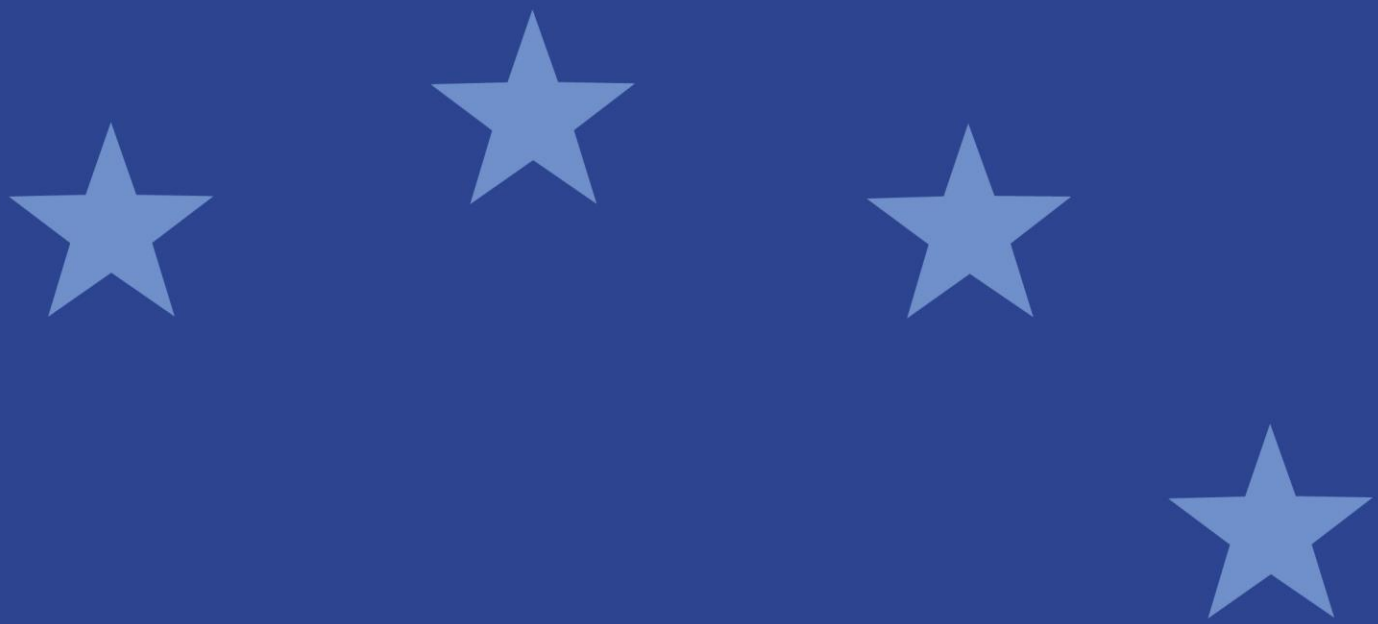
esma European Securities and Markets Authority

Discussion Paper

Draft Technical Standards for the Regulation on improving securities settlement in the European Union and on central securities depositories (CSD)



20 March 2014 | ESMA/2014/299

European Securities and Markets Authority

Date: 20 March 2014
ESMA/2014/299

Responding to this paper

ESMA invites comments on all matters in this paper and in particular on the specific questions summarised in Annex IV. Comments are most helpful if they:

- indicate the specific question to which the comment relates;
- respond to the question stated;
- contain a clear rationale; and
- describe any alternatives ESMA should consider.

ESMA will consider all comments received by **22 May 2014**.

All contributions should be submitted online at www.esma.europa.eu under the heading 'Consultations'.

Publication of responses

All contributions received will be published following the close of the consultation period, unless you request otherwise. Please clearly and prominently indicate in your submission any part you do not wish to be publically disclosed. A standard confidentiality statement in an email message will not be treated as a request for non-disclosure. A confidential response may be requested from us in accordance with ESMA's rules on access to documents. We may consult you if we receive such a request. Any decision we make is reviewable by ESMA's Board of Appeal and the European Ombudsman.

Data protection

Information on data protection can be found at www.esma.europa.eu under the heading 'Disclaimer'.

Who should read this paper

All interested stakeholders are invited to respond to this discussion paper. In particular, responses are sought from CSDs, CSD users or linked entities, market infrastructures and investors.

Table of Contents

I. Executive Summary 7

II. Introduction 8

III. Discussion Paper 10

III.I Settlement Discipline 10
Measures to prevent settlement fails (Article 6(4)) 10
Incentives for early input of settlement instructions 13

System functionalities 13

Lending facilities 14

Details of the system monitoring settlement fails (Article 7(14)(a) 16
Details of operation of the appropriate buy-in mechanism: extension period (Article 7(14)(d) 19
Details of operation of the appropriate buy-in mechanism (Article 7(14)(c)) 21
Details of operation of the appropriate buy-in mechanism: operation types and timeframes under which buy-in is deemed ineffective (Article 7(14)(e) 23
Calculation of the cash compensation (Article 7(14)(f)) 24
Conditions under which a participant is deemed to consistently and systematically fail to deliver the financial instruments (Article 7(14)(g)) 25
Necessary settlement information (Article 7(14)(h)) 26
Penalties for settlement fails (Article 7(13)) 27
Internalised settlement (Article 9(2) and (3)) 28
III.II CSD Authorisation 30
Information to the CA for authorisation (Article 17(8)) 30
CSD identification, policies and procedures, relevant agreements 30

Information to the CA for authorisation - Standard forms, templates and procedures (Article 17(9)) 31
Conditions for participations of CSDs in entities which not provide services listed in Sections A and B of the CSDR Annex (Article 18) 32
Distinction with Articles 46 and 47 32

Guarantees 32

Limit control 33

Limit percentage of income from participations 33

Limit participations to securities chain 33

Review and evaluation (Article 22(10) and (11)) 35
A report summarising material changes to the arrangements, strategies, processes and mechanisms 35

The documentation modified either after the authorisation procedure foreseen under Article 17 CSDR or after the last review of the CSD 36

Information defined to be delivered for each review 36

Other information 36

Information from third country CSDs to ESMA for recognition (Article 25) 38
Monitoring tools for the risks of CSDs, responsibilities of key personnel, potential conflicts of interest and audit methods (Article 26) 39
Risk monitoring and responsibilities of the key personnel 39

Recordkeeping (Article 29(3) and (4)) 42
Data keeping and availability / other aspects 43
Risks which may justify a refusal of access to participants and procedure in case of refusal (Article 33(5) and (6)) 45
Reasons which may justify a refusal by a CSD of access to participants 45
Elements of the procedure where a CSD refuses to provide access to a participant 46
Integrity of the issue (Article 37) 47
Internal Reconciliation 47
The specific case of corporate actions 48
External reconciliation 48
Prohibition of overdrafts, debit balances and securities creation 49
Operational risks (Article 45) 49
Operational risk management framework 50
Identification and mitigation of operational risk 52
Information technology tools 52
Business continuity policy 54
Investment policy (Article 46) 58
Highly liquid 58
Appropriate timeframe for access to assets 58
Concentration limits 59
CSD links (Article 48) 60
Protection of the linked CSDs and their participants in different types of link arrangements 60
Standard and customised links 60
Interoperable links 62
Monitoring and managing additional risks arising from indirect links and the use of intermediaries 62
Reconciliation methods 63
Identification, investigation and rectification of discrepancies 64
DVP settlement 64
Reasons which may justify a refusal of access to issuers and the procedure in case of refusal (Article 49(5) and (6)) 65
Reasons which may justify a refusal by a CSD of access to issuers 65
CSD links: procedure in case of refusal of access (Article 52(3) and (4)) 68
Elements of the procedure where a CSD refuses to provide services to a requesting CSD 68
Reasons which may justify a refusal of access to other market infrastructures and the procedure in case of refusal (Article 53(4) and (5)) 69
Reasons which may justify a refusal by a CSD of access to other market infrastructures 69
Elements of the procedure where a party refuses to provide access to another party 70
Procedure for granting and refuse authorisation to provide banking type of ancillary services (Article 55(7) and (8)) 71
Annex I: Possible minimum requirements for an application for registration as CSD 73

Annex II: Template for CSD Registration application 80

Annex III: Recordkeeping requirements 81

Annex IV: Summary of questions 84

Annex V:Legislative mandate to develop draft technical standards 89

Acronyms Used

CCPs	Central Counterparties
CSDR	"CSD Regulation", Regulation [no.] of the European Parliament and of the Council on improving securities settlement in the European Union and on central securities depositories (CSDs) and amending Directive 98/26/EC – also referred to as "the Regulation" (compromise reached, number to be assigned)
DVP	Delivery versus Payment
EBA	European Banking Authority
EC	European Commission
EU	European Union
EIOPA	European Insurance and Occupational Pension Authority
ESAs	European Supervisory Authorities
ESCB	European System of Central Banks
ESMA	European Securities and Markets Authority
FoP	Free of Payment
ISD	Intended settlement date
ITS	Implementing Technical Standards
MiFID	Directive 2004/39/EU [MiFID I]
MiFID II	Directive no. [X] of the European Parliament and of the Council on markets in financial instruments repealing Directive 2004/39/EC of the European Parliament and of the Council (compromise reached, number to be assigned)
MiFIR	Regulation no. [X] of the European Parliament and of the Council on markets in financial instruments and amending Regulation [EMIR] on OTC derivatives, central counterparties and trade repositories
PFMI	CPSS-IOSCO Principle(s) for Financial Market Infrastructures
RTS	Regulatory Technical Standards
T+2	2 days after the trade date
T2S	TARGET2-Securities
TRs	Trade Repositories

I. Executive Summary

Reasons for publication

This discussion paper seeks stakeholders' views on the possible contents of most of the regulatory and implementing technical standards ESMA is required to draft under the CSDR.

The input from stakeholders will help ESMA in the development of the relevant technical standards to be drafted and submitted to the EC for endorsement in the form of Commission Regulations, i.e. a legally binding instrument directly applicable in all Member States of the EU. One essential element in the development of draft technical standards is the analysis of the costs and benefits that those legal provisions will imply. Input in this respect and any supportive data will be highly appreciated and kept confidential where explicitly requested.

Contents

This discussion paper follows the structure of the CSDR, with the first section focusing on settlement discipline. The second part focuses on CSD authorisation, representing most of the technical standards under CSDR and where market feed-back is welcome.

ESMA is also required to draft a number of standards on supervisory issues, notably under Articles 12 (relevance of certain currencies and consultation of relevant authorities) and 24 (cooperation between regulators on CSDs that are substantially important cross-border). As under EMIR, this consultation does not include those mandates, that are being discussed amongst the competent authorities.

Next steps

As provided for by Regulation No 1095/2010 of the European Parliament and Council establishing ESMA, a public consultation will be conducted on the draft technical standards before they are submitted to the E C for endorsement in the form of EU Regulations. According to ESMA decision ESMA/2011/BS/4a on the procedure for developing and adopting draft technical standards and guidelines, the consultation paper will include the actual legal text of the provisions constituting the draft technical standards, an explanation of the measures adopted and a cost-benefit analysis. Therefore, following this discussion paper and on the basis of the relevant input received, ESMA will finalise its proposed draft technical standards to be included in the consultation paper. The date of publication of such consultation paper and the commenting period will depend on the date of publication of the CSDR in the Official Journal and the final deadline for ESMA to deliver the draft RTS and ITS to the EC.

II. Introduction

1. At the trilogue meeting of February 26th 2014, the European Parliament, the Council and the EC reached a political agreement on CSDR. This discussion paper is based on the version of the text of the Regulation following such agreement (Ref. 6828/13, inter-institutional file 2012/0029 (COD), EF 57, ECOFIN 179, CODEC 527[1]).
2. The Regulation introduces an obligation to represent all transferable securities in book entry form and to record these in CSDs before trading them on regulated markets. It harmonises settlement periods and settlement discipline regimes across the EU. It introduces a common set of rules consistent with international standards addressing the risks of the CSDs' operations and services. As CSDs will be subject to identical substantive rules across the EU, they will benefit from uniform requirements for licensing and an EU wide passport, which will help remove the existing barriers of access. This will also impact on other structures, direct (e.g. investment firms under Article 6) and indirect (e.g. registrars). It should also be noted that a number of related issues may be covered in future legislative initiatives, such as the Securities Law Legislation (SLL), matters around the property of the shares and Member States are responsible of the supervision of this area. Relevant developments are ongoing, notably T2S, that will being operational harmonisation. Where appropriate, T2S elements have (e.g. record-keeping requirements) or will be been considered. ESMA has also considered consistency of the forthcoming implementing and RTS with the CPSS-IOSCO Principles on Financial Market Infrastructures (PFMIs), in line with recital 6 of the CSDR.
3. The Regulation delegates or confers powers to the EC to adopt RTS or ITS on a number of areas (see Annex V for the legal mandate). This discussion paper covers the draft technical standards that ESMA is expected to develop.
4. ESMA's views as presented in this discussion paper are of preliminary nature and aim at gathering the stakeholders' opinions at an early stage of the process. Some of the views on technical standards are more developed than others. This reflects the level of maturity and non-controversial aspects of CSDR, but also the limited time that ESMA had at its disposal to make its analysis on a stable part of the primary legislation. Views and preliminary considerations expressed in this discussion paper will not bind in any way ESMA in the future development of the draft technical standards.
5. One essential element for the drafting of technical standards is the impact analysis of the costs and benefits that the proposed measures might produce. In order for ESMA to be able to base this cost-benefit analysis on objective figures, respondents to this discussion paper are kindly invited to accompany their responses with quantitative evidence. It would also particularly important to understand, for each of the possible envisaged requirements, how long it would be necessary for the industry to implement the necessary arrangements to ensure compliance. Information provided in this respect, as well as any response to this discussion paper will be treated in a confidential manner where requested.
6. EBA is expected to draft RTS on three sections: Articles 47(3) (capital requirements, retained earnings and reserves of a CSD); 54(9) (additional, risk based capital surcharge); 59(5) (monitoring, the measuring and the management and the reporting of the credit and liquidity risks, including those which occur intraday. ESMA and EBA are cooperating in the drafting of all CSDR technical standards.
7. In developing this discussion paper ESMA has closely cooperated with the EBA and ESCB members, by establishing a task force for the drafting of the relevant standards, in which EBA observers and ESCB members participate.

[1] http://register.consilium.europa.eu/doc/srv?l=EN&t=PDF&gc=true&sc=false&f=ST%206828%202014%20INIT

8. As part of the analysis carried out before issuing this discussion paper, ESMA is also consulting the Post-trading Consultative Working Group (CWG), an ESMA stakeholder group.

III. Discussion Paper

III.I Settlement Discipline

Measures to prevent settlement fails (Article 6(4))

9. Under Article 6(4) CSDR, ESMA is expected to develop RTS to specify details of the confirmation and allocation measures and of the procedures between investment firms and their professional clients facilitating settlement and the details of the tools for the management of the timely settlement of transactions. The sections below regard the latter elements. Confirmation and allocation measures were added later in the CSDR negotiations and have not yet been discussed in depth by ESMA; any input is welcome on the possible elements to draft these technical standards.

Q1: Which elements would you propose ESMA to take into account / to form the technical standards on confirmation and allocation between investment firms and their professional clients?

10. The main objectives of ESMA when drafting this standard will be that it contributes to (i) the early settlement of transactions on the intended settlement date; and to (ii) the reduction of the number instructions that fail to settle on the intended settlement date. This is aimed to be achieved whilst not inflicting unnecessary costs on the CSDs and their participants.

a. Automation

i. No manual intervention

11. For the CSD processing of settlement instructions, CSDs should make no use, or very limited use, of manual intervention. Automation may facilitate timely settlement by contributing to an efficient settlement process with lower operational risk. The submission and processing of ordinary settlement instructions, hold and release instructions and other instructions related to the settlement, should therefore be automated. CSDs should not offer services which require manual intervention by default. ESMA is currently of the view that manual intervention should only be allowed in exceptional circumstances that, if any, should be clearly specified in the technical standard.

Q2: In your opinion, are there any exceptions that should be allowed to the rule that no manual intervention occurs in the processing of settlement instructions? If so please highlight them together with an indication of the cost involved if these exceptions are not considered.

b. Communication procedures and standards - STP

12. The use of straight through processing ("STP") through the securities chain should be promoted as it might lead to (i) a more efficient settlement procedure; (ii) possibly reduced settlement costs; (iii) lowering operational risk by reducing manual intervention in the settlement process. By STP is meant the automated end-to-end processing of trades/settlement instructions including, where

relevant, the automated completion of confirmation, matching, routing, clearing and settlement of instructions.[2]

13. While a CSD is normally not in a position to ensure automation in the rest of the securities chain, it may choose technical solutions which accommodate the use of STP. Moreover, CSDR Article 35 requires that CSDs use in their communication procedures with participants of the securities settlement systems they operate, and with the market infrastructures they interface with international open communication procedures and standards for messaging and reference data in order to facilitate efficient recording, payment and settlement, as defined in Article 2(1)(31) of CSDR. The use of such procedures and standards may, amongst others, reduce barriers to entry into a market. In this context, is important to note that use of the message format ISO 20022 is mandatory for T2S as well as for credit transfers and direct debits in the Single Euro Payments Area (SEPA)[3]. These procedures may therefore be considered to facilitate STP and therefore efficiency along the chain.

Q3: ESMA welcomes concrete proposals on how the relevant communication procedures and standards could be further defined to ensure STP.

c. Matching of settlement instructions

14. Matching in the context of CSDs is the process of comparing the settlement details provided by the buyer and the seller of securities in order to ensure that they agree on the settlement terms of the transaction[4].

i. Compulsory matching

15. Matching is a prerequisite for an efficient settlement process as it may reveal inconsistencies between settlement instructions from both counterparties. Matching between CSD participants is a used and generally accepted step in the settlement of a transaction[5] and ESMA is of the opinion that matching prior to settlement should be compulsory. An exception to this would be (i) when the settlement instructions received by the CSD are already matched (e.g. trades entered into on a trading venue where the trading venue sends the trade enriched with settlement information to the CSD); or (ii) FoP instructions which consist in transfer of securities between different accounts opened in the name of the same participant.

ii. Continuous matching

16. The matching of settlement instructions by CSDs should be fully automated; and occur as early as possible. The CSDs should therefore offer matching real-time; and continuously throughout each business day.

iii. Standardised matching fields

[2] In line with the definition of "STP" in the ECB glossary.
[3] Cf. the Annex to Regulation (EU No 260/2012 of the European Parliament and of the Council of 14 March 2012 establishing technical and business requirements for credit transfers and direct debits in euro and amending Regulation (EC) No 924/2009. ISO 20022 is a Universal financial industry message scheme (http://www.iso20022.org/).
[4] T2S URD paragraph 5.5.
[5] Cf. ESCB-CESR Recommendation 2 for securities settlement systems (SSS).

17. CSDs currently set their own standards for determining which information should be provided in a settlement instruction. Standardising this by prescribing which matching fields should be used facilitates STP, because it caters for the scenario of CSD participants (including other CSDs) systems which participate in multiple CSDs; and might facilitate cross-border settlement. This easier settlement is achieved via matching fields harmonisation because all the information for the settlement is included in the settlement instructions; and the settlement instructions are exchanged (between the matching parties) in a standardised way.
18. ESMA therefore considers standardising the matching fields used. Harmonisation work in this field has been performed under T2S, where participant CSDs will be required to use the mandatory matching fields[6] reported below:

- Instruction type code;
- Intended settlement date;
- Trade date;
- Currency (not for FoP);
- Settlement amount (not for FoP), with a certain tolerance level;
- Share quantity (for equities) or nominal amount (for fixed income securities);
- Buy/sell (Deliver/receive for FoP);
- ISIN code;
- The counterparty delivering the securities;
- The counterparty receiving the securities; and
- CSD of the counterparty.

19. These fields could be complemented where appropriate. In T2S clients' codes are not mandatory matching fields. Client codes are generally voluntary matching fields, which become mandatory on the initiative of either or both counterparties. Nonetheless, client codes may be very important in order to avoid matching the wrong settlement instructions and could therefore be included.
20. It is also ESMA's view that CSDs should set appropriate tolerance levels in the settlement amounts in order to smooth the matching process.

Q4: Do you share ESMA's view that matching should be compulsory and fields standardised as proposed? If not, please justify your answer and indicate any envisaged exception to this rule. Are there any additional fields that you would suggest ESMA to consider? How should clients' codes be considered?

[6] T2S URD paragraph 5.5.2.

Incentives for early input of settlement instructions

21. Matching as early as possible in the settlement process gives the possibility to identify and correct inconsistencies in time for the transaction to settle on the ISD. Participants should therefore send settlement instructions to the CSD as early as possible in order to make early matching possible.
22. To accomplish this, disincentives could be applied to (i) the late sending of complete instructions; and/or (ii) the late matching of complete instructions. However, it might be difficult to enforce that specific rule without penalising the participant which sent its instruction timely.
23. It is therefore ESMA's current view that settlement instructions which are not received by the CSD by the end of ISD-2 should be subject to disincentives by the CSD, if the latter is aware that these were not submitted or, after submission, that these could have been submitted before the end of ISD-2[7]. Such measures should avoid participants sending instructions to the settlement system only when they are certain the instructions may be settled to avoid penalties for settlement fails.
24. In order to incentivise early matching, CSDs should offer hold/release and bilateral cancellation facilities, without prejudice of the Settlement Finality Directive provisions.
25. CSDs should develop a procedure to inform participants about pending settlement instructions of counterparties. Participants should be able to know that their instruction did not match the reason why. This information could be made available by the CSD within 30 minutes maximum, or similar cap after the first unsuccessful matching attempt; and at the beginning of ISD.

Q5: Do you agree with the above proposals? What kind of disincentives (other than monetary incentives such as discounts on matching fees) might be envisaged and under which product scope?

System functionalities

26. There are several reasons why it is advantageous to have more than one batch[8] to settle or to have continuous settlement (RTGS[9]) during a business day. One of the advantages is that it enables participants to resolve problems with the settlement instructions which prevented their settlement in the first available settlement batch, while still being able to settle on ISD. This would improve the settlement efficiency and shorten the period in which the parties are exposed to counterparty risk (e.g. credit or liquidity risk). A second reason is that multiple daily settlements may also help ensure efficient use of the cash received by the participants during the settlement cycles, due to different timing of settlement in the payment systems. A third reason is that it may facilitate the establishment of links between CSDs. This because frequent settlement reduces the risk that settlement instructions remain pending in one system as a result of finality not being achieved timely in the linked system.
27. In 2004, ECSDA agreed ten standards for settlement to assist removing the so-called Giovannini (Committee) barriers to settlement[10]. ECSDA Standard 9 states that securities settlement systems should support efficient cross-border settlement in Europe. This should be done by including at least one settlement cycle per hour during the opening time of the relevant European currency's banking system and until, at a minimum, two hours before the banking system closes. Not all Euro-

[7] For some classes the cycle may be different and this would apply with adaptations, notably in the case of shorter than T+2 cycles.
[8] In this document the term 'batch' is used as possibility to settle. This is in line with the definition of the term in the PFMI.
[9] ECB glossary: Real-time gross settlement (RTGS) system: a settlement system in which processing and settlement take place on a transaction-by-transaction basis in real time.
[10] Cfr. the Second Giovannini report from April 2003.

pean CSDs meet this ECSDA standard. Further, it is the understanding of ESMA that in the markets with continuous or multiple daily settlements, not all batches are necessarily widely used.

28. Also according to PFMI8, securities settlement systems should consider adopting real time or multiple-batch processing during the settlement day. There are, however, mixed risk profiles of real time and multiple batches, as further detailed in PFMI8[11].

29. To increase settlement on the ISD, ESMA is of the opinion that the CSDs should be obliged to offer (i) several possibilities to settle; or (ii) ongoing DVP settlement throughout each business day. ESMA's view is that it should be left to each CSD to decide whether real time or multiple daily settlement batches will be most appropriate for the markets they serve. However, all CSDs should be obliged to offer at least three daily settlements (batches), unless they operate on an RTGS basis. The latter, being more stringent, would indeed ensure compliance with a multiple batches system.

Q6: In your opinion, should CSDs be obliged to offer at least 3 daily settlements/batches per day? Of which duration? Please elaborate providing relevant data to estimate the cost and benefit associated with the different options.

30. ESMA finds that several other system functionalities may contribute to settlement efficiency:

- the use of optimisation algorithms, inter alia applying technical netting[12] typically identifying chains of settlement instructions;
- partial settlement/splitting a failed settlement instruction in several instructions (e.g. one which will settle and one which will fail);
- recycling of settlement instructions by the CSD in order to settle any failed settlement instructions in a later settlement procedure;
- shaping a trade by substituting a failed settlement instruction with a number of smaller settlement instructions, which in total are equivalent to the original failed settlement instructions, in accordance with predefined parameters.

Q7: In your view, should any of the above measures to facilitate settlement on ISD be mandatory? Please describe any other measure that would be appropriate to be mandated.

Lending facilities

31. According to CESR-ESCB Recommendation 5 for Securities Settlement Systems[13] that "*A centralised securities lending facility can be an efficient mechanism for reducing settlement failures. However, in markets where the number of settlement failures remains low, centralised securities lending arrangements may not be justified from a cost-benefit perspective*".

32. On the basis of CSDR, any provision to be contained in the TS need to refer to securities lending and borrowing mechanisms where the CSD acts as an agent (facilitator). Any mechanism in which the

[11] In particular Explanatory Note 3.8.7: "*The use of multiple-batch settlement and RTGS involves different trade-offs. Multiple-batch settlement based on a DNS mechanism, for example, may expose participants to settlement risks for the period during which settlement is deferred. These risks, if not sufficiently controlled, could result in the inability of one or more participants to meet their financial obligations. Conversely, while an RTGS system can mitigate or eliminate these settlement risks, it requires participants to have sufficient liquidity to cover all their outgoing payments and can therefore require relatively large amounts of intraday liquidity. This liquidity can come from various sources, including balances at a central bank or commercial bank, incoming payments, and intraday credit. An RTGS system may be able to reduce its liquidity needs by implementing a queuing facility or other liquidity-saving mechanisms".*

[12] In T2S, transactions are grouped into a set to which technical netting is applied by calculating the net quantities and amounts to be settled on an all-or-none basis. These net quantities and amounts are the basis for the checks against the resources available for the settlement. Such technical netting may solve gridlocks in a "Real Time Gross Settlement" (RTGS) system.

[13] "RSSS" 2009, (key issue 3).

CSD takes on counterparty credit risk requires a special authorisation under the regime envisaged for the services under Section C of the Annex to the CSDR.

33. Centralised securities lending facilitates a speedy matching of potential borrowers and lenders, making the lending process faster and potentially more accurate (automated procedures) and thus overally more efficient. In some markets, they are integrated in the securities settlement system, meaning that loans are automatically generated if this is necessary to avoid settlement fails during each settlement batch.

34. The use of centralised securities lending facilities in connection with settlement might reduce the number of settlement fails. ESMA has considered whether it should be mandatory for the CSDs to make such facilities available to their participants. However:

- such facilities are not available in all markets;
- they are often restricted to the most liquid shares, in part because other financial instruments may be too scarce to be supplied through a centralised lending facility;
- they may entail substantial costs for the CSDs and their participants;
- there may be tax disincentives; and
- depending on the design of the lending facility, the lender and the borrower may also have to take liquidity and credit risk on each other.

Against this background, ESMA believes that CSDs should not be obliged to offer arrangements for the lending and borrowing of securities. Should the service be provided, it should be framed in a harmonised manner.

Q8: Do you agree with this view? If not please elaborate on how such arrangements could be designed and include the relevant data to estimate the costs and benefits associated with such arrangements. Comments are also welcome on whether ESMA should provide for a framework on lending facilities where offered by CSDs.

Details of the system monitoring settlement fails (Article 7(14)(a)

35. Article 7(1) CSDR mandates CSDs to establish a system that monitors settlement fails of transactions in financial instruments and provide regular reports to the authorities as to the number and details of settlement fails and any other relevant information. These reports, including the measures envisaged by CSDs and their participants to improve settlement efficiency, are also to be made public by CSDs in an aggregated and anonymised form on an annual basis.
36. This means that a CSD will need to monitor settlement fails for a number of instruments, which, as outlined in Article 5(1), includes transferable securities, money-market instruments, units in collective investment undertakings and emission allowances, depending on the instruments accepted by the relevant CSD.
37. It is important for competent authorities to have regular and timely information on settlement figures, in order to have an overview of how efficiently securities settlement is occurring, as well as being able to identify where problems are or where they may arise. Likewise, ESMA considers that participants to the settlement system also have access to information on settlement fails so that they may address them in a timely fashion and be able to take necessary action to resolve fails.
38. The content of these reports will need to be accurate and useful for competent authorities and securities system participants to assess and act on. Therefore, the number and details of fails are essential pieces of information that should be included. If participants are not actively sent settlement fails reports by the CSD they should at least have open access to their own status on fails and an aggregate status for the CSD operating the systems to which they are participants.
39. At present, a number of CSDs currently operate a system that does such monitoring, in order to identify transactions that have failed to settle. However, for a number of CSDs this was not a legal obligation before CSDR. As well as the CSD, in a number of jurisdictions the CCP also carries out similar monitoring, also following the Short Selling Regulation. A few jurisdictions also have entities such as authorities or trading venues involved in such monitoring.
40. For the determination of the details of such monitoring, ESMA will rely on the existing mechanisms established voluntarily by ESMA and the competent authorities.
41. The table below presents in more detail the key elements for settlement fails reporting by the supervisors of EU CSDs and ICSDs to ESMA and ensures the consistency of the dataset. Data is sent per settlement day and settlement system. Given the easy availability of the software, Microsoft Excel has been used, although any format may be used provided that enables the processing of the data in a EU harmonised way at ESMA and avoid manual processing.

The required data is as follows and further described below.

Field	*Description*
Country Code	Two letter country code[14]
Settlement Date	The intended settlement date
Type of instrument	Type of instrument, like “Equities”, “Corporate Bonds” etc. Use ISIN or, if not available, the CFI (align with MiFID)

[14] The list of country code is provided in Annex 1.

	To be discussed: instruments not yet harmonised / codified (e.g. covered bonds)
% Fail based on volume	Data on failure to deliver securities (sale / sell instructions)
% Fail based on value	
Volume of failed	
Total volume	
Value of failed	
Total value	
% Fail based on volume	Data on failure to deliver cash (purchase / buy instructions)
% Fail based on value	
Volume of failed	
Total volume	
Value of failed	
Total value	

Volume = Number of settlement instructions

Value = Value of settlement instructions

42. This general approach reflects the preliminary and voluntary character of the exercise run by ESMA in the last years. A more detailed approach could be followed under CSDR, considering further fields, notably the identification of the failing party, where available, or at least the CSD member that failed and over which specific issuer. One could also consider distinguishing between FoP and DvP trades. Regulators are analysing further the additional fields that could be considered, having in mind their needs and the CSD datasets.

Q9: Do you agree with the above monitoring system description? What further elements would you suggest? Please present the appropriate details, notably having in mind the current CSD datasets and possible impact on reporting costs.

43. Participants should be able to access the relevant information on their transactions settled/to be settled at a given CSD. ESMA is of the view that participants should not have access to the same level of information as authorities on the overall market, but be provided access by CSDs to all information on the failed instructions involving these participants, either as a buyer or a seller.

Q10: What are your views on the information that participants should receive to monitor fails?

44. As well as reporting to regulatory authorities, it will also be beneficial for certain information to be made public, in order for market participants and other interested parties to gain an overall understanding of the settlement landscape. This is provided for in Article 7(1) CSDR, in aggregate and anonymised form on an annual basis, including the measures envisaged by CSDs and their participants to improve settlement efficiency.

Q11: Do you believe the public information should be left to each CSD or local authority to define or disclosed in a standard European format provided by ESMA? How could that format look like?

Reporting frequency

45. Reporting frequency impacts data quality and may also have costs for the reporting entities and the authorities. CSDR does not define the frequency of reports, but enables ESMA to define the details of the reports from CSDs to competent and relevant authorities. Currently a number of authorities receive this data on a daily basis, hence ESMA is considering whether this should be a harmonised requirement for all CSDs operating in the EU and what would the cost implications for the CSDs that currently do not have such a daily reporting system in place.

Q12: What would the cost implication for CSDs to report fails to their competent authorities on a daily basis be?

Details of operation of the appropriate buy-in mechanism: extension period (Article 7(14)(d)

46. As well as enforcing fines on participants, another measure that can be used to address settlement fails is through the process of buying-in securities that have not been delivered. Whilst for some markets and participants this will bring a change to their market practice, as the requirement will be applicable to a number of instruments, it is an important measure that can be used in order to enhance and promote settlement efficiency and certainty.
47. Although this will be a relatively new requirement for some, it is not an entirely new process, and it is currently employed by various existing market infrastructures. In the cases where it does exist, the process is generally carried out by either the relevant trading venue or CCP. In addition, buying-in of cleared shares is already a requirement in the Short Selling Regulation.
48. Paragraph 3 of Article 7 reads: "Without prejudice to the penalties as defined in paragraph 2, and the right to bilaterally cancel the transaction, where a failing participant does not deliver the financial instruments referred to in Article 5(1) to the receiving participant within 4 business days after the intended settlement date ('extension period') shall be subject to the buy-in whereby those instruments shall be available for settlement and delivered to the receiving participant within an appropriate time frame. Where the transaction relates to a financial instrument traded on an SME growth market the extension period shall be 15 days unless the SME growth market decides to apply a shorter period".
49. Two exemptions apply, as per Article 7(4) CSDR:
    - based on asset type and liquidity of the financial instruments concerned, the extension period may be increased from 4 business days up to a maximum of 7 business days where a shorter extension period would affect the smooth and orderly functioning of the financial markets concerned; and
    - for operations composed of several transactions including securities repurchase or lending agreements, the buy-in referred to in first sub-paragraph shall not apply where the timeframe of these operations is sufficiently short and renders the buy-in ineffective.
50. In developing the draft RTS specifying the extension period, ESMA has considered that a preliminary distinction should carefully be made between asset types. Consideration needs to be given as to which financial instruments will require a longer extension period up to 7 days, and what length could be appropriate to deal with the specific features of such instruments. For example as regards ETFs, a tight deadline for settlement might not be met, given the significant number of underlying financial instruments that need to be bought, for delivery, on several markets. Also instruments such as bonds should have a buy-in regime that takes into consideration factors such as the size and value of typical bond transactions. Besides, for government bonds, a longer buy-in interval would be in line with current market practices and consistent with a wider and more international custody structure that can require more days for delivery.
51. As far as the liquidity of the financial instrument is concerned, the question arises around how less liquid instruments should be identified and what the optimal time-period should be before those securities are subject to a buy-in. This issue needs to be treated with some care as the adverse effects of a buying-in regime could be a decrease in liquidity in certain instruments and an increase in the number of settlement fails where it can prove difficult to obtain the securities for buying-in. While ISD + 4 would appear appropriate if the securities to be bought-in are liquid and not difficult to obtain, certain shares which are not traded frequently may need a longer period to ensure an orderly and robust market, maintaining the continued confidence of issuers and participants who partake in those markets. For instruments that are traded infrequently, where it may be difficult to source securities, the challenge is to ensure that a sufficient period of time is allowed for that transaction to settle before a buy-in is initiated. A risk could arise if a buy-in is conducted on a security that may

already be difficult to source, leading to another fail. As foreseen in CSDR, ESMA will take into account, for the definition of liquidity of the financial instruments, the criteria for assessing liquidity under Articles 2(1)(7a) of MiFIR (definition of liquid market). This could justify a longer period for triggering the buy-in, where a shorter buy-in is counterproductive and would bring undue and disproportionate risks to the infrastructures and potentially the market at large.

Q13: CSDR provides that the extension period shall be based on asset type and liquidity. How would you propose those to be considered? Notably, what asset types should be taken into consideration?

Details of operation of the appropriate buy-in mechanism (Article 7(14)(c))

52. The CSDR intends to provide for uniform rules concerning certain aspects of the buy-in procedure for all transferable securities, money-market instruments, units in collective investment undertakings and emission allowances. To this end, Article 7 CSDR states that any participant to a securities settlement system that does not deliver the financial instruments referred to in Article 5(1) to the receiving participant within the so-called "extension period" shall be subject to a mandatory buy-in procedure that will apply to all transactions on such instruments which are admitted to trading on regulated markets or MTFs, traded on a trading venue or cleared by a CCP. As a consequence, buy-in procedures can be managed by a CSD, a trading venue or a CCP.
53. The key findings of the ESMA survey on buy-in procedures are that the bulk of CSDs do not use buy-in procedures since buy-in are often executed at CCP or trading venue level. The buy-in procedures handled at CSD level entail notices to the concerned parties, execution of the buy-in, cash compensation, and daily penalties.
54. Against this background, it is ESMA's view that a buy-in procedure should at least include:

- notices to the concerned parties, informing them of the activation of the buy-in procedure within a deadline depending on the length of the extension period; in principle, the activation of the buy-in procedure could be notified two or three days before the expiration of the extension period and, as a consequence, for financial instruments to be settled within 4 business days after the intended settlement date, at the end of the market day following the intended settlement date or the following day;

- notices to the concerned parties of the start of the execution of the buy-in at the end of the market day of expiration of the extension period;

- a buy-in execution period starting on the market day following the expiration of the extension period and not longer than XXXX business days;

- notices to the concerned parties of the results of the execution of the buy-in;

- if the buy-in fails or is not possible (see below), deadline for the receiving party to choose between cash compensation and a deferment of the buy-in;

- if a deferred buy-in is chosen by the receiving party, an extension of the execution period not longer than XXXX business days;

- method for the execution of the buy-in (appointment of an intermediary as buy-in agent, auction, any other method).

55. In case the buy-in is only partially successful, the receiving participant has to accept the bought-in securities. For the residual amount cash compensation shall be paid.
56. Article 7(7) envisages the possibility that a buy-in "fails or is not possible", in which case "the receiving participant can choose to be paid a cash compensation or to defer the execution of the buy-in to an appropriate later date ('deferral period')". There may be instances where the CCP, trading venue operator or CSD know in advance that the buy-in cannot be executed by the relevant term because the securities to be bought-in are illiquid and, as a consequence, objectively unavailable. Even more so, a buy-in should be deemed not possible when the securities to be delivered cease to exist, including because the maturity is reached, during the extension period. ESMA is of the opinion that it

should be left to each CCP, trading venue or CSD to decide on the buy-in feasibility, taking into account the parameters to be established in the RTS such as the characteristics of the securities to be bought-in and the relevant contracts/transactions. The decision should be preceded of competent authorities approval and therefore be sent for the CSD supervisors in advance.

57. According to sub-paragraph 3 of Article 7(10), CSDs may monitor the execution of buy-ins with respect to multiple settlement instructions, on the same financial instruments and with the same date of expiry of the execution period, with the aim of minimising the number of buy-ins to be executed and thus the impact on the prices of the relevant financial instruments.

58. This issue becomes particularly important in a cross-CSD settlement, in particular as regards interoperable links and links between CSDs that use a common settlement infrastructure, including links between CSDs that outsource some of their services, related to the operation of such links, to a public entity in accordance with Article 30(5) CSDR – that is, links between CSDs in the context of T2S.

Q14: Do you see the need to specify other minimum requirements for the buy-in mechanism? With regard to the length of the buy-in mechanism, do you have specific suggestions as to the different timelines and in particular would you find a buy-in execution period of 4 business days acceptable for liquid products?

Q15: Under what circumstances can a buy-in be considered not possible? Would you consider beneficial if the technical standard envisaged a coordination of multiple buy-ins on the same financial instruments? How should this take place?

Details of operation of the appropriate buy-in mechanism: operation types and timeframes under which buy-in is deemed ineffective (Article 7(14)(e)

59. Under Article 7(14)(e) ESMA is required to draft RTS specifying the type of operations and timeframes under which a buy-in is deemed ineffective.
Article 7(14)(e) refers to point (b) of paragraph 4, according to which "For operations composed of several transactions including securities repurchase or lending agreements, the buy-in … shall not apply where the timeframe of these operations is sufficiently short and renders the buy-in ineffective". For instance, in a short term repurchase agreement, the buy-in is ineffective when the intended settlement date of the forward leg is earlier than two business days after the expiration of the extension period. Indeed, in such a case, the execution of the buy-in would be useless as the securities could not be received earlier than the intended settlement date of the forward leg, when they are to be delivered again. Even when the intended settlement date of the forward leg is the second business day after the expiration of the extension period, the buy-in will also likely be ineffective.

Q16: In which circumstances would you deem a buy-in to be ineffective?

Calculation of the cash compensation (Article 7(14)(f))

60. Under Article 7(7) CSDR, "If the buy-in fails or is not possible, the receiving participant can choose to be paid a cash compensation or to defer the execution of the buy-in to an appropriate later date ('deferral period'). If the financial instruments are not delivered to the receiving participant at the end of the deferral period, the cash compensation shall be paid. The cash compensation shall be paid to the receiving participant no later than on the second business day after the end of the buy-in period or deferral period, where the deferral period was chosen".
61. Cash compensation is the alternative solution if the security to be bought-in is not available to be delivered. It should be based on the need to "settle" the original trade and it should aim at determining a price for the security, allowing the buyer to be compensated for the fact that he did not receive the securities he bought.
62. Given that, the cash compensation shall only be due when the prices of the financial instruments agreed at the time of the trade are lower than the last publicly available prices for such instruments.
63. As regards the reference price for determining the amount of the cash compensation, for transactions executed on trading venues that price can be the last publicly available price at the trading venue where the trade originally took place. For OTC transactions the reference price could be a specific one or an average market price for such securities across trading venues and/or brokers. Since cash compensations happen in cases where securities are no longer available for a buy-in, it seems reasonable to have more than one pricing source.

Q17: Do you agree on the proposed approach? How would you identify the reference price?

Conditions under which a participant is deemed to consistently and systematically fail to deliver the financial instruments (Article 7(14)(g))

64. In order to set the conditions under which a participant is deemed to consistently and systematically fail to deliver the financial instruments, it is ESMA's view that a proportionate approach should be taken and value, duration and number of fails should be taken into account.
65. In order to avoid considering only failing participants with a large activity, the level of fails of each participant should be weighed on the basis of its own activity. Nevertheless, consideration needs to be given as to the type of instruments/products settled by the failing participant and to the fail rate related to such instruments/products. Considering that the conditions to be set would be the triggers for the suspension of the failing participant, it seems to be reasonable setting thresholds that are able to clearly identify the seriousness and frequency of non-compliance.
66. ESMA is considering the opportunity of setting two quantitative thresholds, the breach of which would trigger the decision-making process to suspend the failing participant. The first threshold would be equal to a certain percentage of the overall value of the settlement instructions submitted by the failing participant over a period of certain months. The second threshold would be equal to another percentage of the number of the settlement instructions submitted by the failing participant over a period of another number of months.

Q18: Would you agree with ESMA's approach? Would you indicate further or different conditions to be considered for the suspension of the failing participant?

Q19: Please, indicate your views on the proposed quantitative thresholds (percentages / months).

Necessary settlement information (Article 7(14)(h))

67. Under this provision CSDs shall provide the necessary settlement information to CCPs and trading venues, in order for buy-ins to be executed, respectively to: (i) transactions cleared by a CCP; and (ii) transactions not cleared by a CCP but executed on a trading venue.
68. In order for CSDs to fulfil this obligation, they need to be able to associate the activity of each clearing member, CCP and participant to a trading venue, to a given securities account. If the clearing member, CCP or participant to a trading venue is a CSD participant, then the securities account in question is the participant's own account. Otherwise, the securities account in question seemingly needs to be in a segregated account opened in the name of the clearing member, CCP or participant to a trading venue.
69. ESMA finds that where the clearing member, CCP or participant to a trading venue is not a CSD participant, the provision under consideration imposes an obligation to open a segregated account on the part of the same clearing member, CCP or participant to a trading venue. A different interpretation would not enable CSDs to provide the necessary settlement information to CCPs and trading venues for the execution of buy-ins.

Q20: What is in your view the settlement information that CSDs need to provide to CCPs and trading venues for the execution of buy-ins? Do you agree with the approach outlined above? If not, please explain what alternative solutions might be used to achieve the same results.

Penalties for settlement fails (Article 7(13))

70. The levels of penalties for settlement fails will be defined in an EC Delegated Act. If ESMA is requested to provide technical advice to the EC on the matter it will consider the possibilities of consulting on the possible elements to be included in such advice.

The processes for collection and redistribution of the cash penalties and any other possible proceeds from such penalties (Article 7(14(b)))

71. Although ESMA is mandated to issue technical standards on the collection and redistribution of the cash penalties and any other possible proceeds from such penalties, this standard will very much depend on the Commission delegated act specifying the parameters for the calculation of a deterrent and proportionate level of cash penalties, for which ESMA has not yet received a mandate for a technical advice. It is therefore expected that ESMA will consult on those aspects at a later stage.

Internalised settlement (Article 9(2) and (3))

72. Under Article 9, ESMA is expected to develop draft RTS which specify the content of internalised settlement reporting and ITS on the format and timing of such reporting.
73. Settlement internalisers are defined as „*any institution including those authorised in accordance with Directive 2013/36/EU or with Directive.../..../EU [new MiFID] which executes transfer orders on behalf of clients or on its own account other than through a securities settlement system*".
74. It must be noted that settlement internalisation (i) should not be confused with the term systematic internaliser which is a practice at trading level and which is dealt with by MIFID; and (ii) that the practice of netting positions at a Central Counterparty (CCP)/clearing member level should not be covered by this definition and was therefore not considered.
75. ESMA did consider the Report on the outcome of CEBS's call for evidence on custodian banks' internalisation of settlement and CCP-like activities[15].
76. Given the specific requirements on settlement discipline under the CSDR, as well as the prudential and organisational requirements applicable to CSDs, and the fact that these do not cover institutions which execute transfer orders on behalf of clients or on their own account other than through a securities settlement system, ESMA believes it is extremely important for competent authorities and for ESMA to monitor the settlement internalisers' activity, in order to determine the scale of this activity (as well as any potential significant movement of settlement from the securities settlement systems to the books of credit institutions/investment firms, under less stringent conditions), and to be able to identify any related systemic risk. With regard to settlement internalisation reporting, ESMA considers that the following elements should be considered as the minimum reporting requirements from settlement internalisers to competent authorities:

- Settlement internalisers shall report to the competent authorities the aggregated volume and value of all transactions settled outside a securities settlement system on a quarterly basis, within 5 working days of the end of each quarter.
- The above mentioned information should include:
    - the types of financial instruments/products settled;
    - identification of the type of operations;
    - if applicable, the volume and value of failed transfer orders (on the intended/agreed settlement date);
    - if applicable, the underlying causes of failed transfer orders (on the intended/agreed settlement date);
    - if the clients were informed about the place of settlement;
    - if applicable, the method by which the clients were informed about the place of settlement:
        - directly, as defined in a specific contractual agreement or standard terms and conditions;
        - indirectly: the clients agreed via a specific contractual agreement or via the standard terms and conditions to have their securities held in omnibus accounts, and therefore to the possibility of having their transfer orders settled internally;

[15] Published on 17 April 2009 and available at http://www.eba.europa.eu/documents/10180/16151/Report+on+the+outcome+of+the+call+for+evidence+on+custodian+banks+activity.pdf .

- indirectly, through the invoicing structure which informs clients that some transfer orders were settled internally (i.e. CSD fee does not apply);
- indirectly, through an order routing system, via which clients can trace their transfer orders;
- other method (to be specified).

- the procedures used for matching and settling internal transfer orders:
  - the same procedures as for the transfer orders settled via a CSD;
  - specific procedures for automatically matching and settling internal transfer orders (to be specified).
- the procedure used for the cash settlement of transfer orders settled internally;
- the procedures used for reconciling the assets held in the omnibus account with the clients' assets recorded at the level of the settlement internaliser;
- the procedures in place to protect the assets of customers (e.g. segregation of assets);
- the risk management practices in use;
- the framework in place to measure, monitor and manage the credit and liquidity risks in relation the transfer orders settled internally;
- if applicable, rules and procedures defining the finality and irrevocability of the securities and cash transfer orders settled internally.

Q21: Would you agree that the above mentioned requirements are appropriate?

III.II CSD Authorisation

Information to the CA for authorisation (Article 17(8))

77. For the identification of the information that the applicant CSD should provide to the competent authority in the application for authorisation, ESMA has considered the CRA Regulation and the TR provisions under EMIR and also the current national practices, which ESMA assessed via a survey to current CSD supervisors. ESMA aimed at ensuring the global compatibility of the EU requirements, thus permitting EU authorised CSDs to operate on a pan-European basis.
78. ESMA proposes that the draft RTS specifying the information that the applicant CSD should provide to the competent authority in the application for authorisation should cover the main elements presented below and in Annex I to this Discussion Paper. Therefore, the following sub-sections should be read in conjunction with that annex.

CSD identification, policies and procedures, relevant agreements

79. ESMA believes that the application for authorisation should include all details needed to demonstrate compliance with all CSDR and relevant technical standards requirements related to the services provided by a CSD. Pursuant to CSDR, ESMA has considered the need for CSDs to include the minimum information listed in Annex I in their application.
80. These minimum requirements include CSD policies or procedures; financial reports and business plans; organisational requirements (e.g. corporate governance; staffing policies and procedures); conduct of business rules; compliance with requirements for CSD services (e.g. book-entry form; intended settlement dates and preventing fails; integrity of the issue); prudential requirements; CSD links and access requirements.

Q22: Would you agree that the elements above and included in Annex I are appropriate? If not, please indicate the reasons or provide ESMA with further elements which you find could be included in the draft RTS, and any further details to justify their inclusion.

Information to the CA for authorisation - Standard forms, templates and procedures (Article 17(9))

81. An application for CSD authorisation should be provided in an instrument which stores information in a durable medium as defined in Article 2(1)(m) of Directive 2009/65/EC of the European Parliament and of the Council.

82. In addition, CSDs should give a reference number to any documentation submitted as part of their application, in order to allow the CA to easily and quickly identify the information. A list of the provided documents accompanied by their reference number has to be provided by the CSD to the CA covering the following:

- Reference to the list of information to be submitted in accordance with Article [X] of the delegated regulation with regard to regulatory technical standards specifying the details of the application for registration of CSDs adopted pursuant to Article 17(7) of Regulation (EU) No [CSDR];
- Unique reference number of the document;
- Title of the document;
- Chapter or section or page of the document where the information is provided or reason why the information is not provided.

83. With reference to the ITS on standard forms, templates and procedures, ESMA proposes that the CSD application for authorisation should cover the main elements specified in Annex II.

Q23: Do you agree that the above mentioned approach is appropriate? If not, please indicate the reasons or provide ESMA with further elements which could be included in the draft ITS.

Conditions for participations of CSDs in entities which not provide services listed in Sections A and B of the CSDR Annex (Article 18)

84. Article 18(4) determines that an authorised CSD may only have a participation in a legal person whose activities are limited to the provision of services set out in Sections A and B of the CSDR Annex, unless such a participation is approved by its competent authority on the basis that it does not significantly increase the risk profile of the CSD.
85. Recital 25 states that in order to avoid any risk taking by the CSDs in other activities than those subject to authorisation under this Regulation, the activities of the authorised CSDs should be limited to the provision of services covered by their authorisation. Additionally, they should not hold any participation, as defined in the Regulation by reference to the Fourth Council Directive 78/660/EEC of 25 July 1978, based on Article 54(3)(g) of the Treaty, on the annual accounts of certain types of companies, or any ownership, direct or indirect, of 20% or more of the voting rights or capital in any other institutions than the ones providing similar services.
86. An exception is a participation approved by CSDs' competent authorities on the basis that it does not significantly increase their risk profile. This exemption is motivated by the existence of participations of CSDs (e.g. in trading venues and CCPs) which only bring limited risks.
87. The technical standard should specify the conditions under which the competent authorities may approve participations of CSDs to make sure that CSDs are not, by means of a participation in another legal person with activities other than those specified in annexes A and B, subject to additional risks. These criteria may include whether the services provided by that legal person are complementary to the services provided by a CSD, and the extent of the CSD's exposure to liabilities arising from that participation.

Distinction with Articles 46 and 47

88. Article 18 should not be confounded with the provisions in Articles 46 (investment policy) and 47 (capital requirements, retained earnings and reserves) CSDR. ESMA finds that the most prominent risk of a CSD's participation is a decline in the value of a participation (the 'business risk'), as a participation cannot depreciate more than its value (in other words it cannot reach a negative value) and hence the risk is limited to its value.
89. This risk is already addressed by paragraphs 3 and 4 of Article 46. If the participation fulfils the requirements of paragraph 3 its risks are already mitigated (because it fulfils the requirements of highly liquid financial instruments with minimal market and credit risk).
90. In case the participation does not fulfil the requirements of paragraph 3 (which might be more likely in case of a participation in e.g. a non-listed legal person), there seems to be no risk for the continuity of the CSD as paragraph 4 states that the participation cannot be taken into account for reaching the required level of capital (assuming the level of required capital has been adequately determined). A loss of the value of the participation can therefore not cause capital to go below the required level. So it does not seem necessary to address this risk in the technical standard.
91. This leads ESMA to understand that the technical standard should therefore focus on the additional risks of participations in legal persons performing activities other than those specified in annexes A and B.

Guarantees

92. As noted, a participation cannot depreciate more than its value (in other words it cannot reach a negative value) and hence the risk of a participation is limited to its value. However, in case the CSD gives guarantees to the legal person in which it participates, these guarantees would be recognised

and reflected by the CSD on its balance sheet, generally following IFRS. In case the legal person in whom the CSD thus holds a participation defaults, the disbursement of these guarantees may be probable.

93. ESMA therefore proposes to: (i) prohibit any CSD guarantees that lead or may possibly lead to an unlimited liability in virtue of a participation; (ii) allow for limited liabilities, on the condition they are fully capitalised by means of liquid capital items (e.g. retained earnings). These items would only be able to be used in case of guarantee disbursement.

Limit control

94. In addition, for participations in which the CSD has ensured control over its subsidiary, the CSD is assumed to be responsible to act in the best interest of the subsidiary (i.e. fiduciary duty). It is thus expected to make the most favourable decisions for the management and financials of the subsidiary. In case of default of the subsidiary, the CSD may thus face the risk of being found guilty in a court for breach of this fiduciary duty (depending on local laws). As a consequence, the CSD may have to consequently share the liabilities incurred by its subsidiary. These liabilities for the subsidiary may generate financial risks for the CSD.

95. The risk may be addressed by prohibiting CSDs to have participations for which they have ensured control (or run the risk of being regarded as being in control by the relevant authorities or in a litigation case) unless covered by liquid capital items, such as retained earnings, which can only be used in case of materialisation of this risk. Also the CSD should provide independent risk analyses and a legal opinion by an independent law firm to properly quantify the risk and make it evident.

Limit percentage of income from participations

96. A CSD may become dependent on the revenues from the participation for financing the core functions of the CSD. In case of a loss of the revenues, the CSD may have a financing problem and hence ESMA proposes to limit these revenues to 20% of the total income of the CSD, based on the average of the preceding three years, if available. If not available, e.g. for newly established CSDs, the 20% limit should be based on the estimated revenues.

Limit participations to securities chain

97. There might be efficiency reasons for CSDs to participate in other legal persons providing services related to CSDs, but there is no typical need for CSDs to participate in another legal person. Participations in non-regulated legal persons can be an additional source of risk for CSDs, as no stringent rules govern the behaviour of these legal persons. Hence, the technical standards might consider this in limiting the scope of entities in which a CSD can participate on. ESMA finds that participations of CSDs should therefore be limited to the following regulated legal persons providing services within the securities issuing, trading, clearing and settlement chain:

- CCPs;
- TRs;
- Trading venues.

98. As regards these infrastructures, particularly CCPs, potential spill-over of risks from one entity to the other affecting the respective financial resources are possible. CCP's recovery or resolution plans may require the CSD as the owner of the CCP to participate in a loss sharing arrangement, to replen-

ish capital, and other, which may exceed the value of the participation and could in turn have negative impact on the financial soundness and going concern assumption of the CSD.

Q24: Do you see other risks and corresponding mitigating measures? Do CSDs presently have participations in legal persons other than CCPs, TRs and trading venues that should be considered? Would banning CSDs from directly participating in CCPs be advisable, in your view?

Review and evaluation (Article 22(10) and (11))

99. In accordance with Article 22(1), a competent authority should, at least on an annual basis, review the arrangements, strategies, processes and mechanisms implemented by a CSD with respect to compliance with CSDR and evaluate the risks to which the CSD is, or might be, exposed or which it creates for the smooth functioning of securities markets. In that regard, ESMA is expected to draft standards on the information that:

- the CSD shall provide to the competent authority for the purposes of the review;
- the competent authority shall supply to the relevant authorities;
- competent authorities shall supply one another.

100. ESMA finds that authorities should, in a post-crisis context, increase their capabilities for performing ongoing supervision rather than over-relying on ad-hoc supervision. Therefore it is ESMA's intention to ensure that for each review the competent authority has sufficient access to information. ESMA considers that in order to determine the scope of information to be delivered for each review, the RTS should follow the set of requirements which CSD has to comply with under the authorisation process under Article 17 CSDR.
101. Information and documents delivered for the purpose of the review should be provided by a CSD to its competent authority with appropriate frequency defined by the competent authority, but not less than annually.
102. ESMA considers that for the purpose of the review, the CSD should deliver the following:

- a report summarising material changes to the arrangements, strategies, processes and mechanisms either after the authorisation or after the previous review of a CSD;
- documentation modified either after the authorisation procedure foreseen under Article 17 CSDR or after the last review of the CSD;
- information defined to be delivered for each review as detailed below;
- other information that the CSD reasonably deems relevant for the review; and
- any additional information if required by the competent authority.

Details on each of the elements above are provided below.

A report summarising material changes to the arrangements, strategies, processes and mechanisms

103. ESMA considers that for the purpose of the review referred to in Article 22(1) and given the wide scope of the provision, a CSD should deliver a report summarising material changes to the arrangements, strategies, processes and mechanisms implemented by a CSD that were introduced, after the authorisation or after the previous review and the corresponding self-assessment on all the points above. CSDs should, however, be prepared to provide further information or additional explanation if the information included in the report is deemed insufficient by the competent authority and also a self-assessment, where relevant from the CSD perspective or required by the competent authority.

The documentation modified either after the authorisation procedure foreseen under Article 17 CSDR or after the last review of the CSD

104. Taking into account the possible burden of gathering and processing a vast amount of information related to the operation of a CSD, ESMA intends to focus on the quality of the information provided, rather than the number of documents submitted by the CSD for the purposes of the review, to the relevant documentation regarding the arrangements, strategies, processes and mechanism that were modified after the authorisation procedure or after the last review of the CSD. Only relevant documents should be provided. ESMA considers that documents should be delivered in a manner that enables the competent authority to identify all the relevant changes made to the arrangements, strategies, processes and mechanisms implemented by the CSD since authorisation or last review (i.e. changes to information delivered under Article 17 CSDR). Additionally, ESMA considers that the competent authority may request that the introduction of material changes in any of the arrangements, strategies, processes and mechanism be communicated to the competent authority without undue delay.

Information defined to be delivered for each review

105. ESMA considers that a specific category of information and documents which is related to the events that by nature occur on a periodic basis (on annual or more frequent basis) or which refers to material events related to the operation of a CSD, are to be delivered for each review. ESMA expects that a defined list of such documents should include at minimum:

- a complete set of the CSD's latest audited financial statements, including those at consolidated level;
- copies of the minutes from the management body meetings that took place since the last review;
- information on any pending judicial, administrative, arbitration or any other litigation proceedings irrespective of their type, that the CSD may be party to, particularly as regards tax and insolvency matters and where significant financial or reputational costs may be incurred;
- a copy of the results of business continuity of similar exercises performed since the last review;
- information on any technical incidents that occurred in the period covered by the report and affected the smooth functioning of the operated securities settlement system;
- information on all cases of identified conflicts of interest that occurred in the period covered by the report;
- information on measures taken to address the identified technical incidents, settlement fails and conflicts of interest as well as the result thereof;
- information on any identified violations of CSD's policies (compliance, risk management, information security).

106. ESMA considers that the competent authority may request that the occurrence of any of the events listed in this section should also be communicated to the competent authority without undue delay, as well as the reasonable expectation of any such events will occur in the future and the mitigating measures being taken.

Other information

107. It is also key that, having regard to the competent authority's risk evaluation task, the competent authority can request further information related to specific risks and activities. Therefore the competent

authority should be able to define and request further any additional information which it considers necessary to be delivered for each review. This should be harmonised as much as possible in the EU (ESMA's convergence role), to avoid regulatory inconsistencies where not justified.

Q25: Do you consider the approach outlined above adequate, in particular as regards the scope and frequency of information provision and the prompt communication of material changes? If not, please indicate the reasons, an appropriate alternative and the associated costs.

Information from third country CSDs to ESMA for recognition (Article 25)

108. ESMA believes that the development of rules on EU recognition of CSDs should follow the general principle of non-discrimination between EU and non-EU CSDs. This suggests that the definition of the items that a non-EU CSD could provide for EU recognition purposes could be similar to the elements required for the registration of an EU CSD, as defined in Article 17 CSDR, with due adaptations. The adaptations regard the fact that the supervision of the recognised CSD would be performed outside the EU, and ESMA should rely on cooperation with the home supervisor.

Q26: Do you agree with this approach? Please elaborate on any alternative approach illustrating the cost and benefits of it.

Monitoring tools for the risks of CSDs, responsibilities of key personnel, potential conflicts of interest and audit methods (Article 26)

Risk monitoring and responsibilities of the key personnel

109. Article 26(1) requires a CSD to have a clear organisational structure with well-defined, transparent and consistent lines of responsibilities and effective processes to identify, manage, monitor and report the risks to which it is or might be exposed. ESMA recognises that the scope for developing draft RTS on this matter is limited to the monitoring tools for the risks of the CSDs and the responsibilities of the key personnel in respect of those risks. In this respect ESMA notes that the monitoring of risks is an integral part of risk management and relies on a well-functioning and adequate internal control mechanism, sound administration and the availability of reliable accounting data.
110. ESMA is of the view that when monitoring risks the CSD should take an integrated and comprehensive view of all relevant risks. These should include the risks it bears from and poses to its participants and, to the extent practicable, clients, as well as the risks it may be exposed to and pose to other entities such as, but not limited to, linked CSDs, other financial market infrastructures including payment systems and settlement banks, liquidity providers, trading venues and other recover service providers. In order to be in a position to monitor and report all relevant risks, a CSD should employ robust information and risk control systems.
111. With respect to the responsibilities of key personnel, which includes the members of the management body and senior management, ESMA considers that the management body and senior management should assume at least the following responsibilities:

a. Management body responsibilities

- establish well-documented policies, procedures and processes by which the management body and senior management should operate;
- establish clear objectives and strategies for the CSD;
- monitor senior management effectively;
- establish appropriate remuneration policies;
- ensure the set-up and the surveillance of the risk management function and the taking of material risk decisions;
- enable the independence and adequate resources of internal control functions;
- monitor outsourcing arrangements;
- monitor and ensure compliance with all provisions of this Regulation and all other regulatory and supervisory requirements;
- be accountable to shareholders or other owners, employees, participants and other relevant stakeholders;

b. Senior management responsibilities:

- ensuring consistency of the CSD's activities with the objectives and strategy of the CSD as determined by the management body;
- designing and establishing compliance and internal control procedures that promote the CSD's objectives;
- subjecting the internal control procedures to regular review and testing;
- ensuring that sufficient resources are devoted to risk management and compliance;
- be actively involved in the risk control process.

112. ESMA believes that where the management body delegates tasks to committees or sub-committees it should retain the approval decisions that could have a significant impact on the risk profile of the CSD. Hence, the management body should assume final responsibility and accountability for managing the CSD's risks.
113. In order for the key risks to be managed, notably from an internal control perspective as provided for in CSDR, ESMA considers that the CSD should have a dedicated chief risk officer, a dedicated compliance officer, a dedicated chief technology officer and a dedicated independent internal audit and clear and direct reporting lines between these functions and the management body.

c. Conflict of interests

114. Article 26(3) requires a CSD to maintain and operate effective written organisational and administrative arrangement to identify and manage any potential conflicts of interest. ESMA is mandated to draft RTS specifying the potential conflicts of interest in that regard, also at the group level and the circumstances in which it would be appropriate, taking into account potential conflicts of interest between the members of the user committee and the CSD, to share audit findings with the user committee.
115. ESMA considers that arrangements by which the management body and senior management operate should include processes to identify, address and manage potential conflicts of interest of members of the management body and senior management. Furthermore, where a CSD is part of larger group it should consider specific procedures for preventing and managing conflicts of interest including with respect to outsourcing arrangements and the potential misuse of information held in the CSD for other business activities.
116. Potential conflicts of interest are exemplified below.

- Where a member of the management body or senior management of the CSD:
  - has a personal interest in the CSD's use of services, materials and equipment of another business.
  - holds shares in another business or enterprise used by the CSD.
  - has a personal interest in any outsourcing company used by the CSD.
  - has a personal interest in any consultancy used by the CSD.
  - has a personal interest in a business that uses the service of the CSD.
  - seats on the Board or committee of any business used by the CSD or that uses the CSD.
  - is related to anyone who has a significant influence on any company used by the CSD or uses the CSD.
- Where the member of the management body or senior management of the CSD has an indirect conflict with other connected persons.

d. Regular and independent audits

117. Article 26(6) requires a CSD to be subject to regular and independent audits and to have the results be communicated to the management body and be made available to the competent authority. ESMA is asked to draft RTS specifying the audit methods.
118. ESMA considers that the financial statement of a CSD should be audited annually by statutory auditors or audit firms within the meaning of Directive 2006/43/EC of the European Parliament and of the Council.

119. ESMA is further of the view that a CSD should establish and maintain an internal audit function which is separate and independent from the other functions and activities of the CSD and which has the following tasks:

- to establish, implement and maintain an audit plan to examine and evaluate the adequacy and effectiveness of the CSD's systems, internal control mechanisms and governance arrangements;
- to issue recommendations based on the result of work carried out in accordance with the previous item;
- to verify compliance with those recommendations;
- to report internal audit matters to the management body.

120. The internal audit function should have the necessary access to information in order to review all of the CSD's activities and operations, processes and systems, including outsourced activities. Furthermore, assessments should be based on a comprehensive audit plan, which does not preclude that special audits may be performed on an event-driven basis at short notice. A CSD's operations, risk management processes, internal control mechanisms and accounts should be subject to independent audit. Independent audits should be performed, at a least, on an annual basis. Audit planning and review should be approved by the management body.

121. In line with international best practice, ESMA is of the view that internal audit assessments should include an on-going monitoring of the performance of the internal audit activity performed through self-assessment or by other persons within the organisation with sufficient knowledge of internal audit practices. Furthermore, periodic reviews of the internal audit activity should be performed by an external auditor.

Q27: Do the responsibilities and reporting lines of the different key personnel and the audit methods described above appropriately reflect sound and prudent management of the CSD? Do you think there should be further potential conflicts of interest specified? In which circumstances, if any, taking into account potential conflicts of interest between the members of the user committee and the CSD, it would be appropriate not to share the audit report or its findings with the user committee?

Recordkeeping (Article 29(3) and (4))

122. ESMA considers that the key elements to draft technical standards on CSD record keeping should require CSDs to ensure that their records include all information necessary to conduct a comprehensive and accurate reconstruction of the operational process. These should also enable records to be searchable by the following fields at least, forming a set of so-called "master data":
    - link;
    - account;
    - participant;
    - financial instrument;
    - currency;
    - issuer;
    - settlement instruction.

    A process of linkage should be used in order to associate different records that correspond to the same participant, for instance.

123. A list of minimum requirements is contained in Annex III and ESMA is therefore considering the keeping of the following categories of records:
    - stock (e.g. issuers, accounts, securities ID);
    - flow (e.g. moment of entry; trade date; currency; …);
    - business (e.g. types of services offered; penalties; …); and
    - governance and policy (e.g. organisational charts; minutes of meetings; …).
124. This grouping was considered having in mind the current available data in CSDs and the CSDR requirements:
    - the CSDR approach is to enumerate the services (Annexes A to C) in order to define what legal person qualifies as a CSD and these services give rise to a diversified set of data;
    - some data is of a more quantitative and operational nature and relates to the business actually performed - part of this data was therefore sub-categorised by using a stock versus flow approach;
    - the transaction data was sub-classified in "stock", "flow" and "other/business" categories in order to take into consideration the data related to the operations actually performed and the data of a more static or descriptive nature reflecting the type of services offered and the different categories of potential actors and financial instruments involved such as issuers, participants and the instruments issued, maintained or settled;
    - on the business data this is usually already at the CSD's immediate and permanent disposal.
125. On ancillary services a functional approach could be considered. This means that depending on each of the specific ancillary service provided, the CSD will need to keep the records as appropriate from the CSD perspective. Under this approach and differently from the one described under the core services, there is no specific list of documents to be kept. This is to allow the necessary flexibility in the performance of non-core services.
126. The section Ancillary services (AS) under Annex III covers most of ancillary services provided, irrespective of the banking or non-banking nature of the CSD. The recording of each of the individual elements under section AS depends on each of the services rendered, as applicable to each CSD specific case.
127. As for governance and policy records, ESMA considers that CSDs should maintain adequate and orderly records of activities related to its internal organisation and business policy. Those records should be made or updated each time a material change in the relevant documents occurs.

Data keeping and availability / other aspects

128. ESMA also considers that:

- based on the seven main elements enumerated as master data above, ESMA considers that the content of CSD records should concretely and, at least, include all items detailed in Annex III to this DP. ESMA understands that most of these records are already part of the current CSD's record set or that they correspond, at least, to current CSDs activities and elements.
- the records should be retained in a medium that allows the storage of information in a format accessible for future reference by the competent authorities, and in such a form and manner that the following conditions are met: i) it is possible for the competent authorities to access the records readily and to reconstitute each key stage of the processing involved; ii) it is possible to record, trace and retrieve the original content of a record before any corrections or other amendments; and iii) it is not possible for the records to be manipulated or altered;
- all records required to be kept by CSDs should be open to inspection by the competent authority - the CSD should name the relevant person or persons that can, without delay, explain the content of the records maintained;
- at a first stage, a list approach of records to be kept should be followed for the drafting of the standard on transaction and governance and policy records, given the input by the industry - nevertheless, these two lists of data to be kept will not be exhaustive lists, in order to allow for specific requests by the competent authorities in future. In this respect, these lists should be considered minimum requirements for all CSDs and the competent authority at their own discretion may demand further records to be kept by the CSD, keeping in mind the principles of proportionality.

129. ESMA is aware that the costs for maintaining the records vary very much as a function of how the records are maintained, i.e. whether they should be maintained online (immediately available) or if they can be maintained offline (i.e. they can be retrieved within few days delay).
130. CSDR requires that all records are maintained for at least ten years. However, CSDR does not specify the modality according to which they can be stored. ESMA could, therefore, consider to differentiate in the ITS the modality according to which these records should be maintained. This would be particularly relevant for transaction records.
131. ESMA considers that if the CSD maintains the relevant records outside of the Union, no legal or technical impediment should occur to the prompt access to this data. Competent authority should be able to access this data with the same modality and delay as if they were maintained within the Union, notably as regards data protection and privacy rules.
132. As regards format in particular, ESMA may consider a number of standard, open, non-proprietary standards. These may include the LEI for legal entities and a client code for the identification of individuals. This is compatible with EMIR and the international trend for the use of LEI in financial infrastructures (CCPs, TRs and financial and non-financial counterparties to derivatives under EMIR for instance). The BIC has been used in CSDs, and the cost of change may be significant. It must be noted, however, that there would also be a cost for regulators and the industry not to use standardised codes and have different codes (e.g. BIC and LEI) for different infrastructures (e.g. CCPs and CSDs and probably many issuers and brokers). ESMA is therefore considering LEI as the code for identifying legal entities under CSDR.
133. Finally, ESMA might also consider requiring that for transaction records a direct data feed to the competent authority could be envisaged, when requested by the latter.

Q28: Do you agree with this minimum requirements approach? In case of disagreement, what kind of categories or what precise records listed in Annex III would you delete/add?

Q29: What are your views on modality for maintaining and making available such records? How does it impact the current costs of record keeping, in particular with reference to the use of the LEI?

Risks which may justify a refusal of access to participants and procedure in case of refusal (Article 33(5) and (6))

134. For each securities settlement system a CSD operates, it should have publicly disclosed criteria for participation as to allow fair and open access for all legal persons that intend to become participants ('requesting parties').
135. According to Article 33(3) CSDR a CSD may only deny access to a requesting party meeting the criteria referred to in paragraph 1 where it is duly justified in writing and based on a comprehensive risk analysis. For transparency reasons ESMA is of the view that the requirements on which a CSD can refuse access to a legal person should be provided for in the CSD's membership criteria to the extent possible and that the CSD's opportunities to refuse a legal person who fulfils its criteria for participation should be restricted to a number of limited cases.

Reasons which may justify a refusal by a CSD of access to participants

136. Article 33(5) CSDR requires standards specifying the risks which may justify a refusal of CSD access to a potential participant.
137. ESMA is of the view, that the risk analysis referred to in Article 33(5) should include at least the following areas: legal, financial and operational. Below are examples of reasons that may justify a refusal of access within each risk area:

a. Legal risks

- the requesting party is not subject to regulation and/or control by competent authorities;
- the requesting party is not compliant with additional requirements specifically tailored for non-regulated entities;
- the requesting party is not compliant with prudential requirements;
- the requesting party is not able to demonstrate that it has the necessary internal anti-money laundering, anti-terrorism financing and anti-tax evasion measures in place;
- the requesting party could expose the CSD to legal risks arising from the insolvency rules in a third country and the requesting party is not able to provide a satisfactory legal opinion;
- the requesting party is not able to guarantee the confidentiality of commercially sensitive information provided through the system.

b. Financial risks

The requesting party does not have the adequate financial resources to fulfil its obligations towards the CSD or its clients.

c. Operational risks

- the requesting party is not able to demonstrate, that it can adhere to the current risk management rules of the CSD or lacks expertise in that regard;
- the requesting party is not able to demonstrate, that it has the technological ability to participate in the system operated by the CSD;
- the requesting party is not able to demonstrate, that it has the operational capacity to participate in the CSD;
- the requesting party does not have appropriate business continuity plans in place;

- access requires changes at the CSD that would impede the risk management procedure or operational functioning of the system operated by the CSD.

138. In case of complaint by the requesting party and in order to allow a proper assessment by the competent authorities the reasons for refusal should be supported by adequate explanation with a level of detail that allows for understanding the risks related with the provision of services. The reasons should be objective, demonstrable and non-discriminatory.

Q30: Do you agree that the CSD risk analysis performed in order to justify a refusal should include at least the assessment of legal, financial and operational risks? Do you see any other areas of risk that should be required? If so, please provide examples.

Elements of the procedure where a CSD refuses to provide access to a participant

139. As noted above, ESMA is required to develop technical standards specifying the elements of the procedure where a CSD refuses to provide access to a prospective participant as described in Article 33(3) of the CSDR. If access is denied, the CSD should provide the requesting party with full written reasons for its refusal within the stipulated response time of one month of the request.
140. To enhance legal certainty and increase the predictability and transparency of the process for the parties involved, ESMA is of the opinion that the technical standard should include fixed time limits for each step of the procedure and therefore proposes the following:

- in case of refusal, the requesting party should have the right to complain to the competent authority of the CSD that has refused access within 1 month from the receipt of the refusal;
- the competent authority of the CSD should duly examine the complaint by assessing the reasons for refusal and should consult the competent authority of the place of establishment of the requesting party on its assessment of the complaint;
- where the competent authority of the requesting party disagrees with the assessment provided, each of the two authorities may refer the matter to ESMA, who may decide to take action in accordance with the powers conferred on it under Article 19 of Regulation (EU) No 1095/2010 (the Annex considers both cases, and where ESMA is not referred to, the scenario is considered 'standard' and the process takes less 3 months);
- the competent authority of the CSD should provide the requesting party with a reasoned reply. The reply should be provided to the requesting party within 6 months from the submission of the complaint;
- where the refusal by the CSD to grant access to the requesting party is deemed unjustified, the responsible competent authority should issue an order requiring that CSD to grant access to the requesting party;
- the CSD should be required to provide access to the requesting party within 3 months of the order.

Q31: Do you agree that the fixed time frames as outlined above are sufficient and justified? If not, which time frames would you prefer? Please provide reasons to support your answer.

Integrity of the issue (Article 37)

141. Article 37 CSDR details the CSD's duties when it comes to maintaining the integrity of the issue of securities maintained by the CSD. ESMA understands that the scope of the reconciliation process covers all financial instruments maintained by the CSD. Such duties entail an obligation for the CSD to reconcile its records, along with a responsibility to cooperate with other entities involved in the reconciliation process. In this respect, it is useful to distinguish between an internal reconciliation process and an external reconciliation process.

142. In drafting this standard, ESMA will aim at:
- contributing for CSDs to have the necessary procedures and controls to protect the integrity of the issue to help to protect market participants from the consequences of securities inflation;
- cater for both (i) dematerialisation; and (ii) immobilisation of physical financial instruments cases.

Internal Reconciliation

143. Article 37(1) depends upon "internal reconciliation" where the CSD responsibilities do not involve any cooperation or communication with other parties/infrastructures. Where the CSD has received part of a securities issue, paragraph 1 relates to how the CSD should protect the integrity of the part of the issue it has responsibility for (cooperation with the other CSD(s) that received the remainder of the issue is dealt with under Article 37(2)). ESMA considers that appropriate reconciliation measures in this context could include:

- CSD end-to-end auditing to verify that its records are accurate and provide a complete accounting for securities that have been issued into it, in accordance with PFMI 11;
- CSD verification of the total number of securities credited in the accounts in the CSD and comparison with the total number of securities issued into the CSD. This is to be carried out on an ongoing basis for each class of securities. According to information provided to ESMA, Member States' CSDs already perform this. Many also compare, for each category of securities, the previous end of day balance with all settlements made during the day and the current end-of-day balance.
- Where securities are held at a CSD in a physical, immobilised form, CSD specific measures to ensure that the physical securities are not destroyed, stolen, or in other way lost[16]. This is important to avoid events that could result in loss to market participants. It is ESMA's current view that physical securities be protected from theft and destruction. Measures should include at least the use of vaults, the design and location of which ensure a high level of protection against floods, earthquakes, fire and other disasters. The CSD should also perform a daily reconciliation between its own accounts and the vault system records. External audit controls of the vaults, including spot checks, should be performed periodically.

144. Where a security cannot be successfully reconciled, the CSD should not consider that security for settlement, until reconciliation has been performed.

[16] PFMI 10 explanatory note 3.10.4 states that CSDs should have appropriate processes, procedures, and controls to manage the risks of storing and delivering physical assets, such as the risk of theft, loss, counterfeiting, or deterioration of assets.

The specific case of corporate actions

145. Where processing corporate actions that involve a securities issue or transformation (e.g. because of mergers) the risk of undue securities creation or deletion may increase. It is ESMA's view that most CSDs use their standard reconciliation measures when processing corporate actions, but may also have specific reconciliation processes for the most complex corporate events.
146. ESMA is considering whether to require CSDs to implement specific reconciliation measures for corporate actions.

Q32: In your opinion, do the benefits of an extra reconciliation measure consisting in comparing the previous end of day balance with all settlements made during the day and the current end-of-day balance, outweigh the costs? Have you measured such costs? If so, please describe.

Q33: Do you identify other reconciliation measures that a CSD should take to ensure the integrity of an issue (including as regards corporate actions) and that should be considered? If so, please specify which and add cost/benefit considerations.

147. ESMA understands that Article 37(2) does not oblige CSDs to ensure that their participants reconcile their own internal book-entry systems recording their own or clients' holdings of securities with the CSD's records (which would be reconciliation "downstream" with the "lower" link in the holding chain). It is therefore the responsibility of the participants to ensure such reconciliation. However, in order for participants to be able to do so, CSDs should provide them with information on what is recorded in each of the participants' accounts maintained by the CSD.

External reconciliation[17]

148. In line with PFMI11, Article 37(2) is intended to ensure that, if other entities are involved in the reconciliation process for a securities issue, there are adequate cooperation and information exchange measures between the CSD and other entities to maintain the integrity of the issue. It therefore depends upon "external reconciliation", meaning reconciliation requiring the involvement of other parties. As some of the entities explicitly mentioned in Article 37 are specific to certain jurisdictions, a short description of 3 major cases is included below. Although CSDR and the standards are not covering registrars, for instance, they may impact these infrastructures, as these need to reconcile with CSDs subject to CSDR rules.

a. Registrars maintain the legal records of title of physical securities, while the record of legal ownership for the dematerialised securities is maintained by the CSD

Registrars are typically required to cooperate with the CSD to reconcile their records for the dematerialised securities issued by the issuers they act on behalf of. The CSD is responsible for monitoring the reconciliation process to ensure that all securities are reconciled each business day. According to ESMA's understanding of the current reconciliation between CSD and registrars, this is operated as follows:

[17] Article 34(2) CSDR.

- a daily reconciliation of the total balance of the CSD register of securities with the corresponding issuer's record of securities, allowing for all securities deposits and withdrawals;
- a daily reconciliation of the balance of each securities account in the CSD's system which has moved that day, with each balance on the corresponding issuer's record of securities that has moved that day; and
- a periodic reconciliation of all securities balances in a security with all balances on the corresponding issuer's record of securities.

b. Transfer agents

In some jurisdictions, the ownership registers are maintained by transfer agents. These transfer agents might for instance operate investment funds registered in a fund register. In this context, a CSD could hold, as a nominee of its participant(s), parts of the investment funds in its account with the transfer agent. The CSD reconciles on regular, and normally daily, basis, the position it holds with the transfer agent.

c. Common depositories

A common depository supports the issuance and distribution of "Classical Global Notes" (physically held securities) which are settled in the two ICSDs, and is appointed jointly by the ICSDs to act as their representative. The common depository reconciles the positions of the Classical Global Notes with the two ICSDs at the end of the business day.

Prohibition of overdrafts, debit balances and securities creation[18]

149. Allowing overdrafts or debit balances to securities accounts in order to credit other participants' accounts would see the CSD effectively creating securities and undermining the integrity of the issue. This justifies the CSDR provision (Article 37(3)), according to which CSDs should clearly prohibit securities overdrafts, debit balances, and securities creation in their rules.
150. In order to achieve this result, CSDs should apply the double-entry accounting principle. This principle means that for each credit made on the receiving account, there should be a corresponding debit entry on the account of the counterparty delivering the securities. There should be no credit to an account maintained by a CSD without a preceding or simultaneous debit on another of its accounts.

Q34: Do you agree with the approach outlined in these two sections? In your opinion, does the use of the double-entry accounting principle give a sufficiently robust basis for avoiding securities overdrafts, debit balances and securities creation, or should the standard also specify other measures?

Operational risks (Article 45)

151. Under this Article, ESMA is expected to specify a number of the operational risks and the methods to test, address or minimise those risks, including the business continuity policies and disaster recovery plans and methods of assessment.
152. ESMA considers that a definition of operational risk should be included in the RTS, in order to clarify its scope in executing the CSDR mandate. ESMA proposes to follow PFMI17 according to which

[18] Article 37(3) CSDR.

"*operational risk is the risk that deficiencies in information systems, internal processes, and personnel or disruptions from external events will result in the reduction, deterioration or breakdown of services provided by an FMI*".

Q35: Is the above definition sufficient or should the standard contain a further specification of operational risk?

Operational risk management framework

153. All CSDs face operational risks. A CSD should actively identify, monitor and manage the plausible sources of operational risk and establish clear policies and procedures to address them. A CSD should have a robust operational risk-management framework with appropriate systems, policies, procedures and controls to identify, monitor and manage operational risk. ESMA therefore has considered the need for CSDs to have a robust operational risk-management framework, including the following.

a. Risk management system and framework

154. CSD should have rolled out an integrated system to identify, measure, monitor, report on, and mitigate, its operational risk. They should, in that context, a robust operational risk-management framework with appropriate IT systems, policies, procedures and controls. In tandem, the management body should have implemented a framework which contains the principles for identifying, measuring, monitoring, reporting on, and mitigating, operational risk and allocates the relevant responsibilities unambiguously. Operational reliability objectives should be defined clearly and the CSDs should have policies in place to achieve those objectives. The latter serve as benchmarks for the CSD to evaluate its efficiency and effectiveness and assess its performance. Operational reliability objectives should include the CSD's operational performance objectives and committed service-level targets. ESMA believes that these objectives and targets should include qualitative and quantitative measures of operational performance and explicitly state the performance standards the CSD is intending to meet.
155. ESMA therefore finds that the CSD should monitor and assess regularly whether the system is meeting its established objectives and service-level targets. The system's performance should be reported regularly to senior management, relevant management body committees, participants, and authorities.
156. In addition, the CSD's operational objectives should be periodically reviewed to incorporate new technological and business developments. The CSD's operational risk-management framework should include formal change-management and project-management processes to mitigate operational risk arising from operations, policies, procedures and controls. Change-management processes should provide mechanisms for preparing, approving, tracking, testing and implementing all changes to the system. Project-management processes (policies and procedures) should mitigate the risk of any involuntary effects on a CSD's current or future activities due to an upgrade, expansion, or alteration to its service offerings. In particular, these policies and procedures should guide the management, documentation, governance, communication and testing of projects, regardless of whether projects are outsourced or executed in-house.

b. Risk management function and resources

157. The CSD should have a central function for managing operational risk. The CSD should ensure that the risk management function has sufficient authority, resources and access to the management body to ensure that its operations are consistent with the risk-management framework set by the management body, which has final responsibility and accountability for managing the CSD's risks. This function should be responsible for developing strategies, policies and procedures to identify, measure, monitor and report on operational risk and for developing procedures to control operational risk, including any necessary adjustments, and should ensure that they are implemented and used. Insofar as some of these tasks are performed by decentralised units, it should also ensure that these units comply with the instructions of the central function, and that it has adequate resources in the central operational risk management function, in the major internal business lines and in internal audit.

158. Finally, the CSD should employ sufficient, well-qualified personnel, notably via appropriate human resources policies to hire, train, and retain qualified personnel, thereby mitigating the effects of high rates of personnel turnover or key-person risk. It should also have appropriate human resources and risk-management policies to prevent and address wrongdoing, including fraud.

c. Integration of risk management system and reporting

159. The operational risk management system should be integrated into the CSD's day-to-day risk management processes. The CSD should have an appropriate reporting system via which the relevant functions within the CSD are regularly informed about operational risk exposures and material operational loss events. And define decision-making competencies and channels so as to be able to react adequately to this information.

d. Documentation of and compliance with the risk management system

160. The operational risk management system (strategies, policies and procedures) should be adequately documented. The CSD should have routines in place for ensuring compliance with the documented operational risk management system. These should include policies for the treatment of non-compliance with internal rules. It should also have comprehensive and well-documented procedures in place to record, report, analyse, and resolve all operational incidents. After every significant disruption, the CSD should undertake a "post-incident" review to identify the causes and any required improvement to the normal operations or business continuity arrangements. Such reviews should, where relevant, include the CSD's participants.

e. Audit and Testing

161. The operational risk management processes and measurement systems should be subject to regular reviews performed by internal or external auditors. These audits should include both the relevant activities of the internal business units and those of the independent operational risk management function. A CSD should regularly evaluate and, where necessary, adjust the systems for the management of operational risk. CSDs should ensure that data flows and processes associated with the operational risk measurement system are accessible to internal and external auditors without delay. They should also test and review arrangements with participants, operational policies and operational procedures periodically and whenever necessary, especially after significant changes occur to the system or a major incident occurs.

Q36: The above proposed risk management framework for operational risk considers the existing CSDs tools and the latest regulatory views. What additional requirements or details do you propose a risk management system for operational risk to include and why? As always do include cost considerations.

Identification and mitigation of operational risk

a. Identification

162. ESMA considers that risk identification of a CSD should consist in the identification of all threats to the CSD, as well as causes of loss and potential disruption. The risk identification process is, on the one hand proactive, based on regular review of processes in order to identify weak areas and points of failure or based on scenarios of disruption or failure taking into consideration all sources of issues (unavailability of systems, human error, etc.) On the other hand, the risk identification process is also reactive, following an incident. Therefore identification of operational risk should take place via:

- risk scenarios;
- internal loss database and external loss database (in accordance with the PFMIs);
- key-risk indicators.

b. Mitigation

163. ESMA considers that mitigation of operational risk should take into consideration at least:

- internal control systems, which are embedded in a CSD's day-to-day business (adequate management controls, such as setting operational standards, measuring and reviewing performance, correcting deficiencies, prevent or detect financial loss and thus protect all business assets);
- business continuity measures;
- complement controls by seeking to transfer the risk to another party such as through insurance in those circumstances where internal controls do not adequately address risk and eliminating the risk is not a reasonable option.

164. When taking measures to mitigate the risks, it should be taken into account that mitigating measures might bring a risk of their own. The risks inherent to mitigating measures should be taken into account when calculating the global risks involved.

Q37: In your opinion, does the above proposal give a sufficiently robust basis for risk identification and risk mitigation, or should the standard also specify other measures? Which and with what associated costs?

Information technology tools

165. CSDs are heavily dependent on reliable IT systems and as such a CSD should maintain appropriate IT tools, pursuant to Article 45(2) CSDR. In that regard ESMA considers that:
    - CSDs should ensure that its information technology systems including hardware and software components are designed and operated in a way that they are reliable and secure as well as

capable of processing the information necessary for the CSD to perform its activities and operations in a safe and efficient manner. The information technology architecture should be well-documented.

- The systems should be adequate to deal with the CSD's operational needs and the risks the CSD faces, be resilient (including in stressed market conditions) and be scalable (to process additional information, if necessary). In particular the CSD should ensure that it has scalable capacity, adequate to handle increasing stress volumes and to achieve its service level objectives. To this end, the CSD should be able to develop demand forecast models which allow adapting its operational capacity correctly. The CSD should provide for procedures and capacity planning as well as for sufficient redundant capacity to allow the system to process all remaining transactions before the end of the day in circumstances where a major disruption occurs. The CSD should provide for procedures for the introduction of new technology including clear reversion plans.
- In order to ensure a high degree of security in information processing and to enable connectivity with its participants as well as with its service providers, a CSD should base its information technology systems on internationally recognised technical standards and industry best practices. The CSD should subject its systems to stringent testing, simulating stressed conditions, before first-time use, after making significant changes and after a major disruption has occurred. Participants and other interested parties will be involved as appropriate in the design and conduct of these tests.
- A CSD should maintain a robust information security framework that appropriately manages its information security risk. The framework should include appropriate mechanisms, policies and procedures to protect information from unauthorised disclosure (confidentiality), ensure data accuracy and integrity and guarantee the availability of the CSD's services. The information security framework should include, at a minimum, the following mechanisms:

    - access controls to the system;
    - adequate safeguards against intrusions and data misuse;
    - specific devices to preserve data authenticity and integrity, including, but not limiting to cryptographic techniques;
    - reliable networks and procedures for accurate and prompt data transmission without major disruptions; and
    - audit trails.

166. When outsourcing its information technology system or parts of it to another entity or to a third party service provider, the CSD should:

- remain fully responsible for discharging all of its obligations;
- make sure that the relationship and obligations towards its participants or issuers are not altered;
- ensure that supervisory and oversight functions, including on site access to acquire any relevant information needed to authorities, is always possible;
- adopt the necessary systems and controls to manage the risks it faces;
- retain the necessary expertise and resources for evaluating the quality of the services provided, the organisational and capital adequacy of the service provider, for supervising the outsourced services effectively and for managing the risks associated with the outsourcing on an ongoing basis;
- have direct access to the relevant information of the outsourced services;
- ensure that the service provider cooperates with the competent authority and the relevant authorities referred to in Article 12 in connection with the outsourced activities;

- ensure that the service provider meets the standards set down by the relevant data protection legislation which would apply if the service providers were established in the Union, making sure that those standards are set out in a contract between the parties and that those standards are maintained;
- define in a written agreement its rights and obligations and those of the service provider, including the possibility of the CSD to terminate the agreement;
- make available and ensure that the service provider make available upon request to the competent authority and the relevant authorities referred to in Article 12 all information necessary to enable them to assess the compliance of the outsourced activities with the requirements of this Regulation.

ESMA finds that the above is only valid without prejudice of Article 30(5) CSDR[19]. Also, the CSD should have adequate and documented arrangements for the selection of such entities or service providers.

167. The information technology systems and the information security framework should be reviewed, at a minimum, on an annual basis. They should be subject to independent audit assessments and the results of these assessments should be reported to the management body and should be made available to the competent authority.

Q38: What are your views on the possible requirements for IT systems described above and the potential costs involved for implementing such requirements?

Business continuity policy

168. Under Article 45(7), ESMA is required to develop technical standards indicating, inter alia, methods to test, address or minimise operational risks, including the business continuity policies and disaster recovery plans and the methods of assessment thereof. Given the systemic importance of CSDs, the continued and uninterrupted functioning of a CSD is of crucial importance for the stability of the financial markets. Having this in mind, ESMA considers that:

- CSDs should have a business continuity policy and a disaster recovery plan approved by the management body and subject to independent reviews which are reported to the management body.
- The business continuity policy should identify all critical business functions and related systems, and include the CSD's strategy, policy, and objectives towards the continuity of these functions and systems. In doing so, external links and interdependencies within the financial infrastructure (e.g. trading venues and central counterparties, other securities settlement systems and payment systems, participants), as well as outsourced functions or services should be duly considered in the business continuity policy.
- The business continuity policy and the disaster recovery plan should contain clearly defined and documented arrangements for use in the event of a business continuity emergency, disaster or crisis which are designed to ensure a minimum service level of critical functions.

[19] ..where a CSD outsources some of its services or activities to a public entity and where that outsourcing is governed by a dedicated legal, regulatory and operational framework which has been jointly agreed and formalised by the public entity and the relevant CSD and agreed by the competent authorities...'.

- The disaster recovery plan should identify for critical functions the recovery point and recovery time objectives and determine the most suitable recovery strategy for each of these functions. In determining the recovery times for each function the CSD should take into account the overall impact on the market efficiency. At a minimum, such arrangements should ensure that in extreme scenarios critical functions are completed on time (in line with the recovery time specified below) and agreed service levels are met.
- A CSD's business continuity policy should identify the maximum acceptable down time of critical functions and systems. Backup systems should commence processing immediately with a maximum recovery time for the CSD's critical functions of 2 hours. Settlement should be completed by the end of day in all circumstances. The status of all transactions at the time of disruption should be identified with certainty in a timely manner.
- CSDs should conduct:
    - A business impact analysis to identify the critical functions for which a minimum service level should be maintained.
    - A proper scenario based risk analysis of these critical functions. In particular they should take into account dependencies on external providers (e.g. utilities) and manage such dependencies through appropriate contractual and organisational arrangements.

169. ESMA finds that the business impact analysis and the scenario analysis should be kept up to date and be reviewed at least on annual basis and also following an incident or significant operational changes. The analysis should take into account all relevant developments, including market and technology developments.
170. Additionally, ESMA believes that CSDs should have in place arrangements to ensure the continuity of their critical functions based on disaster scenarios - including (cyber) attacks, intrusions, natural disasters and pandemic situations - that at least address:

- the availability of adequate human resources;
- the maximum downtime of critical functions;
- the maintenance of a secondary processing site, as provided under Article 45(4) CSDR, with resources, capabilities, functionalities and staffing arrangements adequate to the CSD's operational needs and the risks the CSD faces in order to allow the secondary site to take over operations if needed; the secondary processing site should have a geographically distinct risk profile from the primary site so that it should in principle not be affected by an event that affects the primary site;
- the maintenance or the immediate access to a secondary business site, at least, to allow staff to ensure continuity of the service if the main location of business is not available.

171. To be up-to-date, ready to be used and effective, the business continuity policy and disaster recovery plans and the relevant arrangements should, in ESMA's view, be tested and monitored at regular intervals, at least once every 12 months, and after significant modifications or changes to the systems or related functions. Tests should be planned and documented and should involve at least:

- scenarios of large scale disasters;
- switchovers between primary and secondary sites;
- the participation of customers, external providers and relevant institutions with which interdependencies have been identified in the business continuity policy.

172. ESMA is also of the understanding that CSDs should also regularly review and update their business continuity policies and disaster recovery plans to include all critical functions and the most suitable recovery strategy for them. Updates to the business continuity policy and disaster recovery plan should take into consideration the outcome of the tests and recommendations of independent reviews and other reviews and of competent authorities. CSDs should review their business continuity policies and disaster recovery plans after every significant disruption, to identify the causes, and any required improvement to the CSD' operations, business continuity policies and disaster recovery plans. Finally, every CSD should have a well-documented communication plan to ensure the adequate and up to date information and contact points the relevant stakeholders could rely on during a disruption.

Q39: What elements should be taken into account when considering the adequacy of resources, capabilities, functionalities and staffing arrangements of the secondary processing site and a geographic risk profile distinct from that of the primary site?

a. Interdependencies

173. ESMA considers that before granting access the CSD should assess its ability to meet high operational standards and the potential risks to its operations, for each key participant, for utility providers, critical service providers and other CSDs or market infrastructures.

b. Participants

174. ESMA finds that the CSD should identify both direct and indirect effects on its ability to process and settle transaction in the normal course of business and manage risks that stem from an external operational failure of connected entities. To manage the operational risks associated with its participants, a CSD should consider establishing minimum operational requirements for its participants, e.g. a CSD may want to define operational and business continuity requirements for participants in accordance with the participant's role and importance to the system. A CSD has to identify critical participants based on transaction volumes and values, services provided to the CSD and other interdependent systems and, more generally, the potential impact on other participants and the system as a whole in the event of a significant operational problem. The CSD should have clear and transparent criteria, methodologies, or standards for critical participants to ensure that their operational risks are managed appropriately.

c. Utility providers and critical service providers

175. Normally a CSD is typically dependent on the adequate functioning of utilities and critical service providers. As a result the CSD should identify the risks from utilities and critical service providers and take appropriate actions to manage these dependencies through adequate contractual and organisational arrangements. The CSD should inform its relevant authorities about any such dependencies on utilities and critical service providers and take measures to allow these authorities to be informed about the performance of these utilities and critical service providers. The CSD should provide full information to the authority.

d. Links to other FMIs

176. ESMA considers that CSDs and linked FMIs should provide an appropriate level of information about their operations to each other in order for each FMI to perform effective periodic assessments of the operational risk associated with the link. In particular, FMIs should ensure that risk-management arrangements and processing capacity are sufficiently scalable and reliable to operate the link safely. Systems and communication arrangements between linked FMIs also should be reliable and secure so that the link does not pose significant operational risk to the linked FMIs. Any reliance by a linked FMI on a critical service provider should be disclosed as appropriate to the other FMI. Governance arrangements and change-management processes should ensure that changes in one FMI will not inhibit the smooth functioning of the link, related risk-management arrangements, or non-discriminatory access to the link, in similar terms to the forts on links under Article 48(10).

Q40: In your opinion, will these requirements for CSDs be a good basis for identifying, monitoring and managing the risks that key participants, utility providers and other FMIs pose to the operations of the CSDs? Would you consider other requirements? Which and why?

Investment policy (Article 46)

177. Under this RTS ESMA should specify the financial instruments that can be considered as highly liquid with minimal market and credit risk a CSD can invest in, the appropriate timeframe for access to assets and the concentration limits.
178. In case of assets do not fulfil the requirements referred to in the previous paragraph, there is no risk for the continuity of the CSD as, according to paragraph 4, such assets cannot be taken into account for reaching the required level of capital (assuming the level of required capital has been adequately determined). A loss of the value of the assets can therefore not cause capital to go below the required level.
179. The RTS will apply irrespective of the services offered and/or functions performed by the CSD. When a CSD is authorised to provide banking type of ancillary services from within the same legal entity, it also remains subject to the prudential requirements, as listed in Article 59(3) CSDR.

Highly liquid

180. CSDs may in practice tend to keep their assets as liquid as possible, mostly in cash and less so in financial instruments. Due to the similarity in the wording of Article 46(3) CSDR with Article 47(1) EMIR and as specified in Article 46(6) CSDR, ESMA intends to include similar (but not entirely identical) conditions applicable to highly liquid financial instruments, as listed in Annex II of Commission Delegated Regulation 153/2013 of 19 December 2012 regarding RTS for CCPs.
181. This approach could envisage that an asset is only highly liquid with minimal market and credit risk when it meets the following factors:
    - In the case of financial instruments, debt instruments which (i) have low credit risk, market risk, volatility and inflation risk; (ii) do not have an average duration greater than two years until maturity; (iii) are freely transferable and without any regulatory legal constraints that impairs liquidation; (iv) have an active outright sale or repurchase agreement market at all times with a diverse group of buyers and sellers; (v) have price data published on a regular basis; and (vi) have been issued or are explicitly guaranteed by a government, a central bank, a multilateral development bank as listed under section 4.2 of part I of Annex VI to Directive 2006/48/EC, the European Financial Stability Facility or the European Stability Mechanism.
    - In the case of cash equivalent financial instruments, certificates of deposit, savings accounts and current accounts which are claims on: i) a central bank in the location where the CSD is established; ii) a central bank of issue of a currency in which the CSD settles transactions; iii) credit institutions with a low credit risk and to which the CSD has prompt access when required.
182. Moreover, ESMA considers that CSDs should only invest in assets where disinvestment is possible easily in times of need. CSDs should not be allowed, as principle, to consider their investment in derivatives to hedge their interest rate, currency or other exposures. Investment in derivatives would expose the CSD to additional risks which are not typical for the settlement activity.

Appropriate timeframe for access to assets

183. In order to safeguard continuity of services by the CSD, it should have sound policies and procedures to enable rapid accessibility and availability of its assets, when required. 'Prompt access' implies immediacy, but remains subject to a number of factors, such as the nature, quality and the maturity of its assets. When defining its investment policy, the CSD should take the need for prompt access into account in the selection/diversification of its assets (including if and when assets are held in foreign jurisdictions) and when entering into agreements with third parties for the custody

and safekeeping of these assets. The phrase 'when required' refers to the needs of the CSD for making its financial assets available. Accessibility to assets should be - as much as possible - independent from the market circumstances, i.e. under normal market circumstances and in times of higher market volatility.

Concentration limits

184. ESMA's preliminary thinking is that a CSD should establish and implement policies and procedures to ensure that exposures to institutions that it holds its financial resources will remain within acceptable concentration limits by applying sufficient diversification. Exposures should be assessed on both an individual entity by entity and an aggregated basis. If concentration is perceived in aggregate, the relevant exposures should be treated as a single risk. In this context, the CSD should give consideration to the interconnections between credit institutions that are also major participants in the CSD. In order to keep the policies and procedures up-to-date, these should be subject to regular review and (when and where deemed necessary) adaptation by the CSD. If and when concentration limits are surpassed, the CSD should take appropriate measures to bring the exposures within the limits, without any delay.

Q41: Do you agree with the approach outlined above? In particular, do you agree with the approach of not distinguishing between CSDs that do not provide banking services and CSDs that do so?

Q42: Should ESMA consider other elements to define highly liquid financial instruments, 'prompt access' and concentration limits? If so, which, and why?

CSD links (Article 48)

185. A CSD link is defined in Article 2(28) CSDR as an arrangement between CSDs, whereby one CSD becomes a participant ('requesting CSD') in the securities settlement system of another CSD ('receiving CSD') in order to facilitate the transfer of securities from the participants of the latter CSD to the participants of the former CSD, or accesses the other CSD indirectly via an intermediary. In the CSDR, links are categorised as standard links, customised links, indirect links or interoperable links.
186. Article 48(10) CSDR requires ESMA to specify the conditions under which each type of link arrangement provides for adequate protection of the linked CSDs and of their participants.
187. This protection regards in particular possible credits taken by CSDs and the concentration and liquidity risks as a result of the link arrangement when a CSD intends to participate in the securities settlement system operated by another CSD, the monitoring and managing of additional risks arising from the use of indirect links or intermediaries and reconciliation methods. ESMA is also to specify the cases where DVP settlement through CSD links is practical and feasible and the methods of assessment thereof.

Protection of the linked CSDs and their participants in different types of link arrangements

188. Before entering into a link arrangement the CSDs shall identify and assess all potential sources of risk. ESMA considers that the risks associated with link arrangements can be categorised as follows:

- **Legal risks**
  - risks deriving from the application of different laws or existence of different regimes amongst – or within – jurisdictions, e.g. differences in the law governing settlement finality.

- **Operational risks**
  - risks, deriving from system reliability and scalability;
  - risks, deriving from the need for the CSDs to exchange information, e.g. whether the counterparties to an securities transaction have the securities and the funds necessary to complete the settlement.
  - risks, related to the processing and reconciliation of securities transfers and corporate action events.

- **Financial risks**
  - credit and liquidity risk;
  - risks arising from insolvency issues.

Standard and customised links

189. ESMA is of the view that customised links and standard links should be treated equally from a risk perspective. Customisation is normally intended to reduce operational risk by providing for better efficiency and more automation in the communication procedures. There may be additional reasons for, or configurations of, customised links, and these should be assessed appropriately.

190. To provide the linked CSDs and the participants with adequate protection, ESMA considers, that for the establishment of a standard or customised link as defined in CSDR:

- the requesting CSD ensures that the risks can be assessed and managed and made transparent to its participants
- the requesting CSD meets the receiving CSD's participation requirements;
- the requesting CSD has conducted an extensive analysis of the receiving CSD's financial soundness, governance arrangements, processing capacity, operational reliability and reliance on a critical service provider and has taken the necessary measures to monitor and manage the issues that may arise from such analysis;
- the requesting CSD has taken steps to ensure that the choice of law that governs each aspect of the link's operations recognises the finality of settlement of payment and delivery arrangements and the enforceability of the netting methods in the receiving CSD's jurisdiction;
- measures have been taken to ensure segregation, both on an omnibus and individual basis and to prevent unauthorised use of the securities held by the requesting CSD at the receiving CSD;
- the requesting CSD has taken measures to adequately protect the assets of its participants in the event of insolvency of the receiving CSD or one of its major participants;
- the link has been adequately tested before becoming operational; and
- an emergency plan is available in the event the settlement system of the linked CSD malfunctions or breaks down, defining these situation and the actions to be taken.

DvP links vs FoP links

191. ESMA also believes that it may be necessary to distinguish between free of payment (FoP) links and links designed for DvP. Article 2(26) CSDR defines DvP as a securities settlement mechanism linking a transfer of securities with a transfer of funds in a way that the delivery of securities occurs if and only if the corresponding transfer of funds occurs and vice versa. DvP is generally accepted as a key measure to reduce or eliminate principal risk in securities settlement systems, that is, the risk that the seller of a security could deliver the security but not receive payment or that the buyer of a security could make payment but not receive delivery of the security. DvP settlement in a link is preferred but any additional risks as a result of the cash settlement must be assessed and mitigated. Therefore ESMA considers that in addition to the conditions stated above, the establishment of a delivery versus payment link should be conditioned on at least:

- any credit and liquidity risks arising between the CSDs are being managed;
- CSDs that use an intermediary for the cash settlement ensure that the intermediary will perform as expected (e.g. via due diligence; SLA; …); and

- standards are being agreed between the linked CSDs concerning communication and operational issues related to the cash settlement.

Interoperable links

192. CSD links whereby the CSDs agree to establish mutual technical solutions for settlement in the securities settlement systems that they operate (interoperable links, as per Article 2(32) CSDR) require an advanced form of relationship between CSDs. This may expose the linked CSDs and their participants to additional risks and should be governed by clear legal agreements.
193. ESMA considers that in addition to the above and to the conditions for standard and customised links, including the conditions for DvP links when applicable, the establishment of an interoperable link should be conditioned to:

- standards are agreed between the CSDs concerning reconciliation, the operating hours for particular processes, corporate action processing and cut-off times;

- the interoperable CSDs have established a common IT interface for transmission of instructions between the CSDs, and common communication procedures;

- DvP settlement is allowed and measures have been taken to synchronise settlement batches (where settlement occurs in batches) and with respect to other related issues;

- common risk management models are in place between the interoperable CSDs including adequate collateral arrangements;

- common contingency and default procedures are in place between the interoperable CSDs.

Q43: Do you agree that links should be conditioned on the elements mentioned above? Would there be any additional risks that you find should be considered, or a different consideration of the different link types and risks? Please elaborate and present cost and benefit elements supporting your position.

Monitoring and managing additional risks arising from indirect links and the use of intermediaries

194. According to Article 48(5) CSDR a CSD that uses an indirect link or an intermediary to operate a CSD link with another CSD shall measure, monitor, and manage the additional risks arising from the use of that indirect link or intermediary. An 'indirect link' is defined in Article 2(33) of the CSDR as an arrangement between a CSD and a third party other than a CSD that is a participant to the securities settlement system of another CSD. Such link is set up by a CSD in order to facilitate the transfer of securities to its participants from the participants of another CSD. The conditions for standard and customised links also apply to indirect links. According to the PFMIs, the primary source of additional risk in this context stems from custody risk, i.e. the risk of loss on the securities held via the intermediary in the event of the intermediary's insolvency, negligence, fraud, poor administration, or inadequate recordkeeping. Therefore it is ESMA's view that a CSD that uses an intermediary to operate a CSD link with another CSD should have monitoring and managing proce-

dures in place in addition to those stated above for standard and customised links, that enables the requesting CSD to:

- ensure that the intermediary used is a supervised and regulated entity with robust accounting practices and internal controls;
- ensure that the intermediary has well-functioning routines/systems for handling the services provided, e.g. securities transfers, safekeeping and corporate actions;
- ensure that any credit and liquidity risks are being managed (if applicable);
- ensure that the intermediary has the financial means to cover any securities losses that a custodian may be liable for;
- ensure that the securities held with the intermediary are protected against the intermediary's creditors and are subject to adequate segregation and transfer arrangements;
- ensure that the requesting CSD has good insight/knowledge into the continuity arrangements between intermediary and receiving CSD;
- access the securities at all times;
- perform a yearly due diligence to monitor the above;
- ensure that proceeds from settlement are promptly transferred to the requesting CSD.

Q44: Do you find the procedures mentioned above adequate to monitor and manage the additional risk arising from the use of intermediaries?

Reconciliation methods

195. Article 48(6) CSDR provides that linked CSDs shall have robust reconciliation procedures to ensure that their respective records are accurate.
196. It is ESMA's view that the reconciliation methods used should at least include:

- Daily statements of information from the receiving CSD to the requesting CSD (in cases of indirect links, via an intermediary) specifying per account number and ISIN-number:
    - the aggregated opening balance;
    - the aggregated closing balance;
    - the individual movements.
- Daily comparison by the requesting CSD of the opening balance and the closing balance communicated by the receiving CSD with the records maintained by the requesting CSD itself.

Identification, investigation and rectification of discrepancies

197. As regards interoperable links, as well as in the context of the common depositories, ESMA considers that they should reconcile their positions among themselves and with the common depository, or the issuer or another CSD as the case may be, on a daily basis.

Q45: Do you agree with the elements of the reconciliation method mentioned above? What would the costs be in the particular case of interoperable CSDs?

DVP settlement

198. Article 48(7) CSDR provides that links between CSDs shall permit DvP settlement of transactions between participants in linked CSDs, wherever practical and feasible. Settlement in central bank money (CeBM) is to be recommended, but ESMA recognises the fact that settlement in CeBM, in some cases, is dependent on the requesting CSD or its participant's ability to access the central banks payment system used by the receiving CSD.
199. ESMA considers that a link between CSDs enabling DvP settlement of transactions between participants in the linked CSDs demonstrates that DvP is practicable and feasible, where:

- there is a market demand for DvP settlement, i.e. the link is intended to facilitate the settlement of a transaction between participants' of the linked CSDs as compared to a link arrangement designed to support e.g. securities lending, collateral arrangements or dual listings that may only require FoP transfers;

- the volume/value of the DvP transactions processed through the link is economically justifiable;

- there is a safe and efficient access to cash in the currency of the receiving CSD for the requesting CSD and/or its participants.

200. On the last indent it should be noted that the most suitable payment solution will to a large extent depend on the cash services provided by the requesting and the receiving CSD. Therefore, DvP may be facilitated in two cases:

- if the requesting CSD provides banking services (as it may act as a paying agent on behalf of its participants to enable DvP settlement in the receiving CSD); or

- the receiving CSD offers cash accounts and the participant of the requesting CSD can open a cash account directly with the receiving CSD for payment purposes.

Q46: Do you agree that DvP settlement through CSD links is practical and feasible in each of the cases mentioned above? If not explain why and what cases you would envisage.

Reasons which may justify a refusal of access to issuers and the procedure in case of refusal (Article 49(5) and (6))

201. In many Member States issuers are required by national law to issue certain types of securities, notably shares, within their national CSDs. In order to remove this barrier to the smooth functioning of the Union post-trading market and to allow issuers to opt for the most efficient way for managing their securities, issuers should have the right to choose any CSD established in the Union for recording their securities and receiving any relevant CSD services.
202. Article 49(1) CSDR states that an issuer shall have the right to arrange for its securities admitted to trading on regulated markets or MTFs or traded on trading venues to be recorded in any CSD established in any Member State.
203. However, it is the general view that without prejudice to this freedom of issuers, the national corporate law or other similar law of the Member State under which the securities are constituted shall continue to apply. This is more relevant for shares, where the national rules of corporate law of the issuer may impose certain requirements on the issuer CSD since they impact on the management of corporate actions and thus, ultimately, on investors' rights. CSDs should therefore not be obliged to accept any requesting issuer from another Member State.
204. Article 49(3) CSDR allows a CSD to refuse an issuer access if the CSD does not offer notary services in relation to securities constituted under the corporate law or other similar law of the relevant Member State. A CSD may also refuse to provide services to an issuer due to reasons based on a comprehensive risk analysis.
205. It should be noted that if a CSD wishes to provide notary services to an issuer of financial instruments constituted under the law of another Member State the CSD shall be subject to the procedure referred to in Article 23 CSDR, on freedom to provide services in another Member State.

Reasons which may justify a refusal by a CSD of access to issuers

206. Article 49(5) CSDR requires ESMA to develop standards specifying the risks which may justify a refusal by a CSD. ESMA's view is that such a risk analysis should include at least the following areas: legal, financial and operational risk. Below are examples of such risks within each area that may be considered in the assessment.

a. Legal risks

- The issuer does not provide the information needed to assess its compliance with the CSD's rules and requirements;
- The securities to be recorded do not meet the CSD's requirements for registration in its accounts;
- The issuer cannot guarantee that the shares have been properly issued, i.e. integrity of the issue, and that there is no discrimination between shareholders in the home and other member states;
- The requesting issuer could expose the CSD to legal risks arising from the insolvency rules in a third country and the issuer is not able to provide a satisfactory legal opinion;
- The Member State of the issuer fails to supply ESMA or the CSD with the list of relevant provisions of their laws as stated in Article 49(1).

b. Financial risks

The issuer does not have the adequate financial resources to fulfil its obligations towards the CSD.

c. Operational risks

- Access requires the CSD to implement extensive manual processing, increasing the risk of human error, either due to the increased complexity of the process or due to the costs for implementing automated processing;
- The CSD's system may not be able to handle the currency requested by the issuer.

207. In order to allow a proper assessment of the requesting issuer and, in case of complaint, by the competent authority of the CSD, the reasons for refusal should be supported by adequate explanation with a level of detail that allows for understanding the risks related with the provision of services. The reasons should be objective, demonstrable and non-discriminatory.

Q47: Do you agree that the risk analysis performed by the CSD in order to justify a refusal to ofter its services to an issuer should at least include legal, financial and operational risks? Do you see any other areas of risk that should be considered? If so, please give examples.

d. Elements of the procedure where a CSD refuses to provide services to an issuer

208. The CSDR states that a CSD, under certain circumstances, may refuse to provide services to an issuer. Where a CSD refuses to provide its services to an issuer, it should provide the requesting issuer with full written reasons for its refusal within the stipulated response time of three months of the issuer's request.
209. ESMA, in close cooperation with members of the ESCB, is required to develop technical standards specifying the elements of the procedure where a CSD refuses to provide services to an issuer as described in Article 49(4) of the CSDR.
210. To enhance legal certainty and to increase the predictability and transparency of the process for the parties involved, ESMA is of the opinion that the technical standard should include fixed time limits for each step of the procedure and therefore proposes the following:

- In case of refusal, the requesting issuer should have a right to complain to the competent authority of the CSD that refuses to provide its services. Such a complaint should be submitted to the competent authority within 1 month of the CSD's refusal.
- The competent authority of the CSD should duly examine the complaint by assessing the reasons for refusal provided by the CSD and should also consult the competent authority of the place of establishment of the requesting issuer on its assessment of the complaint.
- Where the authority of the requesting party disagrees with the assessment provided, each of the two authorities may refer the matter to ESMA, who may decide to take actions in accordance with the powers conferred on it under Article 19 of Regulation (EU) No 1095/2010 (the Annex considers both cases, and where ESMA is not referred to, the scenario is considered 'standard' and the process takes less 3 months).

- The competent authority should thereafter provide the issuer with a reasoned reply. The reply should be provided to the requesting issuer within 6 months of the submission of the complaint.
- Where the refusal by the CSD to provide its services to an issuer is deemed unjustified, the responsible competent authority should issue an order requiring the CSD to provide its services to the requesting issuer. The CSD should be required to admit the securities of the requesting issuer within 3-8 months of the order.

Q48: Do you agree that the time frames as outlined in the procedure above are sufficient and justifiable? If not, which time frames would you prefer? Please provide reasons to support your answer.

CSD links: procedure in case of refusal of access (Article 52(3) and (4))

211. Article 52(1) CSDR provides that a CSD ("receiving CSD") should treat a request by another CSD ("requesting CSD") to set up a standard link or a customised link promptly and provide a response within three months. ESMA is expected to draft standards specifying the risks to be taken into account by CSDs when carrying out a comprehensive risk assessment, and competent authorities assessing the reasons for refusal and the elements of the procedures and the related standard forms and templates.
212. According to Article 52(2) CSDR a receiving CSD may only deny access to a requesting CSD where such access would threaten the smooth and orderly functioning of the financial markets or cause systemic risk. Such refusal must be based on a comprehensive risk analysis and must be accompanied with the receiving CSD's full reasons for refusing.
213. The risks to be taken into account by CSDs when carrying out a comprehensive risk assessment, and competent authorities assessing the reasons for refusal, are already covered in this DP section on Article 48 (links). Below some considerations have been included on the procedures.

Elements of the procedure where a CSD refuses to provide services to a requesting CSD

214. CSDR states that a CSD, under certain circumstances, may refuse access to a requesting CSD. If access is denied, the CSD should provide the requesting CSD with full written reasons for its refusal within the stipulated three months from the request.
215. ESMA, in close cooperation with members of the ESCB, is required to develop draft technical standards specifying the elements of the procedure where a CSD refuses access to a requesting CSD as described in Article 52(2) CSDR.
216. To enhance legal certainty and increase the predictability and transparency of the process for the parties involved, ESMA considers that the technical standard should include a set of fixed time limits for each step of the procedure and therefore proposes the following:

- In case of refusal, the requesting CSD should have the right to complain to the competent authority of the CSD that has refused access within 1 month from the receipt of the refusal.
- The competent authority of the receiving CSD should duly examine the complaint by assessing the reasons for refusal and should consult the competent authority of the requesting CSD and the relevant authority of the requesting CSD referred to in point (a) of Article 12(1) on its assessment of the complaint.
- Where any of the authorities of the requesting party disagrees with the assessment provided, any one of the authorities may refer the matter to ESMA, who may decide to take actions in accordance with the powers conferred on it under Article 19 of Regulation (EU) No 1095/2010 (the Annex considers both cases, and where ESMA is not referred to, the scenario is considered 'standard' and the process takes less 3 months).
- The competent authority of the receiving CSD should provide the requesting CSD with a reasoned reply within 6 months from the submission of the complaint.
- Where the refusal by the CSD to grant access to the requesting CSD is deemed unjustified, the competent authority of the receiving CSD should issue an order requiring the receiving CSD to grant access to the requesting CSD. The CSD should be required to provide access to the requesting CSD within 3-8 months of the order.

Q49: Do you agree that the time frames as outlined in the procedure above are sufficient and justifiable? If not, which time frames would you prefer? Please provide reasons to support your answer.

Q50: Do you believe that the procedure outlined above will work in respect of the many links that will have to be established with respect to TARGET2-Securities?

Reasons which may justify a refusal of access to other market infrastructures and the procedure in case of refusal (Article 53(4) and (5))

Reasons which may justify a refusal by a CSD of access to other market infrastructures

217. Article 53(4) CSDR requires ESMA to specify the risks which may justify a refusal by a CSD to provide access to other market infrastructures (e.g. a CCP) and the related standard forms and templates.
218. ESMA is of the view that the risk analysis should include at least the following areas: legal, financial, and operational risks. Below are examples of reasons that may justify a refusal of access within each risk area:

a. Legal risks

- The requesting party is not able to demonstrate that it has the necessary internal anti-money laundering, anti- terrorism financing and anti-tax evasion measures in place;
- The requesting party is not subject to a regulatory and supervision framework comparable to that of the country of the receiving party;
- The requesting party is not able to guarantee the confidentiality of commercially sensitive information provided through the link.

b. Financial risks

- The requesting party does not have the adequate financial resources to fulfil its obligations towards the receiving party;
- The requesting party is not willing or able to finance any customised component of the link, to the extent that this does not go against the non-discrimination principle enshrined in the CSDR.

c. Operational risks

- The requesting party is not able to demonstrate, that it can adhere to the current risk management rules of the receiving party;
- The requesting party is not able to demonstrate, that it has the technological ability to participate in the system operated by the receiving party;
- The requesting party is not able to demonstrate that it has the operational capacity to satisfy the requirements of the receiving party;
- The requesting party does not have appropriate business continuity plans in place;
- Access requires changes at the receiving party that would impede the risk management procedure or operational functioning of the system operated by the receiving party;
- Access requires the receiving party to implement extensive manual processing, increasing the risk of human error, either due to the increased complexity of the process or due to the costs for implementing automated processing.

219. In case of complaint by the requesting party and in order to allow a proper assessment by the competent authorities, the reasons for refusal should be supported by adequate explanation with a level of detail that allows for understanding the risks related with the provision of services.
220. The reasons should be objective, demonstrable and non-discriminatory.

Q51: Do you agree that the risk analysis performed by the receiving party in order to justify a refusal should include at least legal, financial and operational risks? Do you see any other areas of risk that should be considered? If so, please give examples?

Elements of the procedure where a party refuses to provide access to another party

221. The CSDR states that a party, under certain circumstances, may refuse access to another party. If access is denied, the receiving party should provide the requesting party with full written reasons for its refusal within the stipulated response time of three months.
222. ESMA, in close cooperation with the members of the ESCB, is required to develop draft RTS specifying the elements of the procedure where a party refuses to provide access as described in Article 53(4).
223. To enhance legal certainty and increase the predictability and transparency of the process for the parties involved, ESMA is of the opinion that the technical standard should include fixed time limits for each step of the procedure and therefore proposes the following:

- In case of refusal, the requesting CSD should have the right to complain to the competent authority of the CSD that has refused access within 1 month from the receipt of the refusal.
- The responsible competent authority should duly examine the complaint by assessing the reasons for refusal and should consult the competent authority of the requesting party and the relevant authority of the requesting CSD referred to in point (a) of Article 12(1) on its assessment of the complaint.
- Where any of the competent authorities of the requesting party disagrees with the assessment provided, any one of the authorities may refer the matter to ESMA, who may decide to take actions in accordance with the powers conferred on it under Article 19 of Regulation (EU) No 1095/2010 (the Annex considers both cases, and where ESMA is not referred to, the scenario is considered 'standard' and the process takes less 3 months).
- The competent authority of the receiving party should thereafter provide the requesting party with a reasoned reply within 6 months from the submission of the complaint.
- Where the refusal to grant access is deemed unjustified, the responsible competent authority should issue an order requiring the receiving party to provide access to the requesting party. The receiving party should be required to provide access to the requesting party within 3 months of the order.

Q52: Do you agree that the time frames as outlined in the procedure above are sufficient and justifiable? If not, which time frames would you prefer? Please provide reasons to support your answer.

Procedure for granting and refuse authorisation to provide banking type of ancillary services (Article 55(7) and (8))

224. ESMA is required to specify the information that the CSD shall provide to the competent authority for the purpose of obtaining the relevant authorisations to provide the banking services ancillary to settlement. As a background, Articles 54 and 55 CSDR cover the authorisation of a CSD to provide banking type of ancillary services, to designate a credit institution, and the procedure for granting and refusing such an authorisation.
225. According to Article 54, when it is not practical and available to settle in central bank accounts, a CSD may offer to settle the cash payments for all or part of its securities settlement systems:
    - on its own, under a CSD's separate authorisation for banking services (a limited banking license);
    - through accounts opened with one (or more) credit institution designated for that purpose by the CSD, where the credit institution and a CSD can be part of the same financial group or not.
226. Article 55 lays down the procedure for granting and refusing authorisation to provide banking type of ancillary services directly or through a credit institution. The competent authority of the applicant CSD has 30 working days to assess the completeness of the application, and further 6 months after such an assessment to finalise the procedure by informing the applicant CSD whether the authorisation has been granted or refused, with a fully reasoned decision (following the provisions of Article 17).
227. In particular, the standards ESMA is asked to develop include:
    - how the CSD or the designated credit institution meets or intends to meet the conditions set out in Article 54 and, specifically, the prudential requirements set out under Article 59(1), (3) and (4); and
    - the structural organisation of the relations between the CSD and the designated credit institutions, where applicable.
228. An application of a CSD to settle money transfers through accounts held outside a central bank will be assessed by a relevant competent authority against the set of criteria listed in Article 54.
229. The primary condition to grant authorisation is that the entity which is going to provide cash settlement already avails of a banking license. Therefore, at the moment of application for the Article 54 authorisation, the CSD will need to produce appropriate evidence of the formal decision of the relevant prudential supervision authority, referred to under Article 60, regarding authorisation of the CSD or the separate legal entity as a credit institution.
230. A further condition referred to in Article 54 is that the CSD or the separate banking entity is in possession of an adequate recovery plan to ensure continuity of its critical operations, including in situations where liquidity or credit risk crystallises as a result of the provision of banking ancillary services. Therefore, at the moment of application for the Article 54 authorisation, the CSD will need to produce an adequate recovery plan regarding critical operations of the CSD or the separate banking entity.
231. The remaining conditions listed under Article 54 cannot be met at the moment of application. In these cases, the CSD needs to provide to the competent authority evidence as to how intends to comply with them from the moment of authorisation onwards.
232. As regards the condition that the CSD or the separate banking entity meets the prudential requirements referred to under Article 59, paragraphs 3 and 4, responsibility for checking compliance with them rests with the authority referred to under Article 60. Authorisation of the CSD or the separate legal entity as a credit institution can be taken as adequate evidence of compliance with the corresponding requirements. No further evidence is then needed.
233. For the rest, the CSD needs to prove that:

- the authorisation should be used only to provide the banking type of ancillary services referred to in Section C of the Annex of the CSDR and not to carry out any other banking activities;
- the separate banking entity should not itself carry out any of the core services referred to in Section A of the Annex;
- the CSD or the separate banking entity reports at least monthly to the competent authority and annually in its public Pillar 3 disclosure as required under Directive 2006/48/EC on the extent and management of intra-day liquidity risk in accordance with paragraph 5(f) of Article 54;
- it has an additional capital surcharge that reflects the risks, including credit and liquidity risks, resulting from the provision of intraday credit to, among others, the participants to a securities settlement system or other users of CSD services.

As regards these latter conditions, ESMA believes that inclusion in the application of a programme of operations, as required under Article 55(2), which is consistent with such conditions, can be considered sufficient to prove compliance with such conditions at the moment of authorisation.

Q53: Do you agree with these views? If not, please explain and provide an alternative.

234. Finally, Article 55(2) puts emphasis on "*the structural organisation of the relations between the CSD and the designated credit institutions where applicable*". This provision applies when (at least) one separate banking entity is designated to provide banking type of ancillary services, regardless of whether such an entity belongs to the same group as the CSD. In these cases, the competent authority will need to analyse the possible risks stemming from the relations between the CSD and the designated credit institutions.
235. ESMA believes that the following information is of importance to analyse these interconnection risks and it is envisaged that they should be required as part of the application process:
    - Service level agreement (outsourcing);
    - IT platform used for the settlement of the cash leg including analysis of IT organisation and risk;
    - Investment policy of the credit institution;
    - Mechanics and legal foundations of the DVP process;
    - Other relevant arrangements with third parties, such as (but not limited to) links.

Q54: What particular types of evidence are most adequate for the purpose of demonstrating that there are no adverse interconnections and risks stemming from combining together the two activities of securities settlement and cash leg settlement in one entity, or from the designation of a banking entity to conduct cash leg settlement?

Annex I: Possible minimum requirements for an application for registration as CSD

A	General Information on the Applicant / CSD
A1	***CSD identification***
1	Identification and legal status CSD's (articles of incorporation, and/or other statutory documentation)
2	Reference to the securities settlement system(s) operated by the CSD
3	Copy of the Management Body decision regarding the application and the minutes from the meeting in which the Management Body approved the application file and its submission
4	Contact person's details
5	Information on ownership (ownership chart)
6	Identification of any subsidiaries and, where relevant, the group structure
7	List of services that the CSD intends to provide under CSDR: the core services in Section A of the Annex to CSDR and ancillary services explicitly listed under section B of the Annex to CSDR
8	Indication of any other services permitted under, but not explicitly listed in Section B of the Annex to CSDR, that the CSD is providing/intends to provide
9	Indication of any other Member State(s) in which the CSD intends to operate; currency or currencies it processes/intends to process; a programme of operations stating in particular the services which it provides/intends to provide, in case of a branch; the organisational structure of the branch and the names of those responsible for the management of the branch; a comprehensive assessment of how it intends to ensure compliance with corporate or other similar laws whenever relevant
10	Details regarding any outsourcing of a core service to a third party under Article 30 of CSDR
11	Information regarding compliance with the relevant MiFID requirements, where applicable
12	CSD participation in other legal persons
13	Pending judicial, administrative, arbitration or any other litigation proceedings, irrespective of their type, which the CSD may be a party to
A2	***Policies and Procedures***
1	Person responsible for the approval and maintenance of the policies and procedures
2	Description of how compliance with the policies and procedures will be ensured and monitored, and the person responsible for compliance in that regard
3	Description of the measures to adopt in the event of a breach of policies and procedures
4	Procedure for reporting to CA any material breach of policies or procedures which may result in a breach of the conditions for initial authorisation
A3	**Information for groups**
1	Policies and procedures specifying how the organisational requirements apply to the group and to the different entities of the group, in the context of the interaction with the CSD
2	Composition of the senior management, management body and shareholders of the parent undertaking or group of undertakings where relevant
3	Chart showing the ownership links between the parent undertaking, subsidiaries and any other associated entities or branches; the undertakings shown in the chart should be identified by their full name, legal status, legal address, and tax numbers or company registration numbers
4	Where the CSD has a parent undertaking, it should: i) identify the legal address; ii) indicate whether the parent undertaking is authorised or registered and subject to supervision, and when this is the case, state any relevant reference number and the name of the competent authority or authorities
5	Where the CSD offers, or plans to offer ancillary services permitted under section B of the Annex to CSDR, the application for authorisation as CSD should contain a description of the respective ancillary services
6	Where the CSD offers, or plans to offer, through an undertaking within its group, or through an undertaking with which the CSD has a material agreement, ancillary services permitted under sec-

	tion B of the Annex to CSDR, the application for authorisation as CSD should contain a description of the respective ancillary services
7	Where the CSD has a material agreement with an undertaking relating to the offering of trading or post-trading services, the application should contain a description and a copy of such agreement
B	**Financial reports and business plans**
	Financial reports for the 3 preceding years and business plans of the CSD:
1	complete set of financial statements, prepared in accordance with Regulation (EC) No 1606/2002
2	financial reports including the statutory audit report on the annual and consolidated financial statements[20]
3	Name and the national registration number of the external auditor
4	Financial business plan contemplating different business scenarios for the CSD services, over a minimum three years reference period
	Where historical financial information referred to above is not available, an application for authorisation as CSD should contain the following information about the CSD:
5	the pro-forma statement demonstrating proper resources and expected business status in six months after authorisation is granted
6	an interim financial report where the financial statements are not yet available for the requested period of time
7	a statement of financial position, such as a balance sheet, income statement, changes in equity and of cash flows and notes comprising a summary of accounting policies and other explanatory notes
8	audited annual financial statements of any parent undertaking for the three financial years preceding the date of the application
9	an indication of future plans for the establishment of subsidiaries and their location
10	a description of the business activities which the CSD plans to carry out, specifying the activities of any subsidiaries or branches
C	***Organisational requirements***
C1	**Corporate governance**
1	CSD's lines of responsibility, internal corporate governance policies and the procedures and terms of reference which govern its senior management, including the members of the management body, its non-executive members, and committees
2	Processes to identify, manage, monitor and report the risks to which the CSD is or might be exposed
3	The information should include a description of the selection process, appointment, performance evaluation and removal of senior management and members of the management body
4	Where the CSD adheres to a recognised corporate governance code of conduct, the application should identify the code, include a copy and provide an explanation for any situations where the CSD deviates from the code
	Organisational chart detailing the organisational structure of the CSD, including:
5	dedicated staff members and identification of and those members of the staff
6	persons who direct the activities of any branches
7	information about the identity of the person responsible for each significant role
8	a general list of senior management, members of the management body including their role and qualifications per role
9	a specific description of the staff resources dedicated to information technology

[20] *(Link to Proposal for amending Directive 2006/43/EC of the European Parliament and of the Council of 17 May 2006 on statutory audits of annual accounts and consolidated accounts)*

	Staffing policies and procedures
1	Copy of the remuneration policy for the senior management, the members of the management body, and the staff employed in risk and control functions of the CSD
2	Measures put in place by the CSD to mitigate the risk of over-reliance on any individual persons
C2	**Internal control mechanisms**
	Overview of the internal controls of the CSD including:
1	the CSD's internal control policies and procedures
2	the monitoring and evaluation of the adequacy and effectiveness of the CSD's systems
3	the control and safeguard for the CSD's information processing systems
4	the internal bodies in charge of the evaluation of the findings
	Information with respect to the CSD's internal audit function including:
5	an explanation of how its internal audit methodology is developed and applied taking into account the nature of the CSD's activities, complexities and risks
6	a work plan for three years following the date of application
7	a description of the roles and qualifications of each individual(s) who is responsible for internal audit
	Information with respect to the CSD's compliance function including:
8	a description of the roles of the persons responsible for compliance and of any other staff involved in the compliance assessments, including how the independence of the compliance function from the rest of the business will be ensured
9	the internal policies and procedures designed to ensure that the CSD, including its managers and employees, comply with all the provisions of CSDR, including a description of the role of the management body and senior management
10	where available, the most recent internal report prepared by the persons responsible for compliance or any other staff involved in compliance assessments within the CSD
11	information with respect to the procedures for the CSD employees to report potential violations internally through a specific channel
C3	**Management of conflicts of interest**
	Policies and procedures to manage conflicts of interest put in place by the CSD:
1	with respect to the identification, management and disclosure of conflicts of interest between the CSD, including its managers, employees, members of the management body or any person directly or indirectly linked to them, and its participants or their clients, and a description of the process used to ensure that the relevant persons are aware of the policies and procedures
2	any other measures and controls put in place to ensure the requirements referred to in the previous point on conflicts of interest management are met
3	resolution procedures whenever possible conflicts of interest occur
4	the arrangements the CSD makes to structure itself and to allocate responsibility for decisions so that it can continue to take proper regulatory decisions notwithstanding any conflicts, including: the size and composition of the governing body and relevant committees, the roles and responsibilities of key individuals, especially where they also have responsibilities in other organisations, the arrangements for transferring decisions or responsibilities to alternates, and the arrangements made to ensure that individuals who may have a permanent conflict of interest in certain circumstances are excluded from the process of taking decisions (or receiving information) about matters in which that conflict of interest would be relevant
5	an up-to-date inventory, at the time of the application, of existing material conflicts of interest in relation to any ancillary or other related services provided by the CSD and a description of how these are being managed
6	where the CSD is part of a group, the inventory should include any material conflicts of interest

	arising from other undertakings within the group and how these conflicts are being managed
C4	**Confidentiality**
	Internal policies and mechanisms preventing any use, for commercial purposes, of:
1	confidential information
2	information related to participant, clients or issuers
3	any information that the CSD in the performance of its duties may have stored
4	information not permitted for commercial use, for illegitimate purposes or for unauthorised disclosure
5	Internal procedures on the staff permissions for using passwords to access the data, specifying the staff purpose, the scope of data being viewed and any restrictions on the use of data
6	Processes to keep a log identifying each staff member accessing the data, the time of access, the nature of data accessed and the purpose
C5	**Senior management, management body and shareholders**
1	Ownership of the CSD, and in particular, the identity and scale of interests of any parties in a position to exercise control over the operation of the CSD
2	List of the shareholders and persons who are in a position to exercise, directly or indirectly, control over the management of the CSD
	Information in respect of each member of the senior management and each member of the management body including:
3	a copy of the curriculum vitae in order to enable the assessment on the adequate experience and knowledge to adequately perform their responsibilities
4	details regarding any criminal convictions in connection with the provision of financial or data services or in relation to acts of fraud or embezzlement, notably via an official certificate if available within the relevant Member State
5	a self-declaration of good repute in relation to the provision of a financial or data service
6	a declaration of any potential conflicts of interests that the senior management and the members of the management body may have in performing their duties and how these conflicts are managed
7	if applicable, a declaration regarding the independent status of the senior management and the members of the management body
8	description of the roles and responsibilities of the CSD management body
C6	**User committee**
1	Information regarding the user committee for each securities settlement system operated by the CSD, which should be composed by representatives of issuers and by participants to such securities settlement systems, and which should report directly to the management body
2	Mandate for each established user committee, the governance arrangements necessary to ensure its independence and its operational procedures, as well as the admission criteria and the election mechanism for user committee members
C7	**Record keeping**
	Description of the CSD recordkeeping systems, policies and procedures enabling it to comply with the requirements of the Regulation
D	***Conduct of business rules***
D1	**Goals and objectives**
	CSD goals and objectives, such as in the areas of minimum service levels, risk-management expectations and business priorities
D2	**Handling of complaints**
	Procedures for the handling of complaints
D3	**Participation requirements**
1	Criteria for participation which allow fair and open access for all legal persons that intend to become

	a participant of the securities settlement system operated by the CSD
2	Procedure for treating requests for access promptly
3	Procedures for the suspension and orderly exit of participants that no longer meet the criteria for participation
D4	**Pricing policy transparency**
1	Pricing policy, including any existing discounts and rebates and conditions to benefit from such reductions (for core services set out in Annex A to CSDR) for each SSS
2	Methods used in order to make the information available for clients and prospective clients, including a copy of the fee structure where the CSD services should be unbundled
E	***Requirements for CSD services***
E1	**Book-entry form**
	CSD capacity to record securities in book-entry form
E2	**Intended settlement dates and preventing fails**
1	Rules and procedures that facilitate the settlements of transactions in financial instruments on the intended settlement date
2	Details of mechanisms promoting early settlement on the intended settlement date
3	Details of the tools for the management of the timely settlement of transactions (Link to the specific RTS)
E3	**Measures to address settlement fails**
	Details of the system monitoring settlement fails and the reports, cash penalties and measures to address fails
E4	**Integrity of the issue**
	Rules and procedures to help ensure the integrity of securities issues, reconciliation measures including adequate cooperation and information exchange measures (if applicable) and prohibition of securities overdrafts, debit balances or securities creation in each of the securities settlement system operated by a CSD
E5	**Protection of participants' securities**
1	Rules and procedures to help reduce and manage the risks associated with the safekeeping of securities
2	Details of the different levels of segregation offered by the CSD, including a description of the main legal implications of the respective levels of segregation offered, and information on the insolvency law applicable in the relevant jurisdictions
3	Rules that the CSD should not use the securities of a participant, or of a participant's client, for any purpose, unless it has obtained that participant's or its client's prior express consent
E6	**Settlement finality**
1	Rules defining the moments of entry and of irrevocability of transfer orders in the securities settlement system operated by the CSD in accordance with Articles 3 and 5 of Directive 98/26/EC and the point in time at which transfers of funds and securities in a securities settlement system are irrevocable, legally enforceable and binding on third parties
2	Rules ensuring that all securities transactions against cash between direct participants settled in the securities settlement systems operated by the CSD should be settled on a DVP basis
E7	**Participant default rules and procedures**
	Effective and clearly defined rules and procedures to manage the default of a participant ensuring that the CSD can take timely action to contain losses and liquidity pressures and continue to meet its obligations
E8	**Portability**
	Procedure ensuring the timely and orderly settlement and transfer of the assets of clients and participants to another CSD in the event of a withdrawal of authorisation

F	***Prudential requirements***
F1	**Legal risks**
	Information enabling the CA to assess that CSD rules, procedures, and contracts are clear and understandable for all the securities settlement systems it operates and all other services it provides
F2	**General business risks**
	Description of CSD management and control systems and IT tools to identify, monitor and review general business risks, including business strategy, cash flows, and operating expenses
F3	**Operational risks**
1	Description of IT tools that ensure a high degree of security and operational reliability
2	Business continuity policy and disaster recovery plan to ensure the preservation of its services, the timely recovery of operations and the fulfilment of the CSD's obligations in the case of events that pose a significant risk of disrupting operations
3	Description of systems and user facilities developed by the CSD in order to provide services to the clients, including a copy of any user manual and internal procedures
4	Investment and renewal policies on information technology resources of the CSD
5	Outsourcing arrangements entered into by the CSD, together with the methods employed to monitor the service level of the outsourced functions and a copy of the contracts governing such arrangements
F4	**Investment policy**
1	Confirmation that the CSD holding its financial assets at central banks, authorised credit institutions or authorised CSDs, allowing prompt access when required
2	Confirmation that the limitation of investments to financial resources only in cash or in highly liquid financial instruments with minimal market and credit risk
F5	**Capital requirements**
1	Information demonstrating that capital, together with retained earnings and reserves of a CSD, is proportional to the risks stemming from the activities of the CSD
	Plan (approved by the management body or an appropriate committee of the management body of the CSD) for:
2	the raising of additional capital should its equity capital approach or fall below the requirements
3	the achieving of an orderly wind down or reorganisation of its operations and services in case the CSD is unable to raise new capital
G	***Links***
1	Detailed description of the existing links
2	Procedures regarding the identification, assessment, monitoring and management of all potential sources of risk for the CSD and for its participants arising from a link arrangement and the appropriate measures to mitigate them
3	Procedures regarding the measuring, monitoring and management of the additional risks arising from the use of an intermediary to operate a CSD to CSD link, and the appropriate measures to mitigate those risks
4	Robust reconciliation procedures to ensure that the linked CSD records are accurate
5	Applicable law to proprietary aspects
6	Confirmation that the moments of entry of transfer orders into the system and irrevocability of transfer orders were established identically, and the use of equivalent rules concerning the moment of finality of transfers of securities and cash, in the case of interoperable securities settlement systems and CSDs that use a common settlement infrastructure
H	***Access***
	Procedures for dealing with requests for access:
1	of issuers to the CSD

2	between CSDs
3	between the CSD and another market infrastructure

Annex II: Template for CSD Registration application

FORMAT OF APPLICATION

GENERAL INFORMATION

Date of application	…
Corporate name of CSD	…
Legal address	…
The services under CSDR Annex for which the CSD is applying to be registered	…
Name of the person assuming the responsibility of the application	…
Contact details of the person assuming the responsibility of the application	…
Name of other person responsible for the CSD compliance	…
Contact details of the person(s) responsible for the CSD compliance	…
Identification of any parent company	…

DOCUMENT REFERENCES

(Article 17(9) CSDR)

Reference to the list of information to be submitted in accordance with Article [X] of the delegated regulation with regard to regulatory technical standards specifying the details of the application for registration of CSDs adopted pursuant to Article 17(8) of Regulation (EU) No XXX/2013	Unique reference number of the document	Title of the document	Chapter or section or page of the document where the information is provided or reason why the information is not provided
…			
…			
…			

Annex III: Recordkeeping requirements

CS	In relation to core services
SR	**Stock records**
1	Issuers
2	Country of establishment of Issuers
3	Persons exercising control on Issuers
4	Country of establishment of persons exercising control on issuers
5	Issuers' 'securities' accounts
6	Settlement banks used by Issuers
7	Cash accounts used by Issuers
8	Securities initially recorded in the CSD
9	Securities maintained by the CSD
10	Characteristics of the securities initially recorded in or maintained by the CSD
11	Participants
12	Country of establishment of Participants
13	Persons exercising control on Participants
14	Country of establishment of persons exercising control on Participants
15	Participants' securities accounts
16	Settlement banks used by Participants
17	Cash accounts used by Participants
18	Issuers' 'securities' accounts - end of day balances
19	Participants securities accounts - end of day balances
20	Participants cash accounts - end of day balances
FR	**Flow records**
1	Delivering participant
2	Delivering participant settlement instruction (delivering instruction)
3	Client of the delivering participant, where applicable
4	Delivering participant securities account
5	Delivering participant's settlement bank
6	Delivering participant cash account
7	Receiving participant
8	Receiving participant settlement instruction (receiving instruction)
9	Client of the receiving participant, where applicable
10	Receiving participant securities account
11	Receiving participant's settlement bank
12	Receiving participant cash account
13	Moment of entry timestamp of the delivering instruction
14	Moment of entry timestamp of the receiving instruction
15	Moment of irrevocability timestamp of the delivering instruction
16	Moment of irrevocability timestamp of the receiving instruction
17	End of validity date of the delivering instruction, where applicable
18	End of validity date of the receiving instruction, where applicable
19	Matching timestamp, where applicable
20	Trade date

21	Intended settlement date
22	Securities object of the settlement instructions
23	Currency
24	Settlement amount
25	Quantity/nominal amount
26	Settlement: Yes/No
27	Settlement timestamp
28	Settlement agent of the cash leg
29	System generated delivering instructions (in case of partial delivery, shaping)
30	System generated receiving instructions (in case of partial delivery, shaping)
31	Buy-in: Yes/No
BRO	**Business/other records**
1	Issuers' and Participants' details, including authorised signatures
2	Settlement agents for the cash legs
3	Types of services offered
4	Categories of Issuers accepted
5	Categories of securities initially recorded or maintained
6	Categories of Participants accepted
7	Types of securities' accounts offered
8	Volumes and values of settlement fails
9	Penalties
10	Major incidents in relation to core services (including summaries of incidents and of remedial actions)
GP	**In relation to governance and policy records**
1	Organisational charts for the management body and relevant committees, operational units, risk management unit and all other relevant units or divisions
2	Identities of the shareholders or members, whether direct or indirect, natural or legal persons, that have qualifying holdings and the amounts of those holdings
3	CSD participations in other legal entities
4	Documents attesting the policies, procedures and processes required under the relevant organisational requirements
5	Minutes of management body meetings and, if applicable, of meetings of sub-committees of the management body and of senior management committees
6	Minutes of meetings of the user committee
7	Minutes of consultation groups with participants and clients, if any
8	Internal and external audit, risk management, compliance reports, and reports by consultant companies, including management responses
9	Major outsourcing contracts
10	Business continuity policy and disaster recovery plan
11	Complaints received, with information on the complainant's name, address, and account number; the date the complaint was received; the name of all persons identified in the complaint; a description of the nature of the complaint; the disposition of the complaint, and the date the complaint was resolved
12	Records of the results of the back and stress tests performed for the CSDs providing banking type of ancillary services
13	Written communications with competent authorities, ESMA and relevant authorities
14	Legal opinions received in accordance with provisions on organisational requirements

15	Where applicable, legal documentation regarding link arrangements
16	The most complete documents describing the development of new business initiatives
17	Tariffs and fines that the CSD has in place
AS	**Ancillary services**
1	allocation and management of ISIN codes and similar codes (e.g. issuer/requesting party identification, securities type, securities characteristics, notional amount)
2	asset servicing (e.g. ISIN, type of corporate action, amount of securities/cash, relevant dates for the processing of the corporate action, outcome of the corporate action, information flows, General Meetings related operational processes, tax reclaims, portfolio valuation)
3	cash accounts provided by the CSD (e.g. LEI of participant/investor using the cash accounts, credit limits, currency, deposits amounts)
4	collateral management services provided by the CSD (e.g. as agent for its participants) (e.g. ISIN, amount of securities, identification of delivering/receiving parties, collateral use, collateral valuation)
5	data and statistics services to market/census bureaus (e.g. entities served; data provided; purpose)
6	general collateral management services as agent (e.g. entities served; purpose; value details)
7	banking type of ancillary services provided by the CSD including (e.g. incidents in relation to that such service and remediating actions including follow-up, details such as cash account, type of operation, purpose of operation, beneficiary)
8	IT services provided (e.g. details on nature of services and how different from the core IT services)
9	operations in relation to cash accounts (e.g. type; purpose;)
10	order routing and processing, fee collection and processing and related reporting (e.g. types of orders, types of fees, purposes of fee collection/processing, involved parties)
11	regulatory reporting services (e.g. under which regulation; nature of service)
12	securities lending operations performed by the CSD as principal or as agent for its participants (e.g. ISIN, amount of securities, identification of delivering/receiving parties, purpose of the securities lending operation, characteristics of collateral, collateral valuation)
13	services related to shareholders' registers (e.g. ISIN, relevant entities involved in the process, information flows)
14	settlement matching, order routing, trade confirmation, trade verification operations
15	the links established by the CSD

Annex IV: Summary of questions

Q1: **Which elements would you propose ESMA to take into account / to form the technical standards on confirmation and allocation between investment firms and their professional clients?**

Q2: **In your opinion, are there any exceptions that should be allowed to the rule that no manual intervention occurs in the processing of settlement instructions? If so please highlight them together with an indication of the cost involved if these exceptions are not considered? Do you consider that this requirement should apply differently to investment firms? If so, please explain.**

Q3: **ESMA welcomes concrete proposals on how the relevant communication procedures and standards could be further defined to ensure STP.**

Q4: **Do you share ESMA's view that matching should be compulsory and fields standardised as proposed? If not, please justify your answer and indicate any envisaged exception to this rule. Are there any additional fields that you would suggest ESMA to consider? How should clients' codes be considered?**

Q5: **Do you agree with the above proposals? What kind of disincentives (other than monetary incentives such as discounts on matching fees) might be envisaged and under which product scope?**

Q6: **In your opinion, should CSDs be obliged to offer at least 3 daily settlements/batches per day? Of which duration? Please elaborate providing relevant data to estimate the cost and benefit associated with the different options.**

Q7: **In your view, should any of the above measures to facilitate settlement on ISD be mandatory? Please describe any other measure that would be appropriate to be mandated.**

Q8: **Do you agree with this view? If not please elaborate on how such arrangements could be designed and include the relevant data to estimate the costs and benefits associated with such arrangements. Comments are also welcome on whether ESMA should provide for a framework on lending facilities where offered by CSDs.**

Q9: **Do you agree with the above monitoring system description? What further elements would you suggest? Please present the appropriate details, notably having in mind the current CSD datasets and possible impact on reporting costs.**

Q10: **What are your views on the information that participants should receive to monitor fails?**

Q11: **Do you believe the public information should be left to each CSD or local authority to define or disclosed in a standard European format provided by ESMA? How could that format look like?**

Q12: **What would the cost implication for CSDs to report fails to their competent authorities on a daily basis be?**

Q13: **CSDR provides that the extension period shall be based on asset type and liquidity. How would you propose those to be considered? Notably, what asset types should be taken into consideration?**

Q14: **Do you see the need to specify other minimum requirements for the buy-in mechanism? With regard to the length of the buy-in mechanism, do you have specific suggestions as to the different timelines and in particular would you find a buy-in execution period of 4 business days acceptable for liquid products?**

Q15: **Under what circumstances can a buy-in be considered not possible? Would you consider beneficial if the technical standard envisaged a coordination of multiple buy-ins on the same financial instruments? How should this take place?**

Q16: **In which circumstances would you deem a buy-in to be ineffective?**

How do you think different types of operations and timeframes should be treated?

Q17: **Do you agree on the proposed approach? How would you identify the reference price?**

Q18: **Would you agree with ESMA's approach? Would you indicate further or different conditions to be considered for the suspension of the failing participant?**

Q19: **Please, indicate your views on the proposed quantitative thresholds (percentages / months).**

Q20: **What is in your view the settlement information that CSDs need to provide to CCPs and trading venues for the execution of buy-ins? Do you agree with the approach outlined above? If not, please explain what alternative solutions might be used to achieve the same results.**

Q21: **Would you agree that the above mentioned requirements are appropriate?**

Q22: **Would you agree that the elements above and included in Annex I are appropriate? If not, please indicate the reasons or provide ESMA with further elements which you find could be included in the draft RTS, and any further details to justify their inclusion.**

Q23: **Do you agree that the above mentioned approach is appropriate? If not, please indicate the reasons or provide ESMA with further elements which could be included in the draft ITS.**

Q24: **Do you see other risks and corresponding mitigating measures? Do CSDs presently have participations in legal persons other than CCPs, TRs and trading venues that should be considered? Would banning CSDs from directly participating in CCPs be advisable, in your view?**

Q26: **Do you agree with this approach? Please elaborate on any alternative approach illustrating the cost and benefits of it.**

Q27: **Do the responsibilities and reporting lines of the different key personnel and the audit methods described above appropriately reflect sound and prudent management of the CSD? Do you think there should be further potential conflicts of interest specified? In which circumstances, if any, taking into account potential conflicts of interest between the members of the user committee and the CSD, it would be appropriate not to share the audit report or its findings with the user committee?**

Q28: **Do you agree with this minimum requirements approach? In case of disagreement, what kind of categories or what precise records listed in Annex III would you delete/add?**

Q29: **What are your views on modality for maintaining and making available such records? How does it impact the current costs of record keeping, in particular with reference to the use of the LEI?**

Q30: **Do you agree that the CSD risk analysis performed in order to justify a refusal should include at least the assessment of legal, financial and operational risks? Do you see any other areas of risk that should be required? If so, please provide examples.**

Q31: **Do you agree that the fixed time frames as outlined above are sufficient and justified? If not, which time frames would you prefer? Please provide reasons to support your answer.**

Q32: **In your opinion, do the benefits of an extra reconciliation measure consisting in comparing the previous end of day balance with all settlements made during the day and the current end-of-day balance, outweigh the costs? Have you measured such costs? If so, please describe.**

Q33: **Do you identify other reconciliation measures that a CSD should take to ensure the integrity of an issue (including as regards corporate actions) and that should be considered? If so, please specify which and add cost/benefit considerations.**

Q34: **Do you agree with the approach outlined in these two sections? In your opinion, does the use of the double-entry accounting principle give a sufficiently robust basis for avoiding securities overdrafts, debit balances and securities creation, or should the standard also specify other measures?**

Q35: **Is the above definition sufficient or should the standard contain a further specification of operational risk?**

Q36: **The above proposed risk management framework for operational risk considers the existing CSDs tools and the latest regulatory views. What additional requirements or details do you propose a risk management system for operational risk to include and why? As always do include cost considerations.**

Q37: **In your opinion, does the above proposal give a sufficiently robust basis for risk identification and risk mitigation, or should the standard also specify other measures? Which and with what associated costs?**

Q38: **What are your views on the possible requirements for IT systems described above and the potential costs involved for implementing such requirements?**

Q39: **What elements should be taken into account when considering the adequacy of resources, capabilities, functionalities and staffing arrangements of the secondary processing site and a geographic risk profile distinct from that of the primary site?**

Q40: **In your opinion, will these requirements for CSDs be a good basis for identifying, monitoring and managing the risks that key participants, utility providers and other FMIs pose to the operations of the CSDs? Would you consider other requirements? Which and why?**

Q41: **Do you agree with the approach outlined above? In particular, do you agree with the approach of not distinguishing between CSDs that do not provide banking services and CSDs that do so?**

Q42: **Should ESMA consider other elements to define highly liquid financial instruments, 'prompt access' and concentration limits? If so, which, and why?**

Q43: **Do you agree that links should be conditioned on the elements mentioned above? Would there be any additional risks that you find should be considered, or a different consideration of the different link types and risks? Please elaborate and present cost and benefit elements supporting your position.**

Q44: **Do you find the procedures mentioned above adequate to monitor and manage the additional risk arising from the use of intermediaries?**

Q45: **Do you agree with the elements of the reconciliation method mentioned above? What would the costs be in the particular case of interoperable CSDs?**

Q46: **Do you agree that DvP settlement through CSD links is practical and feasible in each of the cases mentioned above? If not explain why and what cases you would envisage.**

Q47: **Do you agree that the risk analysis performed by the CSD in order to justify a refusal to offer its services to an issuer should at least include legal, financial and operational risks? Do you see any other areas of risk that should be considered? If so, please give examples.**

Q48: **Do you agree that the time frames as outlined in the procedure above are sufficient and justifiable? If not, which time frames would you prefer? Please provide reasons to support your answer.**

Q49: Do you agree that the time frames as outlined in the procedure above are sufficient and justifiable? If not, which time frames would you prefer? Please provide reasons to support your answer.

Q50: Do you believe that the procedure outlined above will work in respect of the many links that will have to be established with respect to TARGET2-Securities?

Q51: Do you agree that the risk analysis performed by the receiving party in order to justify a refusal should include at least legal, financial and operational risks? Do you see any other areas of risk that should be considered? If so, please give examples?

Q52: Do you agree that the time frames as outlined in the procedure above are sufficient and justifiable? If not, which time frames would you prefer? Please provide reasons to support your answer.

Q53: Do you agree with these views? If not, please explain and provide an alternative.

Q54: What particular types of evidence are most adequate for the purpose of demonstrating that there are no adverse interconnections and risks stemming from combining together the two activities of securities settlement and cash leg settlement in one entity, or from the designation of a banking entity to conduct cash leg settlement?

Annex V:Legislative mandate to develop draft technical standards

Topic	CSDR	Type of TS
Settlement Discipline		
Measures to prevent settlement fails	6(4)	ESMA RTS
Measures to address settlement fails	*7*	
Processes for collection and redistribution of the cash penalties and any other possible proceeds from such penalties	7(14b)	ESMA RTS
Details of system monitoring settlement fails and the reports on settlement fails	7(14a)	ESMA RTS
Buy-in	7(14c-h)	ESMA RTS
Content and scope of reporting to CAs of internalised settlement	9(2)	ESMA RTS
Format and timing of reporting to CAs of internalised settlement	9(3)	ESMA ITS
Conditions under which the Union currencies referred to in Article 12(1)(b) are considered to be as the most relevant and the arrangements for consultation of the relevant CAs	12(3)	ESMA RTS
Registration and Supervision of CSDs		
Information to the CA for authorisation	17(8)	ESMA RTS
Information to the CA for authorisation [standard forms, templates and procedures]	17(9)	ESMA ITS
Conditions for participations of CSDs in entities which not provide services listed in Sections A and B of the Annex	18(4)	ESMA RTS
Review and evaluation - Information that CSDs provides to the CAs - Information that CAs provide to the relevant authorities - Information that CAs provide to each other	22(10)	ESMA RTS
Review and evaluation [forms, templates and procedures]	22(11)	ESMA ITS
Cooperation Arrangements between CAs [standard forms, templates and procedures]	24(7)	ESMA ITS
Information from third country CSDs to ESMA for recognition	25(12)	ESMA RTS
Requirements for CSDs		
Monitoring tools for the risks of CSDs, responsibilities of key personnel, potential conflicts of interest and audit methods	26(8)	ESMA RTS
Recordkeeping	29(3)	ESMA RTS
Recordkeeping [formats]	29(4)	ESMA ITS
Risks which may justify a refusal of access to participants and procedure in case of refusal	33(5)	ESMA RTS

Procedure in case of refusal of access[standard forms and templates]	33(6)	ESMA ITS
Integrity of the issue	37(4)	ESMA RTS
Operational risks	45(7)	ESMA RTS
Investment policy	46(6)	ESMA RTS
CSD links	48(10)	ESMA RTS
Reasons which may justify a refusal of access to issuers and the procedure in case of refusal	49(5)	ESMA RTS
Procedure in case of refusal of access [standard forms and templates]	49(6)	ESMA ITS
CSD links: procedure in case of refusal of access	52(3)	ESMA RTS
CSD links: procedure in case of refusal of access [standard forms and templates]	52(4)	ESMA ITS
Reasons which may justify a refusal of access to other market infrastructures and the procedure in case of refusal	53(4)	ESMA RTS
Procedure in case of refusal of access [standard forms and templates]	53(5)	ESMA ITS
Procedure for granting and refuse authorisation to provide banking type of ancillary services	55(7)	ESMA RTS
Procedure for granting and refuse authorisation to banking type of ancillary services [standard forms, templates and procedures]	55(8)	ESMA ITS