Luxembourg, June 18th, 2021

Introduction

The Association of the Luxembourg Fund Industry (ALFI) represents the face and voice of the Luxembourg asset management and investment fund community. The Association is committed to the development of the Luxembourg fund industry by striving to create new business opportunities, and through the exchange of information and knowledge.

Created in 1988, the Association today represents over 1,500 Luxembourg domiciled investment funds, asset management companies and a wide range of business that serve the sector. These include depositary banks, fund administrators, transfer agents, distributors, legal firms, consultants, tax advisory firms, auditors and accountants, specialised IT and communication companies. Luxembourg is the largest fund domicile in Europe and a worldwide leader in cross-border distribution of funds. Luxembourg domiciled investment funds are distributed in more than 70 countries around the world.

Please kindly note that these positions/opinions are not specific to any organizations (nor ALFI as an organization), but are the thoughts and observations of the ALFI ad hoc working group "Digital Finance Strategy" in relation to the industry in general. Therefore, these opinions and observations expressed in this paper about the industry belong to the ALFI ad hoc working (which was the outcome of a group discussion about the industry) and not to the authors' employer, organization, committee or other group or individual."

Definitions

ABBL	Association des Banques et des Banquiers, Luxembourg
AIFMD	Alternative Investment Fund Managers Directive
AML	Anti-money laundering
CBDC	Central bank digital currencies
CFT	Combating the Financing of Terrorism
CNPD	National Data Protection Commission
CSD	Central Security Depository
CSDR	Central Security Depository Regulation, Regulation on improving securities settlement in the European Union and on central securities depositories and amending Directives 98/26/EC and 2014/65/EU and Regulation (EU) No 236/2012
DLT	Distributed Ledger Technology

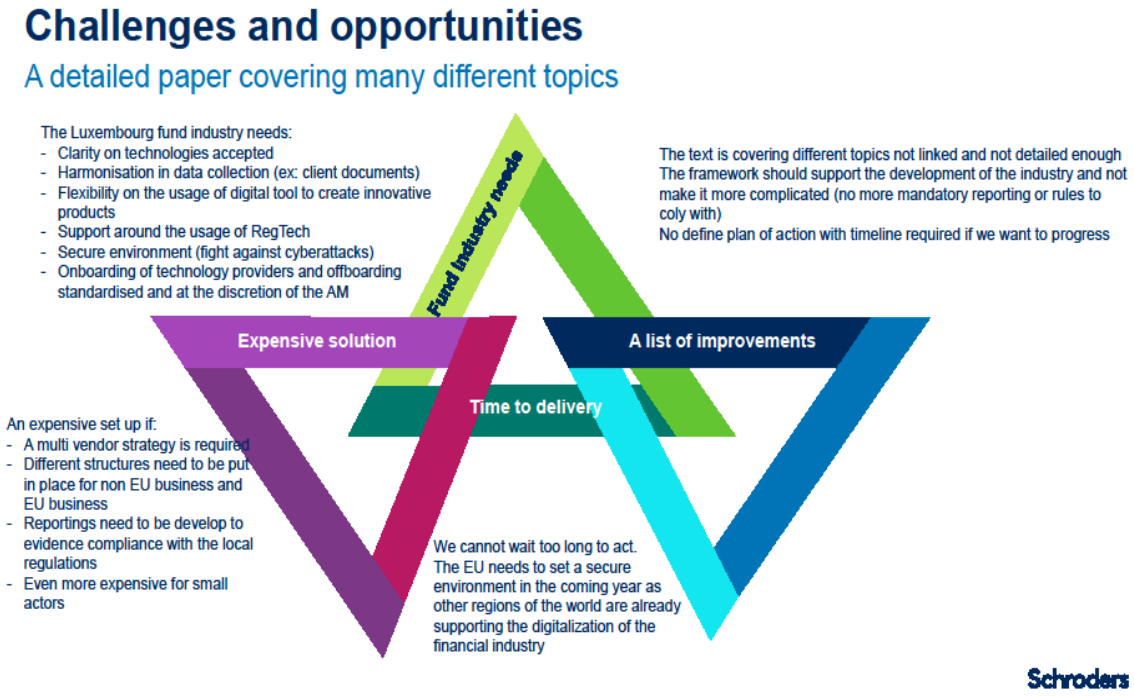
DLT MTF	Distributed Ledger Technology Multilateral Trading Facility
DORA	Proposal for a Regulation of the European Parliament and of the Council on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014
EBA	European Banking Authority
ECB	European Central Bank
EIOPA	European Insurance and Occupational Pensions Authority
ENISA	European Union Agency for Cybersecurity
ESA	European Supervisory Authorities
ESMA	European Securities and Markets Authority
EU	European Union
FMI	Financial Market Infrastructure
ICT	Information and Communication Technology
ICT TPP	Information and Communication Technology Third Party Providers
KYC	Know Your Customer
MiCA	Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937
MiFID	Markets in Financial Instruments Directive
MTF	Multilateral Trading Facility
NCA	National Competent Authorities
Pilot Regime or MI/DLT	Proposal for a Regulation of the European Parliament and of the Council on a pilot regime for market infrastructures based on distributed ledger technology
PRR	Pilot Regime Regulation (see Pilot Regime or MI/DLT)
SFD	Settlement Finality Directive, Directive 98/26/EC of the European Parliament and the Council of 19 May 1998 on settlement finality in payment and securities settlement systems

SSS	Securities Settlement System
UCITS	Undertakings for the collective investment in transferable securities

ALFI's position on MiCA, DORA and the Pilot Regime

ALFI acknowledges the increasing use of digitalisation in the financial sector not only in Luxembourg but also in Europe and worldwide. ALFI observes digital innovation trends offering new opportunities for the finance sector. The digitalisation transforms the finance sector at different levels including notably at investment and trading levels with investments in crypto-assets or the use of distributed ledger technology and at operational level with the increase for a need of operational resilience.

ALFI recognizes that together with the increase of digitalisation, risks and challenges may emerge and need to be addressed via a proportionate regulatory framework. Further, ALFI agrees with the European Commission priorities to make Europe fit for the digital age and to build a future-ready economy so as to embrace the digital revolution, making the benefits of digital finance available to consumers and businesses.



Source: Schroders.

ALFI welcomes the three proposals for Regulations of the European Commission being parts of the digital finance package, a package of measures to further enable and support the potential of digital finance in terms of innovation and competition while mitigating the risks arising from it:

- Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937[1] (**MiCA**);
- Proposal for a Regulation of the European Parliament and of the Council on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014[2] (**DORA**); and

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0593.
[2] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0595.

- Proposal for a Regulation of the European Parliament and of the Council on a pilot regime for market infrastructures based on distributed ledger technology[3] (**the Pilot Regime**).

ALFI reviewed the abovementioned proposals of the European Commission in their version available on EUR-Lex and identified the following considerations from the perspective of the Luxembourg investment fund industry. For that purpose, ALFI also took into account the feedback and comments from the ABBL.

[3] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0594.

REGARDING THE MiCA[4]

The regulation proposal aims to develop a sound legal framework that brings legal certainty for issuers and service providers of crypto-assets falling outside existing EU financial services legislation. The general approach is based in particular on the "same activity, same risk, same rules" principle and on a proportionality principle, with requirements commensurate to the risks created by the crypto-assets at stake and the services provided in connection with them. The proposed taxonomy, in relation with these principles, allows establishing bespoke regimes, adapted to each of the different categories of assets thus defined.

From a general standpoint, this proposal is an appropriate response to some of the main issues and challenges raised by crypto-assets (that do not qualify as MiFID financial instruments nor as central bank digital currencies - CBDC), in particular with regard to global stable coins: market integrity, investors and consumer protection, anti-money laundering, financial stability, monetary policy transmission and monetary sovereignty. The proposal could, however, be supplemented in certain respects.

ALFI agrees with ABBL that a market abuse rule could be implicated, especially referring to crypto asset markets (e.g. requirements relating to the disclosure of inside information as well as prohibitions on insider dealing, unlawful disclosures of insider information and market manipulation).

There is a potential legal uncertainty how custody provisions under MiCA correspond to custody provisions under AIFMD or UCITS Directive, being financial instruments or not.

Global consistency and cooperation with third countries

While crypto-assets regulation at EU level is indispensable, it is also important to ensure a certain degree of regulatory consistency at international level, to avoid potential regulatory arbitrages based on inconsistencies between jurisdictions. It is even more an issue as transactions related to crypto-assets are not likely to have geographical boundaries. The proposal does not address the subject of the cooperation of the EU with third country authorities and it does not include a clear and comprehensive third country regime.

Article 3: Definitions

Article 3 (1, (3) (4)) defines "asset referenced token" and "electronic money token". ALFI agrees with ABBL's view that the definitions are practically identical, the only difference being to limit the reference asset for Electronic Money Token to a single fiat currency. These definitions should be differentiated.

Scope: Definitions and clarification of the notion of crypto-assets

Article 3 includes a list of definitions of key terms, such as DLTs and crypto-assets. In order to capture all crypto-assets and be future-proof, those definitions are not very granular. However, the absence of granularity of certain definitions (DLTs and crypto-assets) may raise legal uncertainty. Article 3 (2) says that a crypto-asset is a digital representation of value or rights which may be transferred and stored electronically, using distributed ledger technology or similar technology.
In particular, if the aim of MiCA is to regulate all crypto-assets that do not qualify as a financial instrument under MiFID, then having a clear and harmonised definition, at EU level, of what constitutes a crypto-asset is necessary to gain certainty on the scope of MiCA.

ALFI also assents to the ABBL's proposal for a definition of token to the MiCA proposal.

Programmable money and smart contracts

Although it is acknowledged that the aim of the MiCA proposal is to remain technological neutral and to regulate the functionalities and responsible actors rather than the methods used to provide a certain service, ALFI notes that MiCA does not include any provision regarding the use of smart contracts in connection with crypto-assets. But, "programmable money" could lead to important changes in the financial sector. Smart contracts will allow to specify both (i) the characteristics of programmable money

[4] All Articles in this section without reference to respective regulation refer to the MiCA.

and (ii) the conditions of the transactions. Terms and conditions would be programmed according to how the parties want to transact. They would be part of the money from issuance through all stages of the transactions (secure, verify and authorize). From a financial standpoint, prudential and accounting issues should be properly addressed, as well as AML issues. From a legal standpoint, the issue of compatibility between smart contracts and traditional contracts should be assessed.

Public and private DLT

MiCA does not make a clear distinction between:

- private, proprietary and permissioned DLTs (i.e. DLT which are managed by a legal person and whose access is permissioned and subject to specific conditions); and
- public and permission-less DLTs (i.e. DLTs which are not managed by a legal person and whose access is free), such as Bitcoin or Ethereum.

While cross-reading the digital finance package, it is to note that Article 6 (2) of the Pilot Regime foresees that "*a CSD operating a DLT securities settlement system, and an investment firm or a market operator operating a DLT […] shall establish rules on the functioning of the DLT they operate, including the rules for accessing the distributed ledger technology, the participation of the validating nodes, addressing potential conflicts of interest, and risk management including any mitigation measures*". Such conditions of access may imply that only proprietary DLTs are allowed (which may be confirmed by the reference to "proprietary DLT" in recital 28 of the Pilot Regime).

Further clarification on this particular point will be welcomed in the MiCA proposal. This absence of distinction between the two types of DLTs raises legal issues, as MiCA remains silent on the responsibilities and governance of DLTs. This differentiation is also a key factor to assess and determine the liabilities of crypto-assets services providers.

ALFI considers that this could be alternatively dealt with at another legislative level (e.g. via the adoption of RTS/ITS (Regulatory Technical Standards and Implementing Technical Standards) based on the insight from ESMA and EBA).

Title III: Asset-referenced tokens

Title III deals notably with questions around the asset-referenced tokens like how the procedure for authority goes, which obligations there are for issues of asset-referenced tokens or which rules has to be followed for the acquisition of issues of asset-referenced tokens.

Financial stability and non-discriminatory access

The competition issues have important implications in terms of financial stability. In this respect, should a stable coin become a leading or even overriding source of payments, it would be critical for all players to have equal access to it, thanks to non-discriminatory agreements, to enable them to continue to serve their clients. The lack of access or a limited access to some tokens with substantial market shares could undermine systemic financial players, threaten the functioning of the payment system as a whole and thereby put at risk financial stability.

Article 17: Content and form of the crypto assets white paper for asset-referenced tokens

Article 17 (5) requires that the crypto-asset shall be made available in machine readable format. The question arises here with regard to crypto-assets which do qualify as a financial instrument if this requirement does not apply. The level playing field is at risk. ALFI shares ABBL's view that the costs have to be checked for these technological requirements to comply with Article 17 (5).

Article 39: Classification of asset-referenced tokens as significant asset-referenced tokens

The criteria as set out by Article 39 (1) and (3) have to be considered together with the cross-border nature of the Luxembourg financial sector. Specifically, with regard to article 39 (1) (e) the criteria of the significance of the cross-border activities of the issuer, which is not at all acceptable for financial sectors with an important cross-border activity as the issuer in these markets would rapidly/immediately qualify

as significant asset token issuers/promoters. This criterion should be deleted. ALFI agrees with ABBL stating that an assessment should be done with regard to the other criteria in order to know what the impact would be for the national financial sector.

Title IV: E-money tokens

Article 43: Authorisation

Article 43 of the proposal provides that electronic money tokens can be offered to the public in the European Union or admitted to trading on a crypto-asset trading platform only if the issuer is authorised as a credit institution or as an "electronic money institution" and notifies a white paper to the competent authority. However, under the same article, issuers of electronic money tokens will not be subject to this authorisation and to the obligation of the white paper "*if the average outstanding amount of electronic money tokens does not exceed €5 000 000*". This threshold of €5 000 000 is taken from the e-money directive (EMD). Article 9 of the latter provides that Member States may waive the application of all or part of the conditions set out in this directive "*if the total business activities generate an average outstanding electronic money that does not exceed a limit set by the Member State but that, in any event, amounts to no more than €5 000 000*".

However, if "conventional" electronic money is used strictly for payment purposes, it seems that e-money tokens could have a wider use. Indeed, with the proposed regulation, it will be possible to exchange e-money tokens on different platforms and potentially for other kind of tokens. It also seems that it will be possible to use e-money token for investment purposes. If the scope of "usages" is indeed wider, it means therefore that the exposure to risks will be greater than for conventional electronic money. For these reasons, this threshold should be lower than for the "conventional" electronic money, in order to deal with this higher level of risks. Beyond that question, the emergence of significant e-money tokens, benefiting from the network effect of some Bigtech leaders, combined with the creation of central bank digital currencies, such as the e-euro envisaged by the European Central Bank, would constitute a real paradigm shift and most probably a revolution for the financial system. It would create new challenges of system-wide importance and associated risks that would not be commensurate with those of traditional electronic money. Indeed, as rightly pointed out by the Financial Stability Board, it would have important implications for the funding of banks, and consequently on the ability of banks to finance the economy at a competitive cost. Indeed, if users hold e-money tokens permanently in wallets, "*retail deposits at banks may decline, increasing bank dependence on more costly and volatile sources of funding*". It would also create new major systemic risks, related to trust in fiat currencies, monetary policy transmission, monetary sovereignty and financial stability issues.

Given these risks, new in their magnitude and which are much more significant than those associated with "traditional" electronic money, it must be asked whether the prudential rules associated with the status of e-money institution under Directive 2009/110/EC are effectively proportionate and sufficient. In order to ensure a proportionate approach and in accordance with the "same business, same risk, same rules" principle, one can consider that issuers of significant electronic money tokens should at least be authorised under a distinct legal regime that would take into account these specific risks, if not authorised solely as credit institutions under Directive 2013/36/EU.

Title V: Authorization and operating conditions for crypto-asset services providers

Title V sets out the provisions on authorisation and operating conditions of crypto-assets service providers.

Wallet providers

MiCA does not provide for precise definitions of the different categories of services providers that may be used for the purpose of creating a wallet (as the case may be). From the ALFI perspective, it would be important to define in particular wallet providers and in which particular situation are wallet providers needed. There are only two parts in the MiCA where wallet providers are mentioned: in the introduction part referring to the impact assessments where it is just indicated that the risks, raised by wallet providers, should be covered and at the end of the proposal (expected results and impacts) where it is mentioned, that wallet providers are an important part of the crypto-assets.

When using crypto-assets, a wallet would be more than just a means of payment. A wallet would be closer to a bank account as it may contain a person's digital identity and allows to store incremental value and make transactions. However, it would literally be neither a physical account nor a digital account. A proper definition of wallet providers should allow to answer notably to the following questions:

- What are the links between wallets and bank accounts?
- Are wallet providers subject to AML/CFT and KYC requirements?
- Are stored assets with wallet providers written in their ledger and their balance sheets?
- Must wallets be located in the EU?

Article 67: Custody and administration of crypto assets on behalf of third parties

Article 67 is under Title V, Chapter 3 that deals with obligations for the provision of specific crypto-asset services. Article 67 itself regularizes the liability of the crypto-asset service providers authorised for the custody and administration of crypto-assets on behalf of third-parties. The Commission's objective of establishing clear liabilities is key in providing clarity and legal certainty to the crypto-asset ecosystem. However, in its current form the text could benefit from further clarifications: Service providers should take all appropriate measures to prevent the loss of, and ensure the safe return of their clients' crypto-assets or means to those crypto-assets.

However, cases may arise where independently of the provider's control, external events lead to the loss of the crypto-assets, or prevent their safe return to the client in a timely manner.

As such, regulation should reflect that providers of crypto-custody services should not be liable for events which lead to the loss or incapacity to return their clients' crypto-assets, when these events are neither directly or indirectly attributable to them, or are beyond their reasonable control.

This is particularly the case for crypto-assets based on public block chains or distributed ledger applications that are not under the service provider's control (e.g. smart contracts). Furthermore, while providers should be liable for the loss of clients' crypto-assets or the rights related to those assets "resulting from a malfunction or hacks up to the market value of the crypto-assets lost", the text does not clearly define these notions.

The notions of "malfunction" and "hacks" should be more accurately specified. Furthermore, if the provider is said to be liable "up to the market value of the crypto-assets lost", no details are given on the process of fixing market value. A solution could be to leave these aspects to be defined contractually through the service provider's custody policy. Clarifications on both these aspects would help increase legal certainty.

Role of custodians and depositaries

When using DLT, it seems possible to put an issuer in a direct relationship with its investors without any intermediaries. However, an investor that does not wish to have direct access to the respective DLT market infrastructure, but prefers indirect access via a custodian and use the latter's ancillary services should be able to do so. Offering direct access does not necessarily mean that investors should be forced to access the DLT market infrastructure directly, especially if they do not have sufficient level of ability, competence, experience or knowledge (see also Recitals 17 and 22). It should therefore be possible for an investor to use an asset service provider, such as a custodian, to access a DLT market infrastructure and to benefit from other services like reporting services, for instance, information, financial advice, tax-related services and so on. This should be reflected in the Pilot Regime accordingly.

EU policymakers should clarify the requirements related to custody, including:

- Whether assets held on a DLT MTF/CSD will be considered assets held in custody;
- The potentially broad liability imposed; and
- Whether the rules of AIFMD/UCITS on depositary liability for financial institutions would apply.

Clarifying these requirements will remove regulatory uncertainty and encourage intermediaries and professional investors to participate in the Pilot Regime. The definition of custody should also be applied consistently across MiCA and the Pilot Regime

Article 125: Transposition of amendment of Directive (EU) 2019/1937

In line with ABBL's comments, Article 125 provides for an extension of 12 months, the deadline could be aligned to 18 months, which seem sufficient. Market actors and stakeholders are already preparing for MiCA. That means a period of more than that (e.g. for 24 months) could prove too long as the technology, business plans, etc. could already have evolved beyond the scope of MiCA. The same applies to Article 123 (2) and Article 126 (2).

REGARDING THE DORA[5]

DORA is also a part of the digital finance package and deals in particular with the existing ICT risks. It aims to ensure that all participants in the financial system have the necessary safeguards in place to mitigate cyber-attacks and other risks. It will require all firms to ensure that they can withstand all types of ICT - related disruptions and threats.

Scope:

The DORA proposal focusses a lot on typical ICT controls and assessments, and does not mention social engineering and other risks specifically. Statistics show that the vast majority of cyber-attacks rely on social engineering techniques, which are designed to circumvent even the most robust ICT architectures. An EU cyber resilience framework should address these risks as well.

Article 2: Personal scope

ALFI agrees with the ABBL that the personal scope, especially also covering credit institutions, investment firms, crypto-asset service providers and credit rating agencies should not be extended. The sensitive groups of the financial sector, as the meaning and purpose of the regulations cover, are regulated. There is also no need for an extension of the personal scope by now.

The establishment of a central security repository of ICT incidents can be supported as long as such information is shared with participants. With a view of the costs coming along with this, there should be benefits for such participants such as ICT- and security information.

Article 3: Definitions

Article 3 includes the necessary definitions for the DORA. ALFI assents ABBL's opinion that these definitions should be reviewed again as they are partly incomplete or inconsistent with established lexicons.

For example, there is a definition of "information asset" in Article 3 (5) stating that "*information asset means a collection of information, either tangible or intangible; that is worth protecting."* This definition is self-referencing, because it explains the phrase with itself. ALFI shares ABBL's view that the definition could be clarified. The definition of "asset" being referenced in the cyber lexicon of the Financial Stability Board could be taken as a basis.

Microenterprises

Definition and threshold

Article 3 (50) defines "microenterprise" which means "*a financial entity as defined in Article 2 (3) of the Annex to Recommendation 2003/361/EC*."
Referring to the definitions there are exemptions for such microenterprises, for example in Article 5 (5), whereinafter it is said that financial entities "*other than microenterprises*" shall ensure appropriate segregation of ICT management function, control function, etc. (…).

The question at that point is, if the member states will agree on a specific threshold of microenterprises and how that will look like.

Proportionality

The idea of protecting smaller firms is worth supporting. ALFI agrees with this comment from ABBL. That also corresponds to the idea of "same activity, same risk, same rules." On the other side, the risk the different firms take should be the main point to take care of. That means that not the number of employees or the balance sheet should be the starting point; otherwise, there is much room for misuse or arbitrariness of such exemptions. Besides that the profile, developed by the industry, allows a proportional risk profile.

[5] All Articles in this section without reference to respective regulation refer to the DORA.

In conclusion, the definitions and even more the exemptions and their limit should be clearly defined and the criteria clearly described.

Article 5: ICT risk management framework

Article 5 (4) says: "*As part of the ICT risk management framework referred to in paragraph 1, financial entities other than microenterprises shall implement an information security management system based on recognized international standards and in accordance with supervisory guidance and shall regularly review it."*

According to the ABBL, the terms "*supervisory guidance*" and "*recognized international standard*" are not precise enough, because there is no differentiation between the varied firms and their specific needs referring to different possible risk managements. Meaning and purpose of the DORA is to ensure that firms are taking the actions appropriate and necessary to create a risk management with the necessary controls. ALFI also considers that the risk management framework shall be adapted to the size and business of the concerned firms to which these requirements are applicable. For example, the recommended "*multi-vendor strategy*" (Article 5 (9)) is an acceptable risk strategy, but it is only one of many risk tools and further strategies may need to be identified in that respect.

Article 5 (9) seems to indicate an additional control for financial institutions working with multiple vendors and not only with one. The institutions with such multiple vendors must explain the reason for that, whereas a single vendor does not have to do that.

Article 8: Protection and prevention

Referring to a risk-based procedure, ALFI shares ABBL's view that the requirement in Article 8 (3) to "*use of the art ICT technology and processes*" should be replaced by "*use a ICT and processes that are appropriate to the firms risk profile*."

Article 13: Communication

Article 13(1) foresees*: "As part of the ICT risk management framework referred to in Article 5(1), financial entities shall have in place communication plans enabling a responsible disclosure of ICT-related incidents or major vulnerabilities to clients and counterparts as well as to the public, as appropriate*."

The requirement to disclose to the public not only ICT-related incidents but also major vulnerabilities creates significant risk for firms. Major vulnerabilities are highly confidential as they represent a significant security risk to the firm. These should not be shared outside the firm. ALFI believes that the text should be changed to "major ICT-related incident".

Article 14: Further harmonization of ICT risk management tools, methods, processes and policies

Article 14 is not account for a risk-based approach nor innovation in cybersecurity. As Article 8 (4) requires, that firms shall have automated mechanisms that "*isolate information assets in the case of cyberattacks*", such a request could potentially lead to operational disruptions.

So, in accordance with ABBL's view, the Article 14 shall be reviewed again to make it more practicable and at least more fitting into the measures and purpose.

Article 17: Reporting of major ICT-related incidents

Article 17 regulates if and how major ICT-related incidents have to be reported by the financial entities. These information go to the relevant competent authorities, which brings risk for the financial entities depending on the used environment of the authorities.

Therefore, ALFI agrees with the ABBL that safeguards and careful controls would need to put in place by the relevant authorities before handling and sharing information on specific major ICT-related

incidents. Such reports can contain highly sensitive information related to the security of the firm which the firm should continue to control. Further, there is a risk of misunderstanding should only details of the full incident report be passed on by competent authorities as in Article 17(5). If the details are then further summarised and transmitted yet again as in Article 17(6) the risk of misunderstanding increases.

A preferred approach is for the competent authority receiving the report to determine if the report needs to be shared with additional competent authorities and subsequently, instruct the reporting firm to do so.

The time requirements in Article 17(3) (a) "*an initial notification, without delay, but no later than the end of the business day, or, in case of a major ICT-related incident that took place later than 2 hours before the end of the business day, not later than 4 hours from the beginning of the next business day, or, where reporting channels are not available, as soon as they become available*" are too short. The firms must be given more time to determine impact and therefore whether an ICT-related incident qualifies as major.

Article 17 (4) requires a delegation of the reporting obligation to a third-party service provider. The associated risk for the financial entities is estimable, but only if there is a notification of the third party service provider.

Article 18: Harmonisation of reporting content and templates

Article 18 deals with the demands referring to harmonisation of the regulatory technical standards or implementing technical standards with the ESA, ENISA and ECB.

That harmonisation should be supported, as long as the reporting remains to the local competent authority that shares it with its counterparts. The reporting harmonisation should replace, and not complement/extend, existing national reporting requirements.

Article 21: General requirements for the performance of digital operational resilience testing

Article 21(5) assumes that all weaknesses, deficiencies or gaps identified in testing should be fully addressed. Agreeing with ABBL, ALFI considers that this is not best practice and does not allow firms to target risk, but rather mandates blanket remediation. The text should be changed from "*fully addressed*" to "*fully dispositioned*" which will allow firms the freedom to risk accept based on their agreed risk appetite.

Article 21 (6) requires "*at least*" a yearly testing of the critical ICT systems and applications. This scope is not clear. The text should be clarified to make clear that it is for the firm to determine what is a "*critical ICT system and application*". Furthermore it is not specified what "*test*" shall mean. Reference should be made to the list given in Article 22 (1) if this is the intention of the Commission.

Article 25: General principles

Article 25 is located under Chapter V (managing of ICT third-party risk). ALFI agrees with the ABBL that the interaction and coherence between the Article 25 and the existing regulations is partly not ideal:

- it should be clarified that for ICT outsourcing the DORA rules apply exclusively and the EBA outsourcing requirements will not apply to ICT related outsourcing;

- because of the amount of other regulations about EU rules on outsourcing and third-party risk management in recent years (e.g. EBA Cloud Guidelines (2017), EBA Outsourcing Guidelines (2019), EIOPA Outsourcing to Cloud Guidelines (2020), ESMA Outsourcing to Cloud Guidelines (CP closed 2020)) there has to be a close look on how the new regulations fit into.

All in all, it should be worked out, when the ICT service is critical and especially to which criteria that is related.

Referring to Article 25 (8), that deals with determination, ALFI shares ABBL's view that the DORA could clarify that termination will not only be required if remediation of the identification concerns is not possible. Furthermore, it should be made clear that termination would be expected to take place under secure and controlled settings according to firms exit strategies. If there is termination without such controls it could lead to a risk to operations and therefore to market uncertainties. It should just be clear that firms have a legal option to terminate if necessary. ALFI agrees with that point of view, too.

Article 27: Key contractual provisions

The contractual arrangements should also include a provision regarding professional secrecy to which the financial entities are subject. Besides that there are some concerns about the interactions of the requirement in Article 27 with other European requirements. It can be noted, that firms have recently updated their contracts with suppliers to support the requirements in the EBA Outsourcing Guideline. Care must be taken to the interaction between such contract updates and with the EBA Guidelines.

Article 28: Designation of critical ICT third-party service providers

At the date of this document, Article 28 (1b) foresees that *"the ESAs, through the Joint Committee and upon recommendation from the Oversight Forum established pursuant to Article 29(1) shall: […] appoint either EBA, ESMA or EIOPA as Lead Overseer for each critical ICT third-party service provider, depending on whether the total value of assets of financial entities making use of the services of that critical ICT third-party service provider and which are covered by one of the Regulations (EU) No 1093/2010 (EU), No 1094/2010 or (EU) No 1095/2010 respectively, represents more than a half of the value of the total assets of all financial entities making use of the services of the critical ICT third-party service provider, as evidenced by the consolidated balance sheets, or the individual balance sheets where balance sheets are not consolidated, of those financial entities."*

ALFI assents ABBL's opinion that it can be seen as critical, that the use of value of assets as the metric to determine designation of oversight is used. That is because the assets do not reflect materiality of the relationship between the financial entity and Critical ICT-TTP. It could be preferable to align the relevant ESA with a Critical ICT TPP based on technical expertise.

Besides that it should not be forgotten that the smaller member states should not be penalized so that there should be more clarification referring to the ICT TPPs to be done.

Article 28 (1a) foresees:

"The ESAs, through the Joint Committee and upon recommendation from the Oversight Forum established pursuant to Article 29(1) shall: designate the ICT third-party service providers that are critical for financial entities, taking into account the criteria specified in paragraph 2;"

The designation of an ICT TPP could affect the relationship between the Critical ICT TPP and the financial institutions using their service as they could change their risk appetites. Besides that there are some other criteria to be changed or clarified, as there are:

- "the degree of substitutability of the provider";
- "the number of Member States in which the services of the ICT TPPs are provided";
- "used by financial entities"; and
- the concept of "large scale operational failure".

Referring to that, Article 28 (9) requires a legal incorporation in the Union of critical ICT TPPs. That leads to a reallocation of responsibility so that the firms have to decide whether a ICT TPP in a third country should be designated critical under the DORA. It should be seen, that most of the firms are not equipped to make such a judgement. That is especially because they are not able to access the information required to assess the criteria stated in Article 28 (2). Moreover, there is a further assessment to be done in order to know whether or not requiring legal incorporation within the EU would negatively impact the internal market providers.

Article 37: Follow-up by competent authorities

Article 37 (2,3) requires, that competent authorities are allowed to monitor the entities or even temporarily suspend the use or development of a service provided by the critical ICT third-party provider. ALFI agrees with the ABBL, that this creates a great risk for financial institutions: The current proposals do not provide a mechanism for financial institutions to receive any information resulting from assessment of a Critical ICT TPP by the lead overseer. Yet, Article 37(3) gives the NCAs the ability to require not only suspension, but even termination of a financial institutions' contract and use of the Critical ICT TPPs service if financial institutions do not account for risks identified through that assessment. This requirement therefore creates significant risk for financial institutions and substantial market uncertainty for firms operating in the EU.

Article 38: Oversight fees

According to Article 38 (1) the ESAs shall charge critical ICT third-party service providers fees that fully cover ESAs' necessary expenditure in relation to the conduct of Oversight tasks pursuant to DORA, including the reimbursement of any costs which may be incurred as a result of work carried out by competent authorities joining the Oversight activities. These ICT providers assessed as "critical" will likely resist this application of oversight fees imposed on them. These fees may lead to significant cost increase. This could end up in the costs being passed on to the financial institutions and ultimately to the end customer.

Chapter VI: Information sharing arrangements

ALFI agrees with the ABBL that information sharing between financial entities remains voluntary, while recognising that this is the intention of the European Commission.

Article 40: Information sharing arrangements on cyber threat information and intelligence

Consolidated EU data on for example reported ICT issues should be shared with the industry in condensed format. Whenever an ICT issue due to a breach or vulnerability is identified, it is almost guaranteed to repeat at other institutions. Hence, a rapid feedback mechanism back to the industry will ensure that the new reporting requirements are not just done for statistical or sanction purposes, but actually contribute to the continuous incremental improvement of the financial sector.

ALFI shares ABBL's view that participation by national authorities in such groups, mentioned in Article 40 (2), will necessarily change the character of the groups. While in some situations the inclusion of competent authorities may be appropriate and helpful, the DORA text seems to assume such participation in Article 40 (2).

Chapter VII: Competent Authorities

Article 41: Competent authority

Regarding the role of the competent authority, instead of the competent authority, member states should be able to designate the respective authority with regards to TLPT-testing.

Article 44, 48: Administrative penalties and remedial measures; Publication of administrative penalties

The possible sanctions mentioned in Articles 44 and 48 as well as in the introduction of the DORA should be published on an anonymised basis, as it will serve as a warning mechanism to other market participants. But it should be noted, that such sanctions can only be published after there is no more room for appeal. Otherwise, the critical information will reach the market month later, which makes the information obsolete.

Article 56: Entry into force and application

According to the ABBL, given the scale, complexity and significance to critical operations of some of the proposed changes it can be seen as critical that it is feasible for firms to implement the requirements in a 12-month period. Therefore, the application period should be extended. ALFI shares the above view.

Costs and losses:

ALFI agrees with ABBL: There is no specific need a reporting on costs and losses caused by ICT disruptions and ICT-related incidents. Costs and losses will likely correspond to the size of the institution rather than the severity of the ICT-related incident.

REGARDING THE PILOT REGIME[6]

The proposal on a pilot regime for market infrastructures based on distributed ledger technology introduces the possibilities for certain types of EU financial market participants to operate a market infrastructure (MI) based on distributed ledger technology (DLT) with clear and uniform requirements.

Echoing ABBL, ALFI notes that the Pilot Regime is in the line of the Luxembourg initiatives regarding the circulation and issuance of securities on DLT basis (law of 1 March 2019[7] and law of 22 January 2021[8]).

Uphold existing investor protection mechanism

ALFI supports the experimental approach taken by the Pilot Regime, which is essential to the development of a safe regulatory framework for security tokens. While fostering innovation is key, ALFI believes investor protection should remain at the heart of any regulation. Existing protection mechanisms, notably in terms of investor protection, market integrity and financial stability, should remain applicable under the Pilot Regime and future framework: the Pilot Regime should not remove successful layers of protection for customers or leave the tremendous responsibility of this protection to stakeholders that do not possess the same level of knowledge, tools and skills.

Eligible market participants

ALFI notices that two main divergent views across the Luxembourg industry are shared with respect to the fact that a custodian bank or investment firm would only be able to apply to the Pilot Regime in the case it was to operate a DLT-based MTF (Article 2 (7), (8), (9)).

On the one hand, this restriction could be considered as restrictive while adopting the view that the Pilot Regime should be opened up to a wider range of participants such as investment firms as well as credit institutions regulated under the Capital Requirements Directive framework. Under this approach, it should be proposed to allow investment firms and custodian banks to participate in the DLT Pilot Regime not only as operators of DLT MTFs but also as operators of DLT securities settlement systems:

- All current conditions (limited size, limited asset universe, e.g. exclusion of government bonds) would still apply.

- The benefits of the regime (e.g. cross-border distribution, certain exemptions from outsourcing regulation, use of certain cash settlement assets, etc.) would be available.

- As existing rules such as the CSDR would continue to apply, it is expected that such settlement arrangements would focus on assets that are not listed on regulated markets, e.g. private equity, private placement regimes and markets with secondary trading, e.g. fund issues (mark up/mark down).

This approach is also justified by the fact that the exclusion of investment firms and credit institutions to offer DLT securities settlement solutions – within the limits (in terms of issuance volume) of the proposal – could undermine some of the core objectives as formulated by the Commission:

- Legal certainty: Investment firms and custodian banks cannot gain direct experience in this Pilot Regime, and thus would not be able to identify shortcomings in the current regulatory framework.

- Innovation: A central tenet of DLT technology is to allow for markets to be designed with a greater level of operational decentralisation and distribution. The current regime, however,

[6] All Articles in this section without reference to respective regulation refer to the Pilot Regime.
[7] Law of 1 March 2019 amends the Law of 1 August 2001 on the circulation of securities.
[8] Law of 22 January 2021 modifies the Law of 5 April 1993 on the financial sector and the Law of 6 April 2013 on dematerialised securities.

would cement a high level of centralisation at the level of CSDs to the disadvantage of innovation coming from intermediaries and new market entrants.

- Investor protection: Investment firms and custodians are subject to robust regulation under various regulatory regimes including CRD/CRR, MiFID II, AIFMD, and UCITS. The inclusion of such participants in the Pilot Regime would thus provide continued adequate investor protection.

- Financial stability: Decentralisation and distribution are important means to improve operational and service stability. In fact, DLT can remove the risk of a "single point of failure" that is characteristic to many national market infrastructures. Creating a pilot regime that is open for CSDs and other participants alike would help to create the momentum to explore how DLT can improve financial stability.

On the other hand, it could be seen that the Pilot Regime would allow the emergence of a potential market for existing market infrastructures that are best placed to continue carrying out their role in a DLT environment.

Incumbent operators are in the best position to understand the challenges and handle the risks inherent to capital market infrastructures. Given these actors' experience in operating such infrastructures, it will be more efficient for the entire value chain to carry out tests in a pilot environment limited to experienced actors. New actors would have to build up such experience and knowledge before being able to develop new solutions in a DLT environment.

The limitation to regulated market operators and CSDs further guarantees that participants in the Pilot Regime have the required substance and internal organisation in place to run a reliable capital markets infrastructure. In particular before the background that retail investors may gain direct access to such platforms, it must be ensured that the DLT infrastructure provides at least the same guarantees than the existing ones.

Agreeing with ABBL, ALFI shares the second view considering that specialisation is to be encouraged for a robust financial environment.

Article 2: Definitions

Article 2 (5) – definition of "DLT transferable securities" – does not include transferable securities within the meaning of Article 4 (1) (44) (c) of Directive 2014/65/EU, that take the form of structured finance products. The legal rationale for excluding such products cannot be identified.

Scope of Financial instruments admitted

Regarding the maximum value of DLT transferable securities allowed to be recorded on a DLT MTF or DLT SSS (€2.5 billion), this threshold seems unlikely to attract regulated financial entities. The latter could indeed quickly reach the threshold (e.g. five €500 million bond issuances) and find themselves unable to pursue any other projects for the following years. A higher threshold would seem more in line with a pilot regime set to remain in place for several years. Widening the scope of financial instruments admitted to the Pilot Regime would go a long way in allowing a more rapid uptake of DLT in financial markets, and attract the required investments. A more flexible scope would have the benefit of including current market players who have been experimenting with security token solutions for some time now, but for which regulatory uncertainty remains a blocking point.

Article 3: Limitations on the transferable securities admitted to trading on or settled by a DLT market infrastructure

Article 3 (1)(a): ALFI agrees with ABBL that there is no legal and operational rationale for only allowing shares, the issuer of which has a market capitalization or a tentative market capitalization of less than EUR 200 million to be admitted to trading on or settled by a DLT market infrastructure. This would not allow issuers that have higher liquidity needs to participate in such new technological offerings. The compatibility of this cap with the 'technology-neutral' principles should be further assessed in this regard.

Article 3 (1) (b): it is to recommend to add a clarification in this section that the issuance size "of less than EUR 500 million" is to be understood on a per securities ISIN basis.

Article 3 (2): this section restricts investment firms or market operators operating a DLT MTF to admit to trading sovereign bonds under the Pilot Regime. It can be recommended to go against such provisions as the inclusion of sovereign bonds on DLT MTFs would (i) permit retail investors to invest in risk-free securities in a disintermediated market (without incurring intermediation fees) and (ii) allow sovereigns to take part in such DLT markets and be more knowledgeable of how such markets function.

Article (3): it is to recommend increasing the ceiling of EUR 2.5 billion in total market value of DLT securities that can be recorded by a DLT market operator to a higher amount, to (i) not stifle a potentially large market and (ii) because reaching the EUR 2.5 billion ceiling would trigger the implementation of a transition strategy[9] for additional assets, which could break transaction flows. Such figure of EUR 2.5 billion appears arbitrary and is not in line with the market value of transferable securities that are operated on non-DLT MTFs. This would only allow for a handful of transaction (potential of five issuances with the maximum issue limit). It is doubtful that market players would spend funds to build a platform with such minimal transaction capabilities.

Article 4: Requirements and exemptions regarding DLT multilateral trading facilities

Article 4 (1) (c): it would be helpful to get more information in the recitals of the proposal on the type of compensatory measures that competent authorities could impose to DLT market operators requesting the relevant exemptions.

Article 4 (2) (c): it would be helpful to have definitions for the terms “member”, “participant”, “issuer” and “client”. This is particularly important as DLT MTFs and DLT SSSs aim to be disintermediated and the role associated with each of these terms may be understood differently than in the context of standard non-DLT MTFs or SSSs.

Article 4 (4) and (3) (e) needs a clarification, too: these requirements would entail that the DLT device that the market operator uses is fully controlled by such market operator, which would mean that only permissioned DLTs are allowed. It may be asked whether a T+2 settlement could not also be achieved on a public permissioned DLT system. Here as well, it would be appreciated to get additional guidelines regarding what would be acceptable for NCAs and ESMA. This could however be achieved by delegating power to the Commission to adopt implementing technical standards or regulatory technical standards after consultation with ESMA. ESMA could in turn consult with the industry to find the right balance between setting clear standards, while remaining sufficiently flexible to foster innovation.

More generally speaking, it may be asked why no power has been delegated to the Commission and ESMA to develop additional level 2 regulation that could define additional principles for important parts where further clarification is utterly needed, such as in the context of the transition strategy or certain minimum requirements the technology has to satisfy in order to be eligible for the operation of those infrastructures. Some of the provisions currently foreseen in the proposal, such as the thresholds, could be moved to a level 2 regulation and be made subject to a review in order to allow for an efficient and fast adaptation process in case issues are identified.

Article 5: requirements and exemptions regarding DLT securities settlement system

Article 5 (2) (c) to (e) are the basis for point (b) of Article 5 (rather than stand-alone points) and they should hence be listed under point (b) as points (i), (ii), and (iii) instead.

[9] ALFI notes at the same time that the transition strategy is an important element of the Pilot Regime as it will have to define the seamless transfer of financial instruments from a DLT environment into the existing trading and settlement systems. One question, amongst others, in that context, remains on the implementation of the transition from a tokenised security to a book entry security. Since the systems are fundamentally different and not necessarily compatible, it would be important to further understand the requirements that will be applied by NCAs and ESMA. For the sake of legal certainty, it would be helpful if the Regulation could already set the high level requirements for such strategy.

Article 5 (2) (c) should read "the recording of the DLT transferable securities is effected on the distributed ledger."

Article 5 (7) should rather be second paragraph of point 6 rather than a standalone point.

Article 6: Additional requirement on DLT market infrastructure

Article 6 (3) requirement to provide an explanation on deviations from a standard SSS: While the functioning of a CSD operating a DLT system would be different from the functioning of a traditional CSD, the functions, services and activities will generally be the same (otherwise the entity would not qualify as a CSD). The current text is hence quite burdensome for CSD operating a DLT system as on one hand, it presupposes that the DLT CSD is in perfect knowledge of the functioning of a traditional CSD and, on the other hand, except for the functionality and relevant exemptions granted, both DLT and traditional CSDs should offer similar services and provide similar activities. As discussed above, an objective-based regime would be more suitable for the purposes of fostering innovation through rapid bringing to the market of new entrants under the Pilot Regime as supervised by national competent authorities and ESMA.

Article 8: Specific permission to operate a DLT securities settlement system

Article 8 (3) should refer to "DLT securities settlement system" rather than "DLT MTF."

Article 8 (6) (a) withdrawal of a permission for any "flaw" in the functioning of the DLT or in the services or activities provided by the CSD operating a DLT securities settlement system is both imprecise and far-reaching. Especially as the regime requires the applicant to show reliance and remedy process for flaws under Art. 6 of the Pilot Regime.

Article 10: Report and review

Article 10 (1) requires a report and review from the ESMA to the commission on the specified requirements (a) to (l) five years from the entry into application of this regulation, at the latest.

The Pilot Regime regulation (and more particularly the applicable thresholds) could benefit from a mid-review instead of having to wait five years after its entry into application for a full review. Since the review that should be performed by the ESMA would be the only way to broaden the scope of the exemptions granted, or of the financial instruments admitted to the Pilot Regime, no adjustments would occur before these five years.

A more frequent review of the Pilot Regime would ensure its relevancy and allow DLT market infrastructures to fully reap its benefits. For instance, the publication of frequent review reports could allow to make necessary adjustments if need be, in a time-sensitive manner without having to wait five years after its adoption. This would also be in line with the Digital finance objective of adopting a future-proof approach towards regulation.

Termination option

In addition, the option for pilot termination should be deleted (Article. 10 (2) (e)). Considering the large investment costs required and the limited duration of specific permissions (six years under Art. 7 (5) and Art. 8 (5)), there should be an automatic extension option for limited permissions granted. Such an option would give the market participants the confidence they need, incentivize investments and help secure the profitability of tested projects.

Participants

It should be noted that currently authorised investment firms and market operators can apply for the Pilot Regime to offer solutions for DLT-based multilateral trading facilities (MTF), as well as authorised

CSDs can apply for the Pilot Regime to offer solutions for DLT-based securities settlement system (SSS).

Echoing the above comments, given the entry barriers to apply for the Pilot Regime, the regime is likely to be particularly interesting for established industry players, with the possibility and the funds to run a Pilot Regime for up to 5 years in an autarchic environment before opening it up to traditional market conditions.

In Luxembourg, there can be seen a potential market, especially, for key players such as Clearstream, LuxCSD and the Luxembourg Stock Exchange.

Securities

The Proposal provides for a limited scope of eligible products to be traded on an MI/DLT; insofar as both quantitative and qualitative criteria need to be complied with.

The current wording ensures, that only less liquid transferable securities (within the meaning of the MiFID definition of financial instruments) are eligible for trading on the MI/DLT, thereby excluding potentially interesting products, such as sovereign bonds and structured finance products.

ALFI agrees with the ABBL, that an extension of the scope of eligible transferable securities is highly recommended, given the market opportunities for these products. Based on a bespoke DLT-MTF, these not-yet-included products could be particularly interesting for Luxembourg in terms of positioning itself in the future ecosystem.

Applicability

The exemption regime is further based on a compensation scheme, where the exemptions granted are measured against compensatory measures. The proposal will need to be significantly clarified in regard of those compensatory measures which are likely to jeopardise the entire Pilot Regime, depending on their scope and nature.

The Pilot Regime has the potential to disintermediate the entire value chain of securities processing (also in terms of shortening the securities transaction timeline, which may be brought down to real-time settlement), which has a significant impact on the entire securities industry in Luxembourg, as well as key industry players such as CSDs, securities services providers as well as existing market infrastructures (e.g. Luxembourg Stock Exchange).

The possibility foreseen in the proposal to extend the Pilot Regime securities offering to retail investors brings about the question on the calibration of investor protection regulation and the difficult trade-off between investment opportunities and protection of retail customers.

The proposal foresees an important role for ESMA, insofar as any admission to the Pilot Regime mandatorily presupposes a non-binding opinion by ESMA. It is difficult to imagine situations in which NCAs would actively go against any such opinion, as non-binding as it can be. This may act as an additional hurdle for the setup of any such pilot regime, especially where niche markets are targeted.

The interaction with the Luxembourg DLT initiatives will have to be fully assessed to ensure a smooth transition between the existing Luxembourg regime and the incoming Pilot Regime.

Conclusive feedback:

The regulations need to be clarified at some points. Some changes and reviews to the above mentioned points should be done to fulfil the measures and purposes.

Principles and risk-based requirements should enable firms to implement controls that are future-proof, flexible, proportionate, and commensurate to the risks. Furthermore there should be both clear definitions and proportionate criteria of designation for the critical third-party service providers. The definitions of criticality should be based on objective criteria and unambiguous.

The EU supervisory authorities should prepare further proposals for technical regulatory standards. It is key however that there is alignment between national and EU authorities to avoid the setting up of multiple reporting lines. Moreover, tests or even exit strategy formalisations must be proposed only with a risk based approach.

Alternative options to address and minimise risks associated with reliance on third country providers include new specifications for the drafting of contracts, which also apply to critical ICT service providers. In addition, all critical ICT service providers (not just third-country providers) could be subject to certifying adherence to a comprehensive and internationally accepted cyber-security standard.

As an additional consideration and due to the existing and future extensive exchange of data between supervisors and supervised entities, ALFI believes that minimum standards for both private market participants and public authorities would be essential in order to make the European financial market as a whole resilient to any IT security gaps.