges to carry out the FIT for all DLT Assets that will be traded on their trading systems. By analogy, VFA exchanges are prohibited from trading DLT Assets which qualify as financial instruments since they are not licensed under the MiFID regime. Failure to attain the necessary licence prior to trading tokens which are categorised as financial instruments would be a breach of law.

[11] Hacker and Thomale, 'Crypto-Securities Regulation: ICOs, Token Sales and Cryptocurrencies under EU Financial Law'. Accessible from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3075820

[12] BaFin 'Tokenisation' Accessible from: https://www.bafin.de/dok/12477346.

[13] As set out in Section C of Annex 1 of MiFID II.

iii. Classes of Securities

The definition of transferable securities calls for 'classes of securities' which possess certain qualities or rights. Thus, this necessarily implies that the securities must share a number of characteristics to be recognised as a class and that the rights or claims represented by the securities are not individually negotiated with investors. Scholars opine that for an issued security to fall under a class of securities, its units must be defined by common characteristics so that it is sufficient to refer to the type and number of units to trade them.

This generally requires fungibility within one class of shares pertaining to a single issuer in a specific round of financing. The rights conferred by share ownership will vary depending on how each company structures its articles of association within the parameters set out in the local Companies Act. To clarify, standardisation is not required for all security tokens issued by all Issuers but will suffice at investor level.

These criteria allow us to take a substance-over-form approach to the classification of transferable securities and are sufficiently broad and technology-agnostic to include transferable securities which have been dematerialised onto DLT.

Respondents also commented on the role played by the FIT within the categorisation of an instrument as a transferable security. The purpose of the FIT is to determine qualification of a DLT Asset and the laws which will regulate it, where applicable. In its 'Guidelines to the Financial Instrument Test', the MFSA notes that the guidelines are applicable to Issuers offering DLT Assets to the public in or from within Malta.[14] Within the context of financial instruments, the FIT should be considered and treated as guidance to Issuers. One may appreciate that it would be difficult to set out every possible question that would capture the spirit of what was intended by 'Other STOs' since this category deals with bespoke structures for financial instruments. The Authority does not wish to overly complicate the FIT since this would run counter to the broad definition given to transferable securities by the EU legislator and could potentially narrow the scope of applicability of the regulatory framework. In light of this, where Issuers have highly complex DLT Asset structures for their business and the token demonstrates certain characteristics of a financial instrument which were not captured by the FIT, legal advice should be sought as set out above, and a case-by-case analysis may need to be undertaken which would supersede the determination achieved in the FIT.

A number of respondents noted that the Consultation Paper did not cover the tokenisation of other financial instruments such as units in CIS. It would be apt to note that at EU level, ESMA received a number of replies in response to its survey wherein a number of NCAs noted that some crypto-assets

[14] Guidelines to the Financial Instrument Test, G1-1.1.2.

may qualify as units in CIS, mostly Alternative Investment Funds ('AIFs'). In its advice, ESMA noted that further analysis will be required to assess whether cases may fall within the scope of the Alternative Investment Fund Managers Directive ('AIFMD')[15] and therefore would need to comply with AIFMD rules. The responses given seem to indicate that, for the time being, ESMA shall focus its efforts on tokenised transferable securities.

Question 2	Do you agree with the Authority's approach to limit Traditional STOs to companies?

1.1.3. Feedback Received

Respondents maintained two different schools of thought with respect to the legal structure of Issuers.

The majority of respondents were in agreement with the Authority and felt that it is practical to limit issuances to companies for the time being. Nonetheless they all maintained the view that this initiative should eventually be extended to other vehicles such as commercial partnerships, special purpose vehicles, associations and foundations.

One respondent maintained that the Authority should create a dedicated regime which addresses STOs made under the private placement regime and which replicates the provisions applicable to traditional issuances made under private placement regimes.

Two respondents disagreed with the proposed restriction. One of these respondents noted that extending STOs to other legal forms such as foundations will give Issuers a wider choice in selecting a suitable structure. The other respondent opined that the MFSA should not reject applications relating to STOs where the Issuer is not structured as a limited liability company if there are no legal restrictions inhibiting Issuers from taking such other corporate forms. Nonetheless, they noted that the same arguments can be made for a traditional issue wherein Issuers are also being exclusively structured as limited liability companies.

[15] European Parliament and Council Directive 2011/61/EU of 8 June 2011 on Alternative Investment Fund Managers and amending Directives 2003/41/EC and 2009/65/EC and Regulations (EC) No 1060/2009 and (EU) No 1095/2010.

Two respondents made reference to the proposed requirement of a legal opinion setting out the specific legislation by virtue of which securities would be created[16]. One respondent opined that the Authority should aim to keep regulations technologically agnostic and to avoid issuing policies or new rules which apply solely in the STO context. However, they maintained that they would be in favour of a requirement setting out the need for a legal opinion where the classification of a security is unclear, irrespective of the form of the security.

1.1.4. MFSA's Position

The Authority notes that, in their feedback, respondents do not provide any particular reasons why the Authority should allow other structures besides companies to issue STOs.

In view of a number of concerns raised, it should be noted that private placement regimes are offers of securities as set out in Article 3(2) of the Companies Act which do not fall within the definition of 'offer of securities to the public' as defined in the same Act. The Authority wishes to clarify that such offerings do not fall under the regulatory remit of the MFSA, and thus no legal opinion will be requested from such Issuers. Since no separate regime has been put in place for private placements in the case of non-tokenised offerings, there would be no legal basis to create a separate regime for private placements of STOs

Question 3	Do you agree with the need to amend certain provisions of the Companies Act? Would you consider further provisions in the Companies Act to be problematic for Traditional STOs?

1.1.5. Feedback Received

All respondents agreed that there is a need to amend certain provisions of the Companies Act. Two respondents opined that the Companies Act, as it currently stands, does not expressly hinder the issuance of tokenised or DLT-enabled securities, but any amendments would ensure clarity and legal certainty. Other respondents felt that amendments would be crucial to accommodate the issuance of securities in tokenised form using DLT. One respondent highlighted the importance of ensuring that future amendments allow Issuers to keep a register of members and comply with the requirement of

[16] Section 2.1, Consultation Document on STOs.

keeping securities in a dematerialised form using DLT. Respondents also highlighted that the DLT platform itself is not a legal person, and this may present difficulties within the current framework.

Whilst agreeing with the Authority that the provisions mentioned in Section 2.2 of the Consultation Document need to be revised, a number of respondents provided ideas for further provisions in the Companies Act which would tackle a number of issues or areas of ambiguity which the industry is currently dealing with. One respondent noted that there is ambiguity in relation to whether voting rights attached to security tokens are given legal legitimacy. By way of example, the respondent questioned whether a unanimous shareholders' resolution can be passed through votes attached to security tokens. Another respondent proposed an amendment to the Ultimate Beneficiary Ownership ('UBO') Regulations[17] to ensure that transfers of instruments on the blockchain are adequately reflected in the UBO Register immediately after trading as well as in the event of dealing outside regulated trading venues.

Two respondents suggested that the current exemption applicable to dematerialised securities from requiring a written instrument for transfers should be extended to tokenised or DLT-enabled securities. One of these respondents suggested that the definition of dematerialised securities should be further clarified in order to refer to digital certificates kept on the DLT platform.

1.1.6. MFSA's Position

The feedback received shows that the industry as a whole would welcome and support amendments to certain provisions of the Companies Act, and the introduction of new provisions which take into consideration new realities and technological advancements which could not have been envisaged at the time of drafting of the Companies Act. The MFSA is in the process of liaising with the Malta Business Registry in order to amend various sections of the Companies Act, particularly in order to ensure that the registers of members and debenture-holders can be kept in a dematerialised form, using DLT. Moreover, the MFSA shall put forward proposals to provide legal clarification and a way forward on the use of DLT within the context of corporate actions.

Technology neutrality is one of the guiding principles which underpin the European Commission's policies[18], and the MFSA agrees that any regulatory actions should seek to strike a balance between the broadening of a number of provisions to allow the use of new technologies (including but not limited to DLT) within a corporate law environment, while, at the same time, avoiding overly broad provisions which may negatively alter the scope of the legislation.

[17] S.L 386.19, Companies Act (Register of Beneficial Owners Regulations), 2018.

[18] European Commission, 'FinTech Action plan: For a more competitive and innovative European financial sector' (COM(2018) 109/2) Accessible from: https://ec.europa.eu/info/sites/info/files/180308-action-plan-fintech_en.pdf

While the Authority is in agreement with the industry, and is actively working towards amending the current legal text, it is the Authority's view that Maltese corporate law is structured in a sufficiently broad way so as to give companies ample discretion when it comes to the drafting of the memorandum and articles of association. After a thorough review of the proposed corporate activity from a Maltese company law perspective, the Authority believes that companies may alter their Articles of Association in order to admit the use of DLT within the internal workings and processes of the company, for example, to open voting rights directly on the blockchain.

Question 4	Do you agree with the requirement for certain Issuers of STOs applying for admissibility to listing, to draw up a Financial Due Diligence Report ('FDDR'), regardless of the nature of the underlying security or asset?

1.1.7. Feedback Received

There were mixed responses with respect to the proposed requirement for certain Issuers of STOs applying for admissibility to listing to draw up a FDDR, regardless of the nature of the underlying security or asset.

Out of the thirteen respondents who provided feedback on this question, six respondents were in agreement with this requirement as a means of providing additional investor protection. One respondent noted that the inclusion of financial due diligence being limited to debt securities is not a commendable trait. However, a number of these respondents had reservations or proposed exemptions from these requirements where they deemed necessary. While these respondents noted that it is essential to assess the issuer's solvency, irrespective of the type of security being issued, many advocated for a proportionate approach to ensure that start-ups, which are increasingly relying on STOs as an alternative source of funding, are not unduly burdened with unnecessary costs and barriers to trade as this would inhibit Malta's competitiveness or attractiveness as a jurisdiction for STOs. Respondents provided various alternatives or mitigations. One respondent advocated for a defined list of cases where Issuers would be exempt from this requirement, for instance, where the company has audited financial statements. Another respondent opined that a FDDR should only be made necessary where the company intends to list securities which are not equal to traditional prospects, irrespective of the nature of the security.

Two respondents noted that the FDDR would not be sufficient or adequate as a disclosure tool for start-ups or companies which are not backed by established business realities since any financial projections made are often inaccurate. One of these respondents also advocated for the introduction

of minimum investment thresholds for issues where the Issuer or its holding company have limited to no track record.

The rest of the respondents disagreed with a requirement to draw up a FDDR for Issuers who will not be issuing debt securities as this was seen as an additional burden which start-up companies would not be able to comply with. One respondent noted that the FDDR requirement would be an additional financial burden on top of the requirement of carrying out a Systems Audit.

One respondent disagreed with this requirement as they found no justification for imposing this requirement solely on the basis of the tokenised form of the security. Instead, the respondent proposed that the Authority should issue a policy wherein it sets out the information which it is willing to accept, or which additional information it is willing to accept *in lieu* of a financial track record for start-ups. Such a policy would need to be framed within the framework imposed under the Prospectus Regulation and in conformity with ESMA's guidance on start-ups.[19] A similar sentiment was echoed by two other respondents who noted that a simplified FDDR would be better suited to start-ups, or companies which seek to raise funds below certain thresholds, e.g. issuances below €5 million.

1.1.8. MFSA's Position

The MFSA agrees that the requirement of a FDDR should be the same for the same type of securities, irrespective of whether these are tokenised or not. Due regard has been taken as to whether the principle of proportionality warrants the application of a lighter regime for start-ups, however, having taken into consideration the considerable risks which investors will be taking when investing in start-ups, the same requirement will be applicable to start-ups. In this respect, the Authority is in the process of revising the present Listing Rules applicable to companies applying for securities to be listed and traded on Regulated Markets in Malta. It is envisaged that such revised Listing Rules will address these issues.

[19] ESMA, 'ESMA update of the CESR recommendations - The consistent implementation of Commission Regulation (EC) No 809/2004 implementing the Prospectus Directive' (ESMA/2011/81, Paragraphs 135 – 139). Accessible from: https://www.esma.europa.eu/sites/default/files/library/2015/11/11_81.pdf

Question 5	Do you agree with the additional corporate governance requirements being recommended for Traditional STOs?

1.1.9. Feedback Received

The Authority proposed that where the board of directors is also responsible for Innovative Technology Arrangements ('ITAs')[20] underpinning the storage and transactions in securities, the following additional corporate governance requirements should apply:

i. The Cyber-Security Framework and IT Infrastructure Requirements[21] set out in the VFA Act[22] should be adhered to; and
ii. A Systems Auditor[23] should be appointed in order to prepare a Systems Audit Report[24]. The Authority would recommend that the requirements relating to the Systems Audit set out in the Systems Auditor Guidelines issued by the Malta Digital Innovation Authority ('MDIA'), be applied.

The majority of respondents were in agreement with the additional corporate governance requirements recommended by the Authority.

A respondent noted that it would be ideal to avoid cross-references to the VFA Act and the rulebooks issued by the Authority in relation to the said Act since the STO regime is separate and distinct from the VFA regime. Instead, similar rules or guidance should be issued. In the same vein, the respondent proposed that the Guidelines issued by the MDIA should be updated, and their scope should be broadened to any type of regulated DLT Asset so that they do not cross-refer only to the VFA Act.

[20] As defined in the Innovative Technology Arrangements and Services Act ('ITAS Act'), Chapter 592 of the Laws of Malta.
[21] The VFA Rulebook, Chapter 2, Title 2, Section 7, provides that the Issuer shall ascertain that its IT infrastructure ensures: the integrity and security of any data stored therein; availability, traceability and accessibility of data; and privacy and confidentiality; and is in line with the provisions of the GDPR.
[22] Chapter 590 of the Laws of Malta.
[23] The Systems Auditor shall be registered with the MDIA in line with the Innovative Technology Arrangements and Services Act, Article 9.
[24] The audit is to be conducted following the ISAE 3000 standard and is to be prepared in line with Part B Systems Audit Report Guidelines, issued by the MDIA.

Although one respondent opined that there is no need to expressly extend requirements to STOs which are already considered to be general requirements for the board of directors, some respondents also commented on the knowledge which directors should possess when sitting on the board of an Issuer, and the obligations which they will undertake. One of the respondents noted that members of the board should have the required tools and knowledge to understand their duties in line with the issuer's business, and ideally be familiar with ITAs underpinning the storage and transactions. Another respondent agreed with the proposed additional corporate governance requirements, provided that the liability of a director remains as set out in the Companies Act. One respondent questioned how the Authority will ensure that the appointed persons will have adequate knowledge and understanding of the business of the company on whose board s/he sits.

One respondent commented on instances where the operator of the ledger becomes engaged in unlawful behaviour. They proposed an additional requirement to record all versions of the ledger. In the case of a fork, this proposed additional requirement would allow the true version of the ledger to be restored in the case that the operator initiates an unlawful transaction. The respondent also proposes that qualified shareholders and the management body of a system should undergo fit and proper testing, and that direct access is given to competent authorities and designated auditors who are responsible for verifying the integrity of the ledger, and for storing the history of the transactions.

1.1.10. MFSA's Position

The majority of industry respondents welcomed, at least in principle, the additional corporate governance requirements proposed in section 2.5 of the Consultation Document, save for a number of reservations which were made in relation to the Systems Audit Report requirements.

The Authority is cognisant that certain MDIA guidelines which may be applicable to Issuers, particularly those who have developed their own underlying technology, make express reference to the VFA framework. To this extent, the Authority shall enter in discussions with the MDIA in order to ensure that the wording in the MDIA guidelines can be applied to any kind of regulated DLT Asset, including financial instruments. The Authority will also engage in discussions with the MDIA in relation to the Systems Audit Report requirements.

Where applicable, regulations or rules which directly tackle disclosures in relation to the underlying technology which fall within the remit of the MFSA shall be adopted within a separate set of guidelines to cater for tokenised financial instruments, or where more apt, any rules or guidance issued by the

Authority which address the underlying technology more broadly, such as the Guidance Notes on Cybersecurity,[25] can also be extended to apply to STO Issuers.

In relation to the Cybersecurity Framework and IT Infrastructure, the onus will be placed on the Issuer to ensure that its cybersecurity architecture complies with any internationally and nationally recognised cyber security standards, any future guidelines issued by the Authority and with the provisions of the GDPR, taking into consideration the nature, scale and complexity of the business. In this respect, the MFSA's Guidance Notes on Cybersecurity shall also need to be taken into consideration.

Respondents also gave their views in relation to what should be expected from the Issuer's board of directors in terms of knowledge and understanding of the Issuer's business, thus it would be apt to address the issue in order to provide more clarity to the industry. Both the Companies Act as well as general corporate governance requirements set out an express duty for directors to have the necessary knowledge, skill and experience that is reasonably expected from a person in the position of director.[26] The Authority is cognisant of the fact that Issuers would significantly struggle to find directors and employees at executive and managerial level with a mature knowledge on the workings of DLT, thus, imposing a general requirement on directors of Issuers of all tokenised financial instruments to have specialised knowledge on the workings of DLT would be unduly onerous. On the other hand, when DLT is set out as one of the objects of the company, the Authority will expect an Issuer's board of directors to collectively demonstrate sufficient knowledge on the workings of DLT. Additionally, it should be noted that, in terms of the Prospectus Regulation, directors are obliged to include in the prospectus information regarding their knowledge and experience. It would be also apt to include disclosures on the level of knowledge possessed by the board of directors collectively on DLT where necessary.

Nonetheless, the Authority draws attention to the proviso set out in sub-paragraph 3A of Article 123 of the Companies Act which sets out that the company shall remain responsible for the proper keeping of the register, irrespective of whether a central securities depositary ('CSD') is holding the register of shareholders. Although there are plans to amend the Companies Act in order to allow registers of members to be held on DLT, by analogy, the company will ultimately still be responsible for its register of shareholders, irrespective of the fact that this process has been delegated to the underlying DLT. This highlights the importance of auditing the DLT because the board of directors would be undertaking responsibility for the functioning of a technology which not all of them may fully understand.

[25] MFSA, 'Guidance Notes on Cyber Security' accessible from: https://www.mfsa.mt/wp-content/uploads/2019/06/Cybersecurity-Guidance-Notes.pdf

[26] Article 136A of the Companies Act, Cap. 386 of the Laws of Malta.

Thus, the Authority reiterates its belief that the additional corporate governance requirements proposed, including the requirement to audit the system, will assist Issuers in the fulfilment of their duties in terms of company law since they act as *prima facie* proof that the directors undertook the necessary steps to ensure the soundness of technological systems used within the inner workings of the company which they may lack technical knowledge in.

Question 6	Do you agree with the requirement of a Systems Audit? If not, what alternative measures for testing and verifying the integrity of the system would you suggest?

1.1.11. Feedback Received

All respondents agreed in principle with the imposition of a Systems Audit requirement, subject to certain reservations. One respondent noted that there should not be a one-size fits all Systems Audit, but it should be made specific to the different types of tokens.

Another respondent proposed that a register of audited ITAs should be created to avoid the re-auditing of an ITA by the same or a different Systems Auditor. That ITA may be availed of for another offer by the same Issuer or another Issuer altogether during the same period, or the ITA itself may already be audited under any other regulatory requirement or voluntarily submitted for auditing. The respondent also proposed that the Systems Audit should not be a requirement for securities issuances across the board and proposed that where an Issuer is exempt from drafting a prospectus in terms of the Prospectus Regulation, it should also be exempt from the requirement of conducting a Systems Audit.

One respondent noted that the requirement to conduct a full Systems Audit, as set out in the MDIA Guidelines, is cumbersome, will drive up costs and delay the STO launch. The respondent posited that an alternative measure for testing and verifying the system would be to create a checklist outlining a number of points for verification. This could take the form of certain internal procedures, which could include know your client ('KYC'), system security, keeping of records, backing management, anti-money laundering ('AML') measures and the system to record financial transactions. They also suggested that Issuers that generate tokens on their own ITA may be required to undergo a Systems Audit every two years, with the first one taking place within one year of the launch of the STO. The rationale behind this proposal is to facilitate the process for launching a STO.

Another respondent agreed with the requirement of a Systems Audit but sought clarification on who would be the subject person responsible for fulfilling this requirement. Where the Issuer operates its own underlying DLT, the respondent opined that the Issuer itself would be responsible for performing the Systems Audit, but where a third-party technological platform is used, it should be the third-party platform, and not the Issuer, that is subject to the additional corporate governance requirements proposed.

One of the respondents noted that the MFSA should clarify that the Systems Audit must be carried out in terms of Systems Auditor Guidelines issued by the MDIA by an approved Systems Auditor, and that it should be required for entities seeking any MFSA-issued licence and using DLT. Along the same vein, another respondent suggested that the entities entrusted with the carrying out of Systems Audits should be approved by the respective authority, and the latter shall review their approval on an annual basis to ensure that the quality of the Systems Audits is kept up to the required standards.

Another respondent proposed an alternative measure whereby an equivalence regime between (a) the positive outcome of a system audit on the security systems of the entity in Malta and (b) the option to rely on storage solutions offered by regulated crypto-custodians (either in Malta or under another reputable jurisdiction) offering both hot and cold wallet arrangements, and which subject themselves to rigid IT-standards/audit.

A risk-based approach was favoured by one of the respondents who argued that any added requirements should not be driven by whether DLT is used or otherwise, but by any additional risk involved. The respondent did not agree with a Type 2 Systems Audit being a requisite across the board for all Issuers using DLT, whether it is a native system or whether it is a third-party technology. They argued that the requirement of a Systems Audit should thus be based on the results of a risk assessment which should be proportionate to the situation of the Issuer and the offering.

1.1.12. MFSA's Position

In light of responses received from respondents who may not be wholly familiar with the ITAS Act, the MFSA would like to clarify that the Systems Auditor responsible for the drafting of the Systems Audit Report would be registered with the MDIA in line with Article 9 of the ITAS Act.[27]

In order to avoid the risk of regulatory arbitrage between the treatment of different regulated DLT Assets, and in view of the fact that the underlying technologies and ITAs which are being used within

[27] The Systems Auditor Role has been designated in Section 2 of Chapter 01, titled 'Systems Auditor Role', Part A – Systems Auditor Guidelines, issued by the MDIA.

the context of initial VFA offerings and STOs present the same risks, the Authority would like to restate and clarify its new position in relation to the proposed requirements:

1. A Systems Auditor will need to be appointed if the Issuer has an ITA in place, as defined in the First Schedule to the ITAS Act; or if the Issuer operates a technological infrastructure which interacts with an ITA in some way or form, including *inter alia* a wallet.

2. Where a company will be operating an ITA which underpins the storage and transactions in securities, a Systems Auditor will need to be appointed to prepare a Systems Audit Report in line with the MDIA's Guidelines. If an Issuer utilises the services of a third-party platform, it should be understood that all the requirements mentioned in this feedback statement and any guidance or rules which have been or which may be issued by the Authority will apply *mutatis mutandis* to such third party platforms and their operators, instead of such Issuer.

Question 7	Do you agree that the Prospectus Regulation and the relevant Annexes are adequate in the case of Traditional STOs? If not, what alternative/additional requirements would you consider sufficient for an informed investment decision to able to be taken?

1.1.13. Feedback Received

Respondents generally agreed that the Prospectus Regulation and the relevant Annexes are adequate in the case of Traditional STOs.

One respondent highlighted the need to digitally facilitate the preparation of the prospectus and the submission process by harnessing the benefits of DLT. This would mitigate legal consultancy and preparation costs and the time required which are considerable challenges, particularly for low-value security issuances.

A respondent proposed that additional key risk disclosures should be made to the investor before the latter invests in the securities, including the risk of a highly speculative valuation, heightened risk of fraud, and lack of a proven track record of the STOs. The respondent also proposed a review of marketing restrictions for STO issuances which may require further elaboration, taking into consideration the cross-border aspect of operations involving DLT.

Two respondents agreed that additional disclosures should be inserted in the prospectus, notably information concerning the systems audit and the Cyber-Security Framework and the IT Infrastructure Requirements as noted in Section 2.5 of the Consultation Document. A respondent also proposed that the offering documentation should also include, *mutatis mutandis*, most of the information set out in the First Schedule of the VFA Act, save where this information overlaps with the standard content required by the Prospectus Regulation.

One respondent agreed and suggested that the Authority could issue non-binding guidance as to how particular DLT-enabled issuances of securities can be addressed within the context of particular (existing) disclosure requirements.

1.1.14. MFSA's Position

The feedback received was in line with the Authority's understanding that the prospectus shall need to contain the relevant information in relation to the 'Code Risk' which tackles pertinent risks associated with the underlying ITA or technology utilised, [28] namely information in relation to the Systems Audit and the Cyber-Security Framework and the IT Infrastructure Requirements set out in Section 2.5 of the Consultation Document. The wording of the Prospectus Regulation is sufficiently broad to allow for these disclosures to be made without the creation of additional requirements which go above and beyond what the Regulation sets out.

1.2. Additional ongoing obligations following an Offer and/or Listing and/or Trading of Traditional STOs

Question 8	Do you agree with the proposed additional requirement? If not, what alternative processes would you suggest ensuring proper controls of the system?

The MFSA proposed that where the company itself operates the underlying DLT, the company is required to prepare annually a Type 2 Systems Audit as outlined in Section 2 of Chapter 1, titled 'Systems Auditor Role', Part A – Systems Auditor Guidelines issued by the MDIA.

[28] To this extent, a specific risk factor should be included which states that it is possible that circumstances may arise where the DLT software may not always reflect the algorithm and features described in the prospectus in order to deter investors from blindly trusting the system being used.

Out of thirteen respondents to this question, eleven agreed in principle that a Systems Audit is needed in order to ensure proper controls of the system; however, the majority of these respondents did not fully agree with the proposed requirement as put forward by the Authority. One respondent requested clarity as to the procedure which will be implemented where the Issuer's company itself does not operate the underlying DLT.

One respondent, who was in agreement with the Authority's proposal, suggested that further elaboration is needed with respect to additional requirements that the DLT system should have, including *inter alia*, whether an ISO standard or MDIA certification for the DLT platform is required.

A number of respondents noted that a requirement to prepare an annual Type 2 Systems Audit would be overly cumbersome and costly for operators. One respondent noted that where the Issuer runs an application built on top of a respective blockchain, a yearly systems audit report should suffice, rather than having a Systems Auditor engaged at all times.

Another respondent disagreed with the additional requirement, noting that carrying out a Type 2 Systems Audit on an annual basis is more cumbersome than a Type 1 Systems Audit. The respondent was of the opinion that a Type 1 Systems Audit should be required instead, which is to be carried out after the launch of the STO on a biennial basis at most. Another respondent shared a similar sentiment, noting that requiring Issuers to hold a Type 2 Systems Audit on an annual basis would be a burdensome cost for operators which would act as a deterrent to start-ups. Instead the respondent proposed that after the first Systems Audit, which is to be carried out on application in the first year, subsequent Systems Audits should be carried out on a less frequent basis. They noted that the MFSA would also need to set out a policy on which significant changes or enhanced risks necessitate a premature review of the systems and proposed that the Authority should have the power to conduct surprise inspections. Another respondent noted that it is not clear how the Authority would manage to supervise the need for a Type 2 Systems Audit in a non-listed exempt offer.

Another respondent maintained that companies should be treated equally in spite of the fact that they are issuing an STO. The respondent opined that where securities are being stored by a custodian, and tokens are the only asset, which is being traded, there is no need for the proposed requirement since the custodian would already be mitigating the risk.

1.2.1. MFSA's Position

The underlying technology underpinning the Issuer's business presents significant risks to investors, particularly because the existence of their investments is contingent on the proper functioning of this technology. Thus, irrespective of whether the underlying technology can qualify as an ITA under the ITAS Act or whether such technical infrastructure falls outside the scope of the said Act but interacts

with an ITA or has a bearing on the transaction or storage of the DLT Asset, it is in the investor's interest to ensure that the technology functions properly.

Having taken due consideration of these risks, the MFSA will be amending its proposal in relation to the requirement of a Type 2 Systems Audit where the company operates its own native ITA.

Instead, a requirement to appoint and have in place a Systems Auditor at all times shall apply where the Issuer has an ITA in place, or if the Issuer operates a technological infrastructure which interacts with an ITA in some way or form. This Systems Auditor shall need to prepare a Systems Audit Report which is in line with the MDIA's Guidelines,[29] as well as the Authority's Guidance Notes on Cybersecurity. Such a requirement will be considered crucial where the ITA underpins the storage and transaction of securities but should not only be limited to such a scenario. It is being proposed that the MDIA's Forensic Node Guidelines shall also be applicable in order to keep a trail of the behaviour of the ITA as a whole, if feasible.

It should be noted that the same regime has been adopted in respect of other MFSA- regulated DLT Assets, namely VFAs in order to avoid regulatory arbitrage.

As reiterated above, where an Issuer utilises the services of a third-party platform, it should be understood that all the requirements mentioned in this feedback statement and any guidance or rules which have been or which may be issued by the Authority will apply *mutatis mutandis* to such third party platforms and their operators, instead of such Issuer.

It should also be noted that non-listed exempt offers, i.e. offers which do not constitute an offer made to the public as set out in section 2 (3) (a) of the Companies Act, will not be required to comply with any of the proposed requirements since they fall outside the regulatory remit of the MFSA.

[29] Reference should be made to the MDIA's Guidelines, with particular reference to Chapter 2, ITA Guidelines.

Question 9	Do you agree with the Authority's expectation that companies operating their own DLT would be only companies offering Traditional STOs to the public, without seeking listing and/or trading of such Traditional STOs on trading venues?

1.2.2. Feedback Received

Five out of eleven respondents to this question agreed with the Authority's expectation that companies operating their own DLT would only be companies offering traditional STOs to the public, without seeking listing and/or trading of such Traditional STOs on trading venues. The other six respondents disagreed with this view for a variety of reasons. Two respondents shared the view that one of the primary reasons why an Issuer would opt for an STO over a traditional issue is the expedient transferability of such tokens since this is a major selling point for potential investors.

Another respondent noted that companies opting to issue an STO would be placed in a disadvantaged position when compared to other companies which would be able to list their securities which are not based on DLT. This situation would lessen the attractiveness of STOs as an investment tool for Issuers and investors alike.

One respondent disagreed with this expectation on the basis that the definition of a trading venue might not be sufficiently broad to cover future operating models of DLT-based trading venues.

1.2.3. **MFSA's Position**

The Authority expressed this expectation in light of the fact that secondary market trading of STOs which is not done on a P2P basis is currently very limited. Additionally, where a company operates its own DLT it is possible that issues of interoperability with the underlying technology used by a trading platform may arise.

The Authority does not intend to limit offers to the public made by Issuers operating their own DLT from attaining the necessary authorisation from the Listing Authority to list their securities on a secondary market; however, on a practical level, a solution is yet to be found for the settlement of such securities since listing and/or trading would trigger the requirement of recording securities in a CSD, which shall be further explored in a section setting out the MFSA's position in relation to Questions 18 to 24 of the Consultation Document.

1.3. Secondary Markets

Question 10	Do you agree that a permission-less decentralised exchange could pose difficulties in ensuring compliance with the transaction reporting requirements contained in MiFIR?

1.3.1. Feedback Received

Seven out of ten respondents agreed that permission-less decentralised exchanges could pose difficulties in ensuring compliance with the transaction reporting requirements contained in MiFIR, particularly due to the lack of a clearly identifiable market operator or central point of compliance. One respondent noted that the Authority would need to undertake a MiFIR suitability process.

Two respondents noted that unless an EU-wide initiative is taken to address the application of DLT within EU securities markets, it will be very problematic for the concept of a permission-less decentralised exchange to comply with current regulations. A more global effort may also be required since permission-less decentralised exchanges cannot be limited to EU participants. One respondent acknowledged that operators will often have to work around the regulatory limitations which will in most cases dilute the advantages and effectiveness of DLT. This regulatory framework leaves very little leeway to jurisdictions to innovate within the context of listed STOs and secondary markets. One respondent also noted that the identifiers and classifications which are currently in use will also need to be reviewed and adapted to the new developments of DLT.

Within the current framework, centralised exchanges and permissioned decentralised exchanges with investment firms granting Direct Electronic Access ('DEA') were preferred by one of the respondents. Where permissioned decentralised exchanges are concerned, one respondent opined that the Authority should focus on the initial limitations that are to be coded at the outset and on the brokers that should be assessed on their competency and knowledge of DLT before being allowed to trade on a decentralised exchange. The respondent also opined that in the case of a decentralised exchange where the inclusion of a CSD is not possible, it would be practical to initially test out whether the DLT itself could act as a settlement internaliser in a sandbox environment.

Another respondent held that where a permission-less decentralised blockchain is used, limitations can be coded at application layer stage. The respondent did not agree that trading of security tokens should be limited to exchanges of a specific architecture only, and suggested that regulations should take a technology neutral approach whereby the onus would be on the prospective applicants to

demonstrate to the Authority that a proposed architecture can adhere to its legal obligations and be subject to the necessary supervision. Another respondent supported the latter point and added that limiting any new regulatory framework to permissioned and/or centralised models to avoid regulatory complications would hinder the jurisdiction's allure for STOs.

On the contrary, one respondent held that a decentralised exchange should not be considered as an option for STOs due to difficulties with KYC and AML obligations, and a general prohibition against bearer shares in the EU.

A respondent opined that a 'permission-less' exchange is something which does not exist in practice. The respondent noted that distinguishing between permission-less and permissioned blockchain is immaterial to the issue of transaction reporting under MiFIR because this categorisation refers to the authority which validates the blocks of transactions. Instead, the respondent argued that compliance mechanisms and restrictions can be imbued in the code of the digital asset itself and of the wallets where such assets are held for investors, thus substituting certain functions which are currently being carried out by intermediaries. Such tokens would be able to restrict who is allowed to transact using the asset, irrespective of the architecture of the underling blockchain. Moreover, they argue that decentralised exchanges can have an operator who is responsible for reporting and fulfilling other regulatory requirements, including *inter alia* KYC requirements.

A respondent opined that the use of decentralised exchanges, where licensed intermediaries have been eliminated, removes an additional layer where any possible abuse of the securities sector to carry out ML/TF can be detected, irrespective of whether the exchange operates on a permissioned basis. The respondent acknowledged that in-built controls within the chain itself can be used to adhere to AML/CTF obligations but questioned how it can be ascertained that these are having the desired result. The respondent also questioned who would ultimately be responsible for obligations such as the submission of suspicious transaction reports, replying to requests for information and the enforcement of AML/CTF requirements, and whether an obligation will be imposed on the operator of the ITA to appoint a technical administrator to ensure compliance with the regulations.

1.3.2. MFSA's Position

While the Authority generally agrees with the majority of respondents that permission-less decentralised exchanges could pose difficulties in ensuring compliance with the transaction reporting requirements contained in MiFIR due to the lack of an identified operator which takes on liability for non-compliance of the platform with the various applicable legislation, it is not its intention to impose a ban across the board for all decentralised exchanges. On the other hand, the MFSA cannot take a "one size fits all" position for all exchanges employing a decentralised element since the projects and

business models put forward by prospective applicants often vary significantly. Thus, it will be the responsibility of prospective applicants to prove to the satisfaction of the Authority how they plan to comply with existing EU legislation.

Question 11	Do you agree that Traditional STOs should be traded on either a centralised exchange via investment firms (with the possibility of investment firms granting DEA) or on a decentralized exchange with investment firms granting DEA?

1.3.3. Feedback Received

Eight respondents gave their feedback to this question, and very different positions were taken by some of the respondents with respect to the preferred architecture of an STO exchange.

Two respondents advocated for the use of decentralised exchanges without the involvement of investment firms acting as intermediaries, citing the fact that the scope of decentralisation is to eliminate intermediaries within the securities value chain. Moreover, one respondent highlighted the fact that with the use of DLT, regulators should be able to automatically access the DLT, and thus review all the transactions without the need to report. Such a scenario implies that the DLT cannot be permission-less and open only to MiFID II licence holders.

Another respondent advocated for the exclusive use of centralised exchanges wherein both investment firms executing orders on behalf of clients, as well as individuals, can directly transact.

The majority of respondents agreed that the trading of Traditional STOs on centralised exchanges via investment firms, possibly with investment firms granting DEA to clients, as well as trading on decentralised exchanges with investment firms granting DEA would be feasible, as long as all the current regulatory requirements can be abided with.

1.3.4. MFSA's Position

The MFSA welcomes the feedback received from respondents and the points put forward. While the current regulations provide for a high degree of intermediation within the current securities value chain which has been criticised over the years, one cannot overlook that some level of intermediation has proven necessary, for example in the avoidance of money laundering and terrorism financing. Thus, to date, the Authority believes that full disintermediation would not be an optimal solution.

Question 12	From the general findings, it appears that a trading platform operating a permission-less decentralised exchange will pose various difficulties from a regulatory point of view. Would you agree? How do you believe that such difficulties can be overcome?

1.3.5. Feedback Received

Six out of eight respondents agreed that there are various difficulties to the adoption of permission-less decentralised exchanges, most notably in relation to AML/KYC considerations. A respondent noted that difficulties will need to be overcome through legislative intervention at EU level, since any workarounds within the current framework will probably dilute the benefits of DLT.

One respondent agreed that permission-less decentralised exchanges will pose a challenge to adherence with the FATF 'Travel Rule' due to the fact that the identity of the recipient is not always known and cannot be verified with certainty. ML/TF concerns also arise due to the ease with which multiple wallets can be created for peer-to-peer transactions, with no possibility of limiting virtual asset transfers between two counter parties. The solution proposed by this respondent rests on the use of token standards which can facilitate AML/KYC compliance such as the ERC 777 token standard.

Along with AML/KYC issues, the lack of supervision and pre-vetting of users were identified as the main disadvantages of permission-less exchanges by another respondent who completely discouraged their use within the context of trading of securities. In the same vein, another respondent raised the same issues, but also noted that if the user holding the securities in his/her personal wallet gets hacked, the security would effectively exchange hands and ownership in the same way as a bearer share. Thus, STOs would need to adopt a token standard which will allow only approved wallets to receive the token, and which require AML/KYC checks to be done before any token holder can transfer the token.

One respondent expressed concerns that without the intervention of an investment firm, difficulties will arise with respect to transaction reporting and monitoring as well. Since the users who often do not possess sufficient technical know-how will be holding the asset, the respondent questioned whether it might be too soon to consider permission-less decentralised exchanges until the industry matures and investors become better acquainted with digital investments. In the interim, the respondent proposes that decentralised permission-less exchanges should be allowed for more sophisticated investors.

1.3.6. MFSA's Position

The MFSA agrees with the majority of respondents that a permission-less decentralised exchange poses various difficulties from a regulatory point of view. The main difficulties which were highlighted by respondents include: the lack of an identified market operator, compliance with prevention of ML/TF obligations, investor protection considerations due to the lack of pre-vetting of users, and other practical considerations from a transaction reporting perspective.

Additionally, the Authority did not agree with the proposition of creating an authorisation process for permission-less decentralised exchanges to offer their services to professional investors since, by definition, their permission-less character can allow anyone to utilise the DLT, including retail investors.

Respondents also suggested that restrictions can be imbued in the code of the token or the wallet itself, rather than the underlying DLT. Such proposals would need to be scrutinised carefully by the Authority, and the prospective applicant would need to prove to the satisfaction of the Authority that its business model adheres to the applicable regulations. Such scrutiny would necessarily require an audit of the underlying system to ensure the operating effectiveness of these restrictions or other technical solutions.

Question 13	To what extent do you believe that a centralised trading platform or a decentralised but permission-based trading platform (hybrid) would work in practice?

1.3.7. Feedback Received

Responses elicited from this question were varied but common understandings emerged among some of the respondents.

Three respondents held that both centralised trading platforms, as well as a decentralised but permission-based trading platforms (hybrid) would provide a workable solution if the conditions imposed at law can be complied with. Respondents noted that decentralised exchanges which have a certain market operator can conduct the necessary AML/KYC transaction reporting and supervisory duties. One respondent noted that this can be done through the imposition of restrictions at the application layer.

One respondent noted that centralised exchanges would defeat the scope of using DLT and advocated for hybrid platforms as an ideal compromise between innovation and investors' need for security, identity and role definition within the blockchain.

A centralised model was favoured by one respondent who noted that until regulatory efforts are undertaken at EU level, this model would be ideal. Another respondent maintained that centralised platforms are the only secure option for regulatory authorities.

One respondent noted that trading platforms could be an ideal test case for the regulatory sandbox.

1.3.8. MFSA's Position

The MFSA is in general agreement with the respondents and believes that both centralised as well as hybrid platforms could provide a workable solution. While some respondents expressed the view that in theory, the technology can still be used in a way that is compliant with the current legal framework, a case-by-case and practical analysis of how the technology will be used will be needed which is where the regulatory sandbox can lend itself well.

1.4. Market Abuse Regulation

Question 14	What are your views regarding transparency/transaction reporting and prevention of financial market abuse? Do you agree that the prevention of financial market abuse is intrinsically dependent on transaction reporting?

1.4.1. Feedback Received

The majority of respondents agreed that transaction reporting plays a major role in the monitoring of market abuse and noted that security tokens and DLT could help expedite and assist in the oversight of market abuse due to the traceability of records which is a fundamental characteristic of DLT.

Four respondents noted that the adoption of DLT could add a layer of legitimacy to the information reporting obligation and could give supervisors and management bodies of trading platforms enhanced tools to monitor market abuse practices, potentially through automated transaction reporting and the provision of live data and direct access to the supervisory authority.

Another respondent opined that having the token holder's rights and legal responsibilities embedded directly onto the token, coupled with the immutable record of ownership, should add transparency to transactions by enabling users to know who they are dealing with, what rights are embedded in the token and who previously owned the token.

Drawing on the experience of VFA exchanges, one respondent maintained that several cryptocurrency exchanges show fake volumes on their websites. Thus, they emphasised the need for rules against data manipulation, and proposed that onsite inspections should be carried out.

1.4.2. MFSA's Position

The feedback received is welcomed as it shows a sound appreciation of the importance of transaction reporting as a tool to prevent market abuse. The Authority will explore further how it can harness the benefits of the blockchain in its market oversight function in order to prevent and detect market abuse, taking into consideration practical and logistical limitations which both the platform and the supervising Authority will face with the adoption of these technologies.

Question 15	Are you of the view that decentralised exchanges pose risks to market integrity?

1.4.3. Feedback Received

Respondents expressed varied views in relation to the risks which decentralised exchanges pose to market integrity. Two respondents were of the opinion that centralised exchanges are more ideal than their decentralised counterparts from a market integrity perspective. One of these respondents noted that decentralised exchanges which allow any wallet to access the market are more susceptible to pump and dump schemes. One respondent opined that where trading platforms are left unregulated, potential risks may arise through fraudulent and negligent behaviours.

One respondent held the view that completely decentralised exchanges pose a higher risk to market integrity but advocated for decentralised but permission-based trading platforms (hybrid) due to the possibility of monitoring who may be admitted on the chain, thus safeguarding the market and controlling market abuse. The respondent suggested that the main risks associated with decentralised

systems should be identified, including *inter alia* the management of the wallets and the private keys that control them. Difficulties in identifying the market operator and judicial representatives was highlighted as a main risk by another respondent who also suggested that decentralised exchanges should initially be allowed to operate in a regulatory sandbox.

Three respondents generally held the view that as long as a decentralised exchange is capable of embracing the principles set out in the applicable laws and providing tools which address any gaps that DLT poses from a risk exposure point of view, the risks of diluted market integrity are mitigated. One of these respondents also noted that decentralised exchanges do not necessarily increase the risk of front running since the illegality behind that practice emerges when trades are placed on the basis of non-public information. If the information on trades is available to the whole market, the respondent argued that all investors would be on equal footing, thus no illegality subsists. The respondent also assumed that planned orders would not be made public, but rather, only actual/settled trades would be recorded on the DLT system. This assumption was supported by another respondent who noted that access to the order book is not normally structured through the blockchain, but remarked that the order book can be publicly available through a public API access for any user of the internet with the ability to make relevant API calls to the matching engine. However, the ability to obtain data from the matching engine can be limited only to users who are approved by the operator of the decentralised exchange.

One respondent disagreed with the view that decentralised exchanges pose risks to market integrity since limitations can be imposed on the users of the platforms. They also argued that a parallel may be drawn with the VFA framework wherein decentralised models are permitted, so long as the requirements imposed on the operators of VFA exchanges are fulfilled. The respondent thus opined that it is still possible to identify a market operator in a decentralised security token exchange who can fulfil the relevant MAR requirements.

Another respondent opined that market manipulation can be avoided or mitigated through the absence of a centralised order book and price chart. They proposed that monitoring can be conducted by a recognised broker while approving orders and transactions, and that, in the future, this process can be automated.

1.4.4. MFSA's Position

The Authority acknowledges the varied feedback received, particularly in relation to how certain types of market abuse can be avoided when there is a DLT element and a decentralised model has been adopted. Nonetheless, a practical evaluation will need to be undertaken depending on the business

model of the platform in order to identify and address weak points within the system which fall within the remit of MAR.

Question 16	Do you agree that in order to safeguard market integrity, Traditional STOs should only be traded on centralised exchanges?

1.4.5. Feedback Received

Four out of nine respondents agreed that in order to safeguard market integrity, Traditional STOs should only be traded on centralised exchanges. One of the respondents noted that the Authority should take this approach for the time being, but should not exclude the possibility that, in the future, and after having adequate controls and systems, trading of tokenised financial instruments should be extended to permission-based decentralised systems. The respondent also advocated against the use of permission-less decentralised exchanges for trading of any financial instrument. Another respondent favoured centralised exchanges for the trading of traditional STOs, provided that additional safeguards are implemented to ensure compliance with MAR and to grant access to regulators. Nonetheless the respondent noted that these safeguards may also be implemented in a decentralised system. One of the respondents who advocated for centralised exchanges noted that these would still need to adhere to strict rules concerning fake volumes, insider trading, and pump and dump schemes which can be carried out by individuals who are external to the exchange.

Five respondents maintained that the trading of traditional STOs should not be limited to centralised exchanges but should also be open to decentralised exchanges provided that these comply, and do not prevent participants from complying, with all relevant MAR and MiFID II requirements. Two of these respondents advocated for decentralised exchanges with a permissioned element, while another respondent agreed with the Authority that a truly decentralised exchange will struggle to comply with the current legislative framework.

One respondent noted that if a decentralised approach is adopted, the 'sponsor' should be responsible to ensure MAR adherence.

1.4.6. MFSA's Position

In light of the varied responses received, the Authority notes that the industry remains divided on the approach which the regulator should take in relation to decentralised exchanges. The Authority reiterates the position expressed in relation to the MIFID framework and concludes that a case-by-case analysis based on the proposed business model will be needed.

Question 17	Do you agree that permissioned systems allow for enhanced investor protection?

1.4.7. Feedback Received

Seven out of ten respondents maintained that, in principle, permissioned systems allow for enhanced investor protection.

One respondent reiterated the belief that if a permission-less decentralised DLT is used and safeguards are implemented at application level, the exchange can be designed in such a way that it does not compromise investor protection. Along the same vein, another respondent noted that the permissioned or permission-less character of a blockchain does not have any impact on exchange transactions or investor protection since restrictions can be imbued into the code of a digital asset itself or the wallets where the assets of the investors are held. Another respondent reiterated that a technology-agnostic approach should be taken where possible.

1.4.8. MFSA's Position

The MFSA shall take into consideration the points highlighted by the respondents.

1.5. Post-Trade Settlement

Question 18	What are your views in relation to the extent of applicability of the CSDR? Do you think that the legal requirements relating to settlement could possibly impede the application of DLT?

A number of respondents expressed the view that the legal requirements set out in CSDR in relation to settlement may impede the application of DLT unless a number of challenges are addressed, or the current legislation is optimised to embrace the use of DLT within the settlement process. Respondents held varied views as to whether compliance with CSDR can be maintained within the context of a DLT-based system. A respondent held the view that until the legislation is revised, there is little scope to innovate within the area of STO listing or secondary market trading of security tokens, and opined that legal requirements relating to settlement would possibly impede the application of DLT. On the other hand, a respondent maintained that it is not necessarily the case that the legal requirements regarding settlement may impede the application of DLT, and noted that, in theory, some of the services provided by CSDs as defined in CSDR could be provided through the use of smart contracts. This would facilitate the CSD's functions and allow for better post-trade flows. However, they also noted that while a harmonised regulatory landscape at EU level can be achieved through existing legislative tools, global settlements may require a greater effort among jurisdictions.

A respondent maintained that the integration of a decentralised concept within the ambit of a centralised-focused regulation poses challenges to regulators, but opined that if a 'point of reference' infrastructure (such as a local forensic node) is implemented, adherence to CSDR would be facilitated.

Some respondents also noted that DLT has the capacity to take over functions which previously required the services of a centralised third party, such as the central maintenance of the depositary or registry and the notary service. In the light of this, a respondent suggested that the concept of a CSD being strictly limited to a legal entity such as a CSD may become outdated.

Two respondents noted that compliance with the legal requirements to maintain a CSD on a DLT exchange would be greatly cumbersome and may create new expenses and obligations, thus revisions in the legislation may be required.

A respondent highlighted a number of incongruences between wholly decentralised peer-to-peer systems and CSDR which essentially relies on a centralised legal entity. Firstly, they noted that the definition of a securities settlement system ('SSS') will not capture peer-to-peer platforms since the

definition itself notes that there needs to be a formal arrangement between three or more participants. Thus, they proposed that a centralised or decentralised exchange which is operated by an operator would qualify as a settlement internaliser since in their view there are no legal requirements imposed on a settlement internaliser that cannot be fulfilled by an operator of a decentralised exchange.

A respondent suggested that CSDs should apply DLT as part of their operating procedures. If Malta is able to license such a CSD, it would be the first of its kind in the EU to offer such a service to local and EU-based STOs.

Question 19	Do you agree that the CSDR implicitly implies that a centralised concept is required? If not, how could a decentralised concept be adopted to ensure adherence with the CSDR requirements?

This question elicited mixed responses from respondents, but the majority acknowledged that the CSDR was drafted with a centralised authority in mind. However, a number of respondents proposed that a decentralised concept could be adapted to coexist within the current legal framework. Respondents gave various interpretation as to how this can be done.

A respondent maintained that if the understanding of centralised and decentralised exchanges provided by the Authority in Section 4.1 of the Consultation Document was to be applied to the settlement function, CSDs are to be considered centralised since they must retain custody of funds in order to perform the clearing and settlement of tradable securities by transferring cash. The respondent equated the holding of funds with the custody of tokens. The aforementioned section was interpreted by another respondent to infer that through the possibility of automating the settlement process on a decentralised exchange, the CSD's task will be facilitated.

A respondent, who agreed that CSDs were envisaged as centralised and permissioned entities, opined that a decentralised model could be feasible where permission-based arrangements are utilised, but maintained that certain activities will need to be carried out in a separate centralised environment. Another respondent also agreed that a permissioned decentralised system may be adopted by utilising a settlement internaliser which is to report to a CSD.

Another respondent asserted that it is immaterial whether a centralised or decentralised model is adopted since focus should be placed on the structure of the tokens.

Question 20	To what extent do you believe that DLT would be used for settlement purposes? Do you believe that settlement is an integral part for a DLT system to succeed, or would a central maintenance service / notary service be sufficient?

All respondents agreed that settlement is an integral part for a DLT system to succeed since it represents a cornerstone element of investor protection within the securities trading. Respondents to this question provided various insights as to which services which are traditionally carried out by a CSD can be automated through DLT. One respondent noted that without settlement on the DLT platform, market participants will lose interest in security tokens.

A respondent advocated against a prescriptive or singular approach towards which services can devolve onto a DLT system but noted that the appropriateness of a particular service line should be examined in light of an applicable business model.

Another respondent opined that for a DLT exchange to succeed as a DLT system, it should offer a central maintenance service, a notary service, ensure settlement finality in terms of the SFD, and provide for correctability, i.e. the possibility of reversing a transaction. The need for correctability was also supported by another respondent who noted that where a private ledger is operated by a central body, revoking a transaction will be a relatively easier exercise.

It was also proposed that the Authority should introduce guidelines on locking funds on the time of investigation and assign an authority whose decision would be the basis for revoking a transaction.

One respondent opined that DLT exchanges will seek to carry out settlement on their own platforms, without the need to involve a third party to perform the notary service since this would defeat one of the main benefits of DLT.

Another respondent posited that the notary service and the central maintenance service have a traditional and restrictive meaning in the CSDR, thus DLT cannot replace these two core CSD services entirely without imposing relatively high costs. Nonetheless, they maintained that DLT will have a crucial role to play in improving the quality and efficiency of the settlement infrastructure; however, the current legislative framework shall need to be amended to cater for scenarios where DLT is used.

A respondent noted that the use of DLT for settlement purposes will provide a solution to a number of international settlement problems which are currently experienced.

Question 21	What are your views in relation to a DLT operating a settlement internaliser activity? In the event that settlement is carried out through a settlement internaliser rather than a CSD, how would the systemic risk associated with participation in payment and SSSs be reduced?

Respondents shared varied views with respect to the possibility of a DLT operating a settlement internaliser activity.

A respondent opined that while a centralised exchange can perform the role of a settlement internaliser since it can deal on own account, a decentralised exchange would not be able to fulfil this function since buyers and sellers would carry out trades on a peer-to-peer basis. Another respondent also shared the view that an autonomous DLT-based platform cannot operate a settlement internaliser activity but founded this view on the basis that a settlement internaliser needs to be a licensed credit institution or a MiFID II investment firm. The latter argued that a settlement internaliser could operate a DLT system and ensure compliance with the relevant criteria and obligations.

Three respondents were of the opinion that the DLT platform itself can act as a settlement internaliser, thus meeting the settlement requirements set out in the CSDR. A respondent posited that the collection of the quarterly data required in compliance with Article 9 of CSDR can be automated.

Respondents also had different views with respect to the mitigation of systemic risk associated with participation in payment and SSSs. Respondents argued that the technology integrated into the DLT should ensure more efficient settlement through the implementation of technical solutions within the DLT's infrastructure. Another respondent highlighted the need for robust governance frameworks to mitigate risks, particularly in view of the fact that settlement internalisers are not subject to certain safeguards found in the CSDR and the SFD. One respondent argued that no additional risks posed by the settlement internaliser (whether it operates a DLT or otherwise) are foreseen as opposed to a CSD since such risks already exist today in a non-DLT context.

Question 22	In instances where a DLT would be operating as a settlement internaliser, who is expected to ensure the integrity of the issue? Similarly, who would be considered to be responsible with respect to safekeeping of securities and the management of the rights and obligations related to such securities?

Respondents provided highly-varied replies as to who should be responsible for the integrity of the issue, the safekeeping of securities and the management of the rights and obligations related to such securities where a DLT would be operating as a settlement internaliser.

Some of the respondents indicated that the DLT platform itself can ensure integrity of issue, for example, through the use of smart contracts. This view was supported by two respondents. However, no details were provided on the manner in which this would operate in practice.

A respondent suggested that the operator of the permissioned DLT platform can also be tasked with double checking verifications of transactions carried out on the DLT platform and the reporting of such verifications to the CSD. Another respondent opined that the DLT platform itself, or the natural or legal persons who operate it, should take responsibility for integrity of the issue if the platform itself clears and settles transactions. This view was supported by two other respondents. One of these respondents noted that where a settlement internaliser is operating the DLT platform, it would be expected to ensure integrity of settlement, safekeeping of securities and management of rights and obligations in relation to the securities which it holds for clients. The respondent also noted that decentralised exchanges where no operator can be identified will not be able to operate under the existing legal framework.

A respondent suggested that the management of rights and obligations related to securities should be the responsibility of the person in possession of the token. Where a custodian is used, the respondent proposed that the exchange should ask specific questions to the investors and should act with a power of attorney. Where investors retain direct possession of the token, the board of directors of the entity issuing the token should be ensuring proper communication with the shareholders.

Question 23	What are your views in relation to the notion of legal certainty discussed in paragraph 6.2? How can this uncertainty be mitigated or clarified?

A number of respondents agreed with the Authority that the governing law should be the law of the jurisdiction of the CSD, or the law of the place of the relevant intermediary, i.e. the law of the securities account to which the relevant securities are credited (through the application of the principle of Place of the Relevant Intermediary Approach ('PRIMA')). Indeed, a respondent noted that since there is no private international law solution to date on the matter, PRIMA should continue to apply. Another respondent was in favour of using the law of the location of the DLT exchange since it is easily determined, and it especially concerns the jurisdiction since the order is placed therein.

Another respondent proposed various alternatives in relation to the governing law depending at which level the DLT is being utilised. They proposed that where an Issuer issues securities on its own blockchain and does not intend to list the securities, the governing law should be the law of the Issuer; where an STO is issued on a third-party DLT, and the tokens shall not be listed, the applicable law should be the law of the operator of the platform since the wallets on which the tokens are held are part of the infrastructure provided by such operator, and where the security tokens are traded on a decentralised exchange, the governing law should be the law of the operator of the exchange.

A respondent proposed alternative solutions wherein the participants sign a governing law clause, or the CSD is integrated as one of the members on the DLT in order to bind everyone by the same law, but ultimately noted that their preferred solution would be to opt for the law of the jurisdiction of the CSD.

Another respondent proposed that a legal entity can be created in Malta which would be entitled to issue and control the tokens, and thus would be subject to Maltese law.

Question 24	What are your views on the issues highlighted under section 6.3 relating to securities accounts? Such views should also consider instances where the DLT arrangements are acting as settlement internalisers.

Respondents had varied views in relation to the issues relating to security accounts which were highlighted in the Consultation document.

Two respondents expressed the view that the central maintenance service, which is a core service in terms of CSDR, can be catered for by the DLT itself since nodes can record transactions on blocks which comprise the blockchain, thus replicating the function of a securities account. One of these respondents noted that securities accounts could be substituted in full by blockchain wallets. Where security tokens are issued as representations of traditional securities (i.e. the DLT-enabled tokens are not securities in and of themselves, but mere representation of a security), the respondent argued that a link between the wallet and the securities account should be established in order to ensure legal certainty over the title of the security, without recognising the wallet itself as a securities account.

Another respondent noted that it is crucial that a company is in possession of an updated ledger with a list of all members of the company at all times and argued that benefits of DLT can be leveraged to facilitate this task. They suggested that this can be done either through the use of a centralised platform whereby clearing and settlement is done through a settlement internaliser or through a CSD which is part of the DLT system which has one central ledger which is automatically updated. Alternatively, this can be done through the use of a forensic node within a decentralised permissioned platform. The forensic node would have priority and control over other nodes and could be considered as a register of members. The forensic node could also give direct access to the authorities or authorised persons such as supervisors and licensed CSDs. Another respondent agreed with this point and noted that a 'golden record' could prove to be a solution, provided that an interconnected ecosystem is created.

1.5.1. **MFSA's Position in relation to Questions 18**-24 on Settlement

A brief on the role of CSDs

In the light of this discussion, it would be important to clarify the role of a CSD in the maintenance of post-trade infrastructures, and to shed light on the systemic importance of a SSS which is operated by CSDs.

CSDs perform three main core services, namely:

1. operating a SSS ('settlement service');
2. recording newly issued securities in a book entry system ('notary service'); and
3. providing and maintaining securities accounts at the top tier level ('central maintenance service').

In order to qualify as a CSD under the CSDR, an institution needs to operate a SSS, and provide at least one of the other two core services i.e. the notary service and the central maintenance service. The core services operated by CSDs give market participants confidence that securities transactions are executed properly and in a timely manner, even in periods of extreme stress. Moreover, by virtue of CSDR, CSDs can also perform certain non-banking ancillary services as well as non-banking-type ancillary services that do not entail credit or liquidity risks.

The function of a SSS is to facilitate the mobility of securities by enabling the transfer of securities between buyers and sellers. Since CSDs hold a position of trust, they are subject to onerous requirements to ensure settlement finality of transactions. CSDs need to ensure that financial product transfers and payment orders can be finalised, thus minimising a number of risks in relation to the insolvency of a participant. This is most commonly done through what is known as delivery-versus-payment ('DvP'), a method of settling transactions which allows for the simultaneous delivery of financial assets to the buyer against cash payment to the seller. If transactions are not settled within the time period stipulated in the CSDR, CSDs must report failed settlement transactions to their NCA. CSDs also provide for the integrity of a securities issue by hindering the undue creation or reduction of issued securities, thus maintaining investor confidence in the securities markets.

Nonetheless, CSDs are not the only institutions which settle transactions. The CSDR envisages the possibility of setting up settlement internalisers which execute transfer orders on behalf of clients or on their own account other than through a SSS. A settlement internaliser can be any institution, including a licensed credit institution or investment firm.

The importance of a CSD's public interest function should not be discounted, which is why CSDs are subject to stricter governance requirements than credit institutions, and to the oversight of central banks.

The role of CSDs within the context of Maltese Law

CSDs also play an important role in relation to a plethora of civil and criminal issues which arise in relation to securities. We have envisaged a number of scenarios where it is unclear how a DLT can perform services which are currently being performed by the CSD. By way of example, where garnishee orders have been imposed on the financial instruments of a particular investor, CSDs are required to record the execution of such garnishee orders against holders of securities upon being instructed to do so by Issuers after these have been served with the garnishee orders themselves. CSDs must ensure that no dividends or interest payments are executed in respect of any holdings of securities against which a garnishee order has been recorded. Along the same vein, where pledges are imposed against an investor's securities account, CSDs are required to record the details of any pledges registered against a pledgor's account. To date, the automation of these processes cannot be envisaged because human intervention cannot be completely done away with. Even if smart contracts were to be employed to digitally impose restrictions on a tokenised security, there are situations where an 'if-this-than-that' logic will not adequately address the situation, for example when a certain result is dependent on the conclusion of court proceedings.

Other issues arise when financial instruments need to be transferred by virtue of a causa mortis or are subject to litigation in relation to unresolved estates. To date, CSDs play an integral role in such causa mortis transfers which require a private writing and the completion of a share transfer form in terms of Article 118 of the Companies Act.

Considerations on the feedback received

The industry can appreciate that any proposed system for settlement, irrespective of the technology being used, should at a minimum be able to provide for the same safeguards as envisaged and mandated by the CSDR. Within the context of a decentralised DLT-based system, we understand that a system can be theoretically designed in such a way as to adhere with the CSDR's obligations through technological solutions such as smart contracts and forensic nodes.

However, in practice, a number of concerns arise which need to be addressed when secondary market trading is involved.

The CSDR expressly sets out a requirement for securities which are traded on trading venues to be recorded in book entry form in a CSD. Respondents to our consultation document identified this

requirement as one of the largest inhibitors to the use of DLT-based systems since it renders the benefit of using the DLT as an immutable ledger redundant when it comes to secondary market trading. Moreover, all respondents expressed the view that a DLT system would need to cater for settlement in order to succeed as a securities trading platform. The respondents also listed other services and settlement mechanisms which they deemed to be integral to the success of such platforms, including novel mechanisms such as the possibility to reverse transactions on a DLT.

The qualification of a DLT system itself as a CSD or as a settlement internaliser was also discussed at length by respondents. In its *Advice on ICOs and Crypto-Assets*, ESMA had reiterated that fulfilling this requirement might not be feasible since it would require either the DLT to seek authorisation as a CSD, which would raise a plethora of legal issues and be overly onerous for the Issuer, or pass on information to the CSD, potentially by on-boarding the CSD as one of its nodes, which may not be practically feasible for CSDs.

Respondents proposed an alternative solution where a DLT platform is classified as a settlement internaliser. This argument was based on the fact that a decentralised DLT system allows peer-to-peer trading without the inclusion of a third party, thus, the platform cannot qualify as a SSS since the latter necessarily requires three or more participants in a system.[30]

Whilst a settlement internaliser may provide a solution in theory, it should be noted that Article 3(2) of CSDR requires that transferable securities admitted to trading on a trading venue are required to be recorded in book entry-form in a CSD. Accordingly, it appears that the CSD cannot be totally removed from the ecosystem of a traded STO.

In this respect, it is also important that investors are aware that transactions which are settled through settlement internalisers may not have the safeguards set out in CSDR and SFD, *inter alia* in relation to settlement finality.

Moreover, this scenario would also imply the need for the DLT to have a direct[31] or indirect[32] connection with the relevant CSD wherein the transferable securities in question have been recorded. If the DLT becomes a participant in the SSS operated by the CSD, it would also need to comply with the participation and the reconciliation requirements set out in CSDR.

[30] 'Securities settlement system' means a system under the first, second and third indents of point (a) of Article 2 of Directive 98/26/EC that is not operated by a central counterparty whose activity consists of the execution of transfer order.
[31] The DLT network would be a participant in the SSS operated by the CSD.
[32] Via a participant in the SSS.

This issue is currently being explored further by the Authority in order to understand the risks which would emerge and how these can be mitigated if a settlement internaliser is opted for. Ensuring integrity of the issue will also require further evaluation where the DLT qualifies as a settlement internaliser, since current institutions which qualify as a settlement internalisers are not under the obligation to ensure integrity of issue, but merely to report quarterly aggregate internalised settlements.

Potentially, a CSD operating its own DLT could be used by Issuers in order to record their securities. Such a solution would harness the benefits of DLT without the need to work around the current framework.

Additionally, it should be noted that much of the discussion in relation to settlement has focused on the securities leg of the transaction, and little consideration has been given to the cash-leg of a transaction. The International Securities Services Association ('ISSA') has prepared a highly detailed document named *'Crypto-Assets: Moving from Theory to Practice'* wherein it explored salient practical inhibitors to the adoption of DLT within the context of the securities market. The ISSA opined that there are two solutions to the settling of the cash lag of a transaction. Settlement can either happen off-chain through the use of commercial or correspondent banks which have access to the real-time gross settlement system which is operated by a central bank, but argues that this option still creates counter-party risk which will need to be managed by the operators or the users of the DLT network.

Alternatively, a DLT network can opt for on-chain settlement of the cash leg of a transaction through the use of separate payment tokens or stable coins which are exchangeable between accounts on the distributed ledger, thus allowing transactions to be settled immediately through the exchange of security tokens and payment tokens. The drawback of this system is that both security tokens and payment tokens would need to be available for delivery when the trade is matched prior to settlement, this requiring the pre-funding of accounts before the start of trading. This would create a new liquidity problem for markets which is not experienced by the existing securities markets today where the funding and positioning for settlement can be arranged post the execution of the transaction. In turn, this system would stifle market-makers which are the primary source of liquidity within most securities markets, and hinder the applicability of certain techniques such as short-selling, securities financing, back-to-back trades, block orders to buy or sell large numbers of securities, and pre-trade allocations to customer accounts as orders are fulfilled which aid the markets to maintain their liquidity. The Authority is in general agreement with a number of respondents who opined that the lure of STOs lies in increased liquidity and the ease of transacting. Thus, the Authority believes that these issues will need to be ironed out before secondary market trading for tokenised securities can take off.[33]

[33] ISSA, 'Crypto-Assets: Moving from Theory to Practice' (November 2019)

To date, the Authority has not received concrete business proposals seeking to provide such a solution to the industry. In a report issued by ESMA in July 2019 on the licensing of FinTech business models, ESMA asked NCAs to indicate the type of authorisations held by the regulated FinTech firms in their jurisdictions, and it resulted that only an estimated 0.7% of all regulated FinTech firms in the EU perform counterparty clearing or operate a CSD.[34] Therefore, while DLT may have gained traction within the context of primary market security issuances, the use of DLT within the context of secondary markets will be hindered by the lack of availability of institutions which are capable of providing settlement for tokenised transferable securities.

Until such time as the European legislator intervenes in order to amend certain provisions in CSDR, there is common consensus that some benefits of DLT will be lost in order to ensure compliance with current regulation. ESMA is also aware of this situation and has recently reiterated the need to amend and adapt existing regulations to new business models in order to provide for clearing and settlement on blockchain and the authorisation of a CSD based on blockchain technology.

Apart from a regulatory effort on behalf of the European regulator to amend provisions which are stifling further development in this area, it should be noted that for DLT to succeed within the ambit of the securities markets, inter-operability between the old markets and the new markets utilising DLT, as well as interoperability between different types of technologies and DLTs utilised will be a very important challenge to overcome. This will entail the creation of common standards to automate the way that information is exchanged between different parties in the securities value chain[35].

[34] ESMA 'Report - Licensing of FinTech business models' (12 July 2019, ESMA50-164-2430)
[35] Ibid, ISSA (n 29).

2. MFSA's Position

Defining STOs	
Categorisation of STOs	The Authority understands that the definition of transferable securities in Article 4 (1) (44) of MiFID is construed very broadly and is loosely defined at EU level, and in fact it is not harmonised within the laws of the Member States. In this respect, the MFSA has identified the need to provide guidance on the interpretation of what constitutes transferable securities, by delving into the three formal requirements which are required for an instrument to qualify as such, namely, [i] transferability; [ii] negotiability on the capital markets, and [iii] the creation of a class of securities.
Limitation of the issuance of STOs to companies	The Authority noted that market participants did not provide viable justifications why the Authority should allow other structures besides companies to issue STOs. Accordingly, for the time being the MFSA's approach to limit traditional STOs to companies remains unchanged in this regard.
Amendments to the Companies Act	Following feedback received from the industry, the MFSA will be liaising with the Malta Business Registry in order to amend the relevant provisions of the Companies Act, particularly in order to ensure that the registers of members and debenture-holders can be kept in a dematerialised form, using DLT. Having said that, we are of the view that Maltese corporate law is structured in a way to give companies discretion when it comes to the drafting of the memorandum and articles of association.
FDDR	The MFSA confirms that the requirement to draw up an FDDR should be the same for the same type of securities, irrespective of whether these are tokenised or not.

Corporate Governance Requirements	Most respondents were in agreement with the additional corporate governance requirements recommended by the Authority. Accordingly, the Authority confirms the additional corporate governance requirements as proposed in the Consultation Document, including the requirement of a systems audit. These will assist Issuers in the fulfilment of their duties in terms of company law.
Prospectus Regulation Requirements	The Authority confirms that the Prospectus Regulation and the relevant Annexes are adequate in the case of STOs.

Additional Ongoing Obligations

Systems Audit

In order to avoid the risk of regulatory arbitrage between the treatment of different regulated DLT Assets, and in view of the fact that the underlying technologies and ITAs which are being used within the context of initial VFA offerings and STOs present the same risks, the Authority would like to restate and clarify its new position in relation to the proposed requirements:

1. A Systems Auditor will need to be appointed if the Issuer has an ITA in place; or if the Issuer operates a technological infrastructure which interacts with an ITA in some way or form, including *inter alia* a wallet.

2. Where a company will be operating an ITA which underpins the storage and transactions in securities, a Systems Auditor will need to be appointed to prepare a Systems Audit Report in line with the MDIA's Guidelines.

The MFSA proposed that where the company itself operates the underlying DLT, the company is required to prepare annually a Type 2 Systems Audit. Whilst the majority of respondents agreed that a systems audit is required, a number of respondents noted that a requirement to prepare an annual Type 2 Systems Audit would be burdensome for operators. Taking into

account our understanding that the underlying technology underpinning the Issuer's business presents significant risks to investors, the MFSA has reconsidered its proposal in relation to the requirement of a Type 2 Systems Audit where the company operates its own native ITA. Instead, a requirement to appoint and have in place a Systems Auditor at all times shall apply where the Issuer has an ITA in place, or if the Issuer operates a technological infrastructure which interacts with an ITA in some way or form.

Companies Operating DLT	The Authority does not intend to limit offers to the public made by Issuers operating their own DLT from attaining the necessary authorisation from the Listing Authority to list their securities on a secondary market.

Secondary Markets

Permission-less Decentralised Exchanges	The majority of respondents agreed that permission-less decentralised exchanges could pose difficulties in ensuring compliance with the transaction reporting requirements contained in MiFIR, nevertheless the Authority does not intend to impose an outright prohibition on decentralised exchanges.
Trading of Traditional STOs	Whilst existing regulations provide for a high degree of intermediation within the current securities value chain which has been criticised over the years, one cannot overlook that some level of intermediation is in fact necessary. In this respect, the Authority believes that full disintermediation would not be an optimal solution. This is in line with the majority of responses which were in agreement with the MFSA's proposal that traditional STOs should be traded on either a centralised exchange via investment firms (with the possibility of investment firms granting DEA) or on a decentralized exchange with investment firms granting DEA.

Centralised or Decentralised but Permission-based Trading Platforms	The MFSA agrees with the feedback received and is of the view that both centralised as well as decentralised but permission-based trading platforms (hybrid platforms) could provide a workable solution. In light of the varied responses received, the Authority notes that the industry remains divided on the approach which the regulator should take in relation to centralised vs decentralised exchanges. The Authority reiterates the position expressed in relation to the MIFID framework and concludes that a case-by-case analysis based on the proposed business model will be needed.

Market Abuse Regulation

Transparency/Transaction Reporting	The majority of respondents appreciated the importance of transaction reporting as a means to detect financial market abuse. The Authority will explore further how best exploit the use of blockchain in its market oversight function in order to prevent and detect market abuse.

Post-Trade Settlement

Applicability of the CSDR	A number of respondents expressed the view that the legal requirements set out in CSDR in relation to settlement may impede the application of DLT unless a number of challenges are addressed, or the current legislation is optimised to embrace the use of DLT within the settlement process. Whilst a settlement internaliser may provide a solution in theory, it should be noted that Article 3(2) of CSDR requires that transferable securities admitted to trading on a trading venue are required to be recorded in book entry-form in a CSD. Accordingly, it appears that the CSD cannot be totally removed from the ecosystem of a traded STO. Nevertheless, this issue is

currently being explored further by the Authority in order to understand the risks which would emerge and how these can be mitigated if a settlement internaliser is opted for.

It was also noted that much of the discussion in relation to settlement revolved around the securities leg of the transaction, and little consideration has been given to the cash-leg of a transaction. The Authority believes that in this respect, certain issues would need to be resolved before secondary market trading for tokenised securities can take off.

All in all, it appears that while DLT may have gained ground vis-a-vis primary market security issuances, the use of DLT within the context of secondary markets will be hindered by the lack of availability of institutions which are capable of providing settlement for tokenised transferable securities. In this regard, pending proper intervention from the European legislator to amend certain provisions in CSDR, there seems to be common agreement that some advantages of DLT will be lost in order to ensure compliance with current regulation.