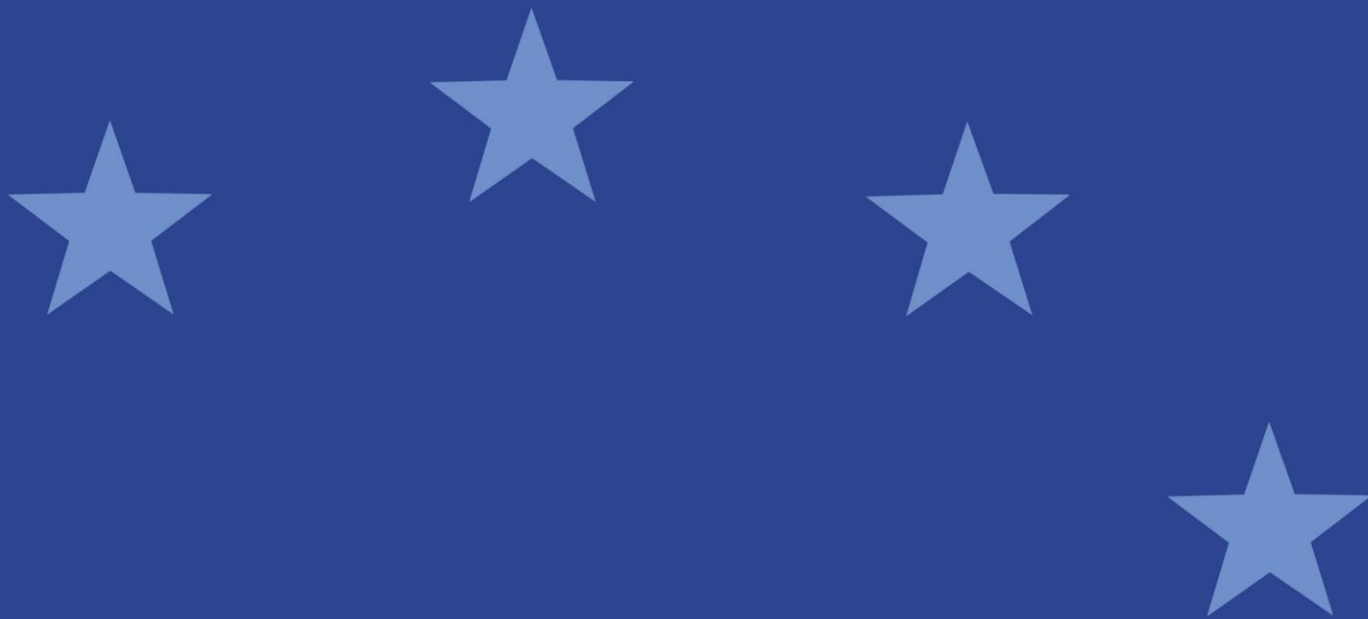


# Impact Assessment

**Annex III to the Final Report on draft Technical Standards under the Regulation No 909/2014 of the European Parliament and of the Council of 23 July 2014 on improving securities settlement in the European Union and on central securities depositories and amending Directives 98/26/EC and 2014/65/EU and Regulation (EU) No 236/2012 (CSDR)**



## Table of Contents

<b>1</b>	<b>EXECUTIVE SUMMARY / INTRODUCTION</b>	<b>3</b>
<b>2</b>	<b>CSD REQUIREMENTS - DRAFT RTS AND ITS</b>	<b>5</b>
2.1	Relevant Currencies (Article 12 CSDR)	5
2.2	CSD Authorisation (Article 17 CSDR)	8
2.3	CSD Participations (Article 18 CSDR)	9
2.4	CSD Review and Evaluation (Article 22 CSDR)	14
2.5	Cooperation Arrangements (Article 24 CSDR)	16
2.6	CSD Recognition (Article 25 CSDR)	18
2.7	Risk Monitoring Tools (Article 26 CSDR)	19
2.8	Record Keeping (Article 29)	24
2.9	Reconciliation Measures (Article 37 CSDR)	37
2.10	Operational Risk (Article 45 CSDR)	42
2.11	CSD Investment Policy (Article 46 CSDR)	48
2.12	CSD Links (Article 48 CSDR)	55
2.13	Access (Articles 33, 49, 52 and 53 CSDR)	68
2.14	Authorisation to provide banking-type ancillary services (Article 55 CSDR)	79
<b>3</b>	<b>INTERNALISED SETTLEMENT (ARTICLE 9 CSDR) – DRAFT RTS AND ITS</b>	<b>80</b>

## 1 INTRODUCTION

This impact assessment provides the European Commission and other interested parties with an assessment of the potential impacts of the different options that were considered as part of the decision making process for formulating the CSDR draft technical standards. Its purpose is to demonstrate how ESMA has ensured that the intended objectives of the CSDR are achieved in a proportionate and effective manner.

This impact assessment has been drafted to analyse the costs and benefits of the draft regulatory and implementing technical standards (RTS and ITS) that ESMA has to deliver under the Central Securities Depositories Regulation (CSDR) covering areas related to CSD Requirements (RTS and ITS) and Internalised Settlement (RTS and ITS). To conduct these assessments and to draft the technical standards, consultations were carried out in the form of a discussion paper (DP) and a consultation paper (CP) published on the ESMA website. In addition ESMA hired a specialised consultancy company to support this study. This firm gathered information from a number of sources, including publicly available information, direct interviews with market participants and professional associations, and non-public answers to questionnaires addressed to CSDs, CCPs and other market participants.

ESMA also requested the opinion of the Securities and Markets Stakeholder Group, and worked with members of the European System of Central Banks.

The CSDR technical standards also cover areas related to settlement discipline; however, given the need to analyse the responses received following ESMA's specific consultation paper on the buy-in process, which closed on 6 August 2015, as well as the need to continue the discussions with the European Commission on the legal feasibility of the options to be considered regarding the entity responsible for the execution of the buy-in the case of transactions not cleared by a CCP, ESMA is delaying the delivery of the RTS on Settlement Discipline.

With reference to the quantitative information attached to the identified costs and benefits, it should be noted that in the DP and CP, ESMA asked respondents to provide data to support this cost-benefit analysis. Unfortunately, data provided by respondents did not include sufficient quantitative evidence to perform a full cost-benefit analysis of a quantitative nature.

In addition, the responses provided to the consultancy company hired by ESMA only supported to a limited extent the quantitative nature of this study. When conducting the cost-benefit analysis the consultancy firm analysed information provided by 32 CSDs. Of the 32 CSDs, the data provided by 19 of the CSDs were deemed suitable for the purposes of the study and included in the final analysis by the consultancy firm, based upon their locations (operating in the European Economic Area), their status (with or without a banking license), T2S status (whether the CSDs signed the T2S Framework Agreement) and the currency (including a range of CSDs both inside and outside the Eurozone). A representative sample was selected, referring to these characteristics. Reference will be made to these CSDs throughout this report. All but one of the 19 CSDs included in the sample operated within the European Union (EU), and the remaining one was part of the European Economic Area. Some had banking licenses, some had signed the T2S framework agreement and two were ICSDs.

Where possible, the consultancy firm made estimations of potential costs and benefits from a quantitative perspective. This involved identifying one-off costs or annual ongoing costs, converting costs to Euros and then using relevant calculation methodologies.

When a range of costs was provided by a single CSD, the central value of the range of costs was assumed to be closest to the potential quantitative cost of that specific option. If a CSD provided only the maximum cost of an option, then this number was used instead. In order to aggregate these costs for all the CSDs sampled, the average was calculated and used as the estimated cost of a specific option.

Other stakeholders considered in the impact assessment included nine CCPs, six banks, some professional associations and one confirmation and allocation platform.

In addition, ESMA worked with the national competent authorities (NCAs) to try to gather relevant data on specific aspects of the technical standards. Data received from the NCAs was generally qualitative and not directly supported by quantitative data. Where possible, ESMA performed its own quantitative impact assessment, or justified some of its policy choices using elements of a quantitative nature that are available to the public, such as academic research papers, or studies elaborated by well-established international organisations (BIS, etc.) and associations (ICMA, ISDA etc.).

Despite attempts to receive quantitative evidence for the different options, the feedback received from stakeholders was not always useful. There was a lack of quantitative evidence to support the arguments of the different stakeholders and assess the impacts of the various options. This was not caused by a lack of effort, rather by limitations in the data that exists in relation to specific areas of the technical standards. To understand the baseline scenario, it is important to mention that CSDs are not currently subject to any formal harmonised requirements across the EU.

In carrying out a cost-benefit analysis on the draft technical standards, it should be noted that:

- The main policy decisions have already been taken under the primary legislation and the impact of such policy decisions have already been analysed and published by the European Commission;
- ESMA does not have the ability to deviate from its specific mandate set out in the primary legislation;
- ESMA's technical choices should be of a purely technical nature and should not involve matters of a political nature.

## 2 CSD REQUIREMENTS - DRAFT RTS AND ITS

### 2.1 Relevant Currencies (Article 12 CSDR)

The options mentioned below were considered following discussions among competent and relevant authorities and following the arguments provided during ESMA consultations.

To analyse the effectiveness of the proposals and their potential results, ESMA conducted a simulation exercise with the cooperation of competent authorities and central banks. ESMA used 2014 data applied to 2013 total settlement value figures of the ECB's Statistical Data Warehouse (SDW). The information allowed ESMA to make estimations based on EU CSD data. The exercise indicated that a 5% threshold (compared with the total value of DVP settlement by a CSD) would lead to only EUR and GBP being considered as relevant currencies across the EU CSDs, the latter currency only in one ICSD. Therefore ESMA considered this to be an ineffective way of measuring relevance and instead lowered the originally proposed threshold.

The simulation exercise showed that even by lowering the threshold from 5% to 1% (compared with the total value of DVP settlement by a CSD) would have led to a very restrictive involvement of central banks of issue other than domestic central banks. For some currencies, even if 100% settlement in securities denominated in these currencies takes place in one CSD, these currencies would not be considered relevant.

This showed that even very small percentages within a CSD with high settlement volumes could represent a significant amount of settlement activity in a particular currency. Therefore ESMA defined a second threshold that considered the total settlement activity in a given currency within the EU, i.e. the central bank of issue perspective. If a relevant proportion of that settlement activity is conducted by a CSD (more than 10% of the settlement activity), that currency should be considered relevant even if in percentage terms it represents less than 1% of a CSD's overall settlement activity.

#### How should the most relevant currencies in which settlement takes place be decided upon?

<b>Specific Objective</b>	To ensure that the appropriate authorities are involved in the authorisation and supervision of CSDs, notably central banks of issue for the most relevant EEA currencies in which settlement takes place.
Option 1	Leave the decision to the CSD or the competent authority.
Option 2	Consider the 3 currencies with the highest relative shares in the CSD's total value of securities settled, provided that each currency's individual share exceeds 5% of the total value of settlement by the CSD
Option 3	The most relevant currencies shall be identified according to either of the following calculations: <ul style="list-style-type: none"> <li>- the relative share of each Union currency in the total value of the settlement by a CSD of settlement instructions against payment, calculated over a period of one year, provided that each individual share exceeds 1%; or</li> <li>- the relative share of settlement instructions against payment settled by a</li> </ul>

	CSD in a Union currency compared to the total value of settlement instructions against payment settled in that currency across all CSDs in the Union, calculated over a period of one year, provided that each individual share exceeds 10%.
Preferred Option	<b>Option 3</b> provides the most objective approach with a consideration of different scenarios, taking into account that even very small percentages within a CSD with high settlement volumes could represent a significant amount of settlement activity in a particular currency.

***Impact of the proposed policies***

<b>Option 1</b>	<i>See Option 1 in 'Specific Objective' table above</i>
	Description
<i>Benefits</i>	Flexibility in the determination of relevance per jurisdiction.
<i>Costs to regulator:</i>	Competent authorities will need to establish a procedure to assess relevance as this option does not propose a standard approach. This will require individual cost-benefit analysis work at each competent authority to determine an appropriate measure.
<i>Compliance costs:</i>	Need to establish internal measures to determine whether currencies settled are 'relevant', according to the approach taken by the national competent authority for making the determination.
<i>Indirect costs</i>	<ul style="list-style-type: none"> <li>- Lack of harmonisation and therefore risk of inconsistency across the EU which would not create a level playing field across the EU when assessing which currencies are relevant as part of the authorisation or supervision of a CSD.</li> <li>- Unfair treatment of relevant authorities that would face the discretion of the competent authority.</li> </ul>

<b>Option 2</b>	<i>See Option 2 in 'Specific Objective' table above</i>
	Description
<i>Benefits</i>	<ul style="list-style-type: none"> <li>- Consistency with the approach followed under EMIR for CCP colleges (even if under EMIR the percentage was 10%);</li> <li>- Easy calculation;</li> <li>- Objective and unique assessment.</li> </ul>
<i>Costs to regulator:</i>	<p>Establishing the framework to apply the threshold and keep the results updated.</p> <p>Based on ESMA's simulation exercise, assessing the currencies at different CSDs, this option would only qualify EUR and GBP as relevant currencies and the latter only in one ICSD. In particular it is noted that for some currencies (e.g. DKK, NOK, PLN, SEK) a 5% threshold effectively means that even if 100% of settlement in securities denominated in these currencies takes place in the EU's largest (I)CSDs, none of these currencies would be considered 'relevant' under the proposed parameter. Therefore, there is potential for this approach putting investors at risk on occasions where large proportions of certain currencies are settled in a specific CSD, the currency will not be deemed significant and risks may arise that are not supervised by the central bank relevant for that currency.</p> <p>The central banks of issue for the relevant currencies considering the volume of settled transactions in their currency would not receive information necessary for assessing potential risks related to settlement in their currency.</p> <p>The cost for the competent authority would be low under this option, given the limited number of relevant authorities with which to cooperate.</p>
<i>Compliance costs:</i>	<p>Compliance costs would be relatively small, as there would be a simple assessment of currencies settled in CSDs and this would indicate which ones should be considered relevant. There will be some cost associated with the reporting of the required information needed by the competent authorities for doing the calculations.</p>

<b>Option 3</b>	<i>See Option 3 in 'Specific Objective' table above</i>
	Description
<i>Benefits</i>	<ul style="list-style-type: none"> <li>- Consistency within the EU;</li> <li>- Objective assessment;</li> <li>- Inclusive approach for relevant authorities;</li> <li>- Strengthened cooperation;</li> <li>- Consistency with the objectives of the CSDR.</li> </ul>
<i>Costs to regulator:</i>	<p>Higher costs than under previous options to calculate the threshold, given the need to calculate the total settlement activity in a specific currency.</p> <p>Higher costs than the other options for the competent authority that will need to cooperate and share information with more relevant authorities.</p> <p>Lower costs than the other options for the relevant authorities that receive information necessary for assessing potential risks related to settlement in their</p>

	local currency.
Compliance costs:	Compliance costs should be relatively limited for CSDs as competent authorities are carrying out the necessary calculations. There will be some cost associated with the reporting of the required information needed by the competent authorities for doing the annual calculations.

## 2.2 CSD Authorisation (Article 17 CSDR)

**What relevant information should be submitted to competent authorities to enable a thorough and robust assessment of a CSD's application for authorisation?**

<b>Specific Objective</b>	To ensure the relevant documentation is submitted to competent authorities to enable a thorough and robust assessment of a CSD's application for authorisation.
Option 1	To include only the minimum information required for the authorisation of CSDs.
Option 2	To request more detailed information as part of the application for authorisation as a CSD, with the technical standards referring to a comprehensive list of information required by competent authorities.
Preferred Option	<b>Option 2</b> - more detailed relevant information, harmonised at EU level, should ensure a more thorough and robust assessment of a CSD's application, and a higher degree of consistency across the EU.

### **Impact of the proposed technical options**

<b>Option 1</b>	<i>See Option 1 in 'Specific Objective' table above</i>
<i>Benefits</i>	This would allow CSDs to leverage their existing internal procedures and documentation with the submission of information during the application process. This option would be simpler for CSDs allowing them to prepare the documentation that they consider sufficient to achieve compliance with the CSDR requirements.
<i>Costs to regulator:</i>	This option may entail a lower initial cost (one-off); however the costs may increase during the assessment of the application as the competent authority might be required to send a number of additional information requests to the CSD which will require additional resource on the part of the competent authority. The information received in line with this option may not enable a thorough assessment of a CSD's application. The information may contain significant gaps which may delay the registration process. The CSD may be unclear on whether there is a need to elaborate further the information to be submitted. The CSD may be uncertain on how its application is going to be processed by the competent authority. This approach would not ensure a high degree of harmonisation, nor a level playing field amongst different CSDs in the EU.
<i>Compliance costs:</i>	This option may entail fewer costs in the initial delivery of the information to the competent authority (one-off). However, it may increase the costs during the



	assessment of the application as the competent authority might have to send a number of additional information requests to the CSD.
--	---

<b>Option 2</b>	<i>See Option 2 in 'Specific Objective' table above</i>
	Description
<i>Benefits</i>	This option will allow an in-depth assessment of the different provisions of the CSDR and of the relevant technical standards. The cross check of the information submitted as part of an application will improve the quality of the supervision and the safety of CSDs. It will also ensure a more harmonised process, which should foster a level playing field. The overall authorisation would be better organised, so the completion timeframe could be reduced; therefore, the cost of authorisation would overall decrease even if the list of documents specified in the standards is longer and more granular than under Option 1.
<i>Costs to regulator:</i>	Overall, this may mean that more information is required to be submitted to the competent authority. However, this may reduce the cost as it may allow a faster assessment of the applications (one-off).
<i>Compliance costs:</i>	Providing more documentation to the competent authority is likely to incur increased compliance costs (one-off), however it will reduce the likelihood that further information is required at a later stage.

## 2.3 CSD Participations (Article 18 CSDR)

Below is a summary of the existing practices in relation to participations at the CSDs involved in the research.

According to the research conducted by the external consultant, only one CSD out of more than 30 respondents to the external consultant's questionnaire held participations outside of activities mentioned in sections A&B of the Annex to CSDR. Seven of these nine CSDs held participations outside the 'securities chain' i.e. outside CCPs, TRs, trading venues.

Activities of the subsidiaries	Number of CSDs
CSDs	Mentioned by 2 CSDs. Minor interests as part of the requirements for becoming a participant
Dematerialisation of securities	1 Dormant entity formerly used for such purpose. Initial incorporation required by local regulator
Deposit guarantee fund	1
Energy market services	1
Financing and credit insurance for exporters	1
International financial associations (ex: ANNA - Association of National Numbering Agencies, SWIFT)	Mentioned by 2 CSDs (minor interests)
Issuer of securities (issuance of CSD own securities)	1
Management of a parking lot	1

Representative offices abroad	1
Real estate companies to hold equity in headquarters' buildings	2
Services for organization and IT	1 (IT development, project management, consulting)
Trust arrangements to protect clients' assets	2
Other	1 Company used for keeping former CSD name

### Nominee companies

One CSD included in the research participates in a number of companies designated as 'nominee companies'. These are said to serve three holding purposes:

- Client assets
- Amounts to be paid as stamp duty tax
- Own CSD assets

According to information provided by market sources, firms in the jurisdiction of this CSD may safeguard client assets either in the name of the client or through nominee companies (clients can also hold certificates themselves and be the actual custodian of the assets).

These sources suggest that in practice, nominee companies with trust arrangements are frequently used in this jurisdiction for the holding of securities notably for asset protection reasons. As regards asset protection, assets held under nominee structures are excluded from insolvency procedures:

- At the CSD level, as the nominee is the legal owner of the securities
- At the nominee level, as "property held by the bankrupt on trust for any other person" is excluded from the bankrupt's estate, as mentioned in the relevant legislation of the jurisdiction

Nominee companies are not regulated as such, yet they are defined in the appropriate law in this jurisdiction as both safeguarding and administering of assets.

### Participations within the securities chain

Six CSDs out of 32 hold participations within the securities chain (CCPs, TRs, trading venues):

Participant	Direct participation in trading venues	Direct participation in CCPs	Direct participation in trade repositories
CSD 1	Yes	Yes – (from 17% to 50%)	No
CSD 2	Yes (33%)	No	No
CSD 3	No	No	Yes (50%)
CSD 4	No	Yes (99.72%)	No
CSD 5	No	No	Yes (50%)
CSD 6	No	Yes (100%)	Yes (100%)

Only 2 CSDs have participations only within the securities chain. The remaining 4 CSDs also have participations outside the securities chain.

### **Control of the participated entity** (level of the participations)

In terms of control of their participations and interests, there are generally three types of arrangements:

- Full control of the subsidiaries

- Partial control
- Marginal interests in a variety of businesses related to securities processing

### **Income from participations**

Data was collected for 6 CSDs on the proportion of the total income which came from participations:

- CSD 1: below 20% of total income
- CSD 2: 1% of income
- CSD 3: 30% of total income stems from clearing activities
- CSD 4: below 20% of total income
- CSD 5: below 20% of total income
- CSD 6: below 20% of total income

### **Guarantees**

Only 3 CSDs out of more than 30 questionnaire respondents have been identified as guarantors. They are guarantors on activities related to non-CSD activities or banking activities. One of the guarantor CSDs guarantees perpetual bonds issued by a subsidiary that is a fully owned financial vehicle.

### **2.3.1 How can the CSDR technical standards ensure CSD participations are limited to activities that do not significantly increase the risk profile of the CSD?**

<b>Specific Objective</b>	Restrict CSD participations to activities not significantly increasing the risk profile of a CSD
Option 1	The CSD should hold sufficient financial resources that fulfil the criteria referred to in Article 46 of Regulation (EU) No 909/2014 to cover the risks resulting from the following: (i) the guarantees given by the CSD to that legal person; (ii) any contingent obligations undertaken by the CSD in favour of that legal person; (iii) any loss sharing agreements or recovery mechanism of that legal person.
Option 2	Prohibit any CSD guarantee (limited or unlimited guarantees)
Preferred Option	<b>Option 1</b> would give more flexibility to CSDs, while at the same time achieving the objective.

### **Impact of the proposed policies**

Option 1	See Option 1 in 'Specific Objective' table above
	Description
<b>Benefits</b>	This provision will allow CSDs: <ul style="list-style-type: none"> <li>- to avoid increasing the risks they manage, especially by limiting future exposure to guarantees to subsidiaries;</li> <li>- some flexibility through the authorisation of limited liabilities provided they are fully capitalised.</li> </ul> It would: <ul style="list-style-type: none"> <li>- not change the risk profile of the CSD, and</li> <li>- not represent significant costs having in mind the current CSD</li> </ul>

	practices.
<i>Compliance costs:</i>	Compliance functions would need to be more vigilant when considering potential participations to ensure they meet the related requirements and do not create additional risks to CSDs and investors.

Option 2	<i>See Option 2 in 'Specific Objective' table above</i>
	Description
<i>Benefits</i>	This option would effectively avoid increasing the risks that CSDs manage.
<i>Compliance costs:</i>	Possible one-off costs since this would apply to current guarantees as well, that would be terminated and would need to be replaced by other funding arrangements. This could have an impact on the CSD if the guarantees are intra-group or on the market as a whole if the guarantees are granted to relevant entities.
<i>Indirect costs</i>	This option may limit the possibility for CSDs to enter in some businesses.

## LIMIT PARTICIPATIONS TO THE SECURITIES CHAIN

### 2.3.2 Should the CSDR technical standards limit participations to the securities chain so as not to significantly increase the risk profile of the CSD?

<b>Specific Objective</b>	Limit the participations of the CSDs to activities which do not involve an increase in the risk profile of the CSD.
Option 1	The legal person in which the CSD holds a participation should provide services that are complementary to the core services offered by the CSD, as referred to in Article 18(4) of Regulation (EU) No 909/2014, such as: <ul style="list-style-type: none"> <li>- a CCP authorised or recognised under Regulation (EU) No 648/2012 of the European Parliament and of the Council or</li> <li>- a trading venue as defined in point (42) of Article 2(1) of Regulation (EU) No 909/2014.</li> </ul>
Option 2	Limit participations of CSDs to trading venues (but no limitation of participation to CCPs).
Preferred Option	<b>Option 1</b> allows flexibility and consistency with the reality of the securities value chain.

### *Impact of the proposed policies*

Option 1	<i>See Option 1 in 'Specific Objective' table above</i>
	Description
<i>Benefits</i>	This option would reduce the risk whilst not fully eliminating the CSD's ability to hold participations along the chain.
<i>Compliance costs:</i>	Some CSDs would need to either relocate existing participations elsewhere within their group structure, or possibly sell them. This would notably impact 7 CSDs that responded to the CBA survey, the cost of which cannot be

	estimated (revenues, potential profit or loss resulting from the sale of the participation).
<i>Indirect costs</i>	This option may limit the possibilities for CSDs to engage in some strategic moves aside from with CCPs or trading venues (for instance developing a business on financial information).

<b>Option 2</b>	<i>See Option 2 in 'Specific Objective' table above</i>
	Description
<i>Benefits</i>	This option has the same advantages as option 1. In addition, adding a restriction for CCPs lowers the risk profile of the CSD. This is because CCPs, acting as counterparts and managing collateral deposited, have a significantly different and higher risk profile compared to trading venues.
<i>Costs to regulator:</i>	From a risk focused perspective, this option will reduce the risks that CSDs are exposed to. This is likely to reduce regulatory costs.
<i>Compliance costs:</i>	This option would have an impact on 2 CSDs that responded to the CBA survey, which would need to adjust their group structure to locate the participation in the CCP to a different level.
<i>Indirect costs</i>	This option may further limit the possibilities for CSDs to engage in some strategic moves, even more than Option 1.

### 2.3.3 Should CSDs be required to conduct independent risk analyses?

<b>Specific Objective</b>	Ensure all CSDs offer the appropriate standards of risk mitigation
Option 1	Provide an exemption from the requirement to offer independent risk analyses for CSDs that have banking licenses
Option 2	Do not provide for different requirements for CSDs that have banking licenses, require them to provide independent risk analyses as expected of all CSDs
Preferred Option	<b>Option 2</b> – it is important to ensure all CSDs conduct rigorous risk analyses on potential participations, regardless of whether they already have a banking license.

#### **Impact of the proposed technical options**

<b>Option 1</b>	<i>See Option 1 in 'Specific Objective' table above</i>
<i>Benefits</i>	These CSDs are already subject to increased capital requirements under CSDR for ancillary banking service provisions as they are subject to capital adequacy standards relating to operational, legal, custody, investment and business risks
<i>Costs to regulator:</i>	This may increase regulatory costs, if problems occur in the absence of a proper independent risk analysis.
<i>Compliance costs:</i>	This option would not lead to an increase in compliance costs for CSDs with banking licenses.
<i>Indirect costs</i>	This option may put clients of CSDs at risk as adequate checks are not carried out on CSD participations.

<b>Option 2</b>	<i>See Option 2 in 'Specific Objective' table above</i>
	Description
<i>Benefits</i>	This will ensure that appropriate analysis is conducted on all CSD participations. Capital requirements for CSDs with banking licenses are related to the banking nature and not to the risks arising from participations that are irrespective of this. Therefore it is appropriate and proportionate to require all CSDs to conduct independent risk analyses on participations.
<i>Compliance costs</i>	This is burdensome on compliance functions, particularly for cases with low participation values. The compliance costs would be greater than for Option 1 linked to the checks required and related analysis to ensure participations are appropriate.

## 2.4 CSD Review and Evaluation (Article 22 CSDR)

### INFORMATION FOR SUBMISSION TO COMPETENT AUTHORITIES

#### 2.4.1 What documentation should CSDs be required to submit to competent authorities for the purpose of each review and evaluation?

<b>Specific Objective</b>	The competent authority should have access to all the necessary information to review the arrangements, strategies, processes and mechanisms implemented by a CSD with respect to compliance with CSDR, and to evaluate the risks to which the CSD is, or may be, exposed or which it creates for the smooth functioning of securities markets.
Option 1	<p>For the purpose of each review and evaluation, a CSD should provide to the competent authority a report on the CSD's activities and the substantive changes referred to in Article 16(4) of Regulation (EU) No 909/2014 made during the review period and all related documents, and information regarding periodic events and the activity of the CSD during the review period.</p> <p>The CSD should also submit a declaration of an overall compliance with the provisions of Regulation (EU) No 909/2014 and the delegated and implementing acts under Regulation (EU) No 909/2014 during the review period.</p> <p>The CSD should also submit any additional information requested by the competent authority that is necessary for assessing the compliance of the CSD and its activities with Regulation (EU) No 909/2014 and the delegated and implementing acts under Regulation (EU) No 909/2014 during the review period.</p>
Option 2	The CSD should send to the competent authority all the documentation covering the arrangements, strategies, processes and mechanisms in place, including those that were submitted for the authorisation process, even if they have not been changed during the review period.

Preferred Option	<b>Option 1</b> - it would enable the competent authority to gain a thorough insight into the CSD's arrangements, strategies, processes and mechanisms which demonstrate the CSD's compliance with CSDR, while focusing on the material changes to the arrangements, strategies, processes and mechanisms which were introduced by the CSD in the review period. The competent authority would also have the flexibility to ask for additional information that is necessary for assessing the compliance of the CSD and its activities with Regulation (EU) No 909/2014.
------------------	---

**Impact of the proposed technical options**

<b>Option 1</b>	<i>See Option 1 in 'Specific Objective' table above</i>
	Description
<i>Benefits</i>	It would enable the competent authority to gain a thorough knowledge of the CSD's arrangements, strategies, processes and mechanisms which demonstrate the CSD's compliance with CSDR, while focusing on any material changes to the arrangements, strategies, processes and mechanisms which were introduced by the CSD in the review period. The competent authority would also have the flexibility to ask for additional information that is necessary for assessing the compliance of the CSD and its activities with CSDR.
<i>Costs to regulator:</i>	This may reduce the costs for the regulator, as it would allow for a faster and more focused assessment of the relevant documents.
<i>Compliance costs:</i>	This will slightly increase the costs of compliance for the CSDs, as they would have to keep track of their material changes and provide a report summarising the changes.

<b>Option 2</b>	<i>See Option 2 in 'Specific Objective' table above</i>
	Description
<i>Benefits</i>	It would enable the competent authority to gain a thorough knowledge of a CSD's arrangements, strategies, processes and mechanisms which demonstrate the CSD's compliance with CSDR.
<i>Costs to regulator:</i>	Overall, this may mean that more information is required to be submitted to the competent authority. It may also increase the costs for the regulator that would have to go through all the documents, which would make the review and evaluation process less efficient.
<i>Compliance costs:</i>	This option may imply lower compliance costs for CSDs, it will require less time for sorting the required documentation as all the documentation should be sent to the competent authority regardless as to whether the documents have been altered or not during the review period.

**2.4.2 Should a CSD submit statistical data to the competent authority to enable it to evaluate the risks to which the CSD is, or might be, exposed or which it creates for the smooth functioning of securities markets?**

<b>Specific Objective</b>	The competent authority should have access to all the necessary information to evaluate the risks to which the CSD is, or might be, exposed or which it creates for the smooth functioning of securities markets.
Option 1	For the purpose of each review and evaluation, a CSD should provide to the competent authority statistical data regarding the activity of the CSD during the review period.
Option 2	A CSD should not provide to the competent authority statistical data regarding the activity of the CSD during the review period.
Preferred Option	<b>Option 1</b> - statistical data would enable the competent authority to properly evaluate these risks.

#### **Impact of the proposed technical options**

<b>Option 1</b>	<i>See Option 1 in 'Specific Objective' table above</i>
	Description
<i>Benefits</i>	The statistical data would enable the competent authority to properly evaluate risks. The competent authority will be able to use statistical data to monitor the size and importance of securities transactions and settlements within the financial markets as well as to assess the on-going and potential impact of a given CSD on the securities markets as a whole.
<i>Costs to regulator:</i>	This may imply costs for the competent authorities, as they would need to assess the statistical data received, however this would be useful for the performance of their supervisory tasks.
<i>Compliance costs:</i>	This may imply some small costs for the CSDs, as they would have to aggregate the statistical data. However, the additional costs should not be very high, given the fact that CSDs should already have the respective data either from their own system or should obtain it (in the case of the data on the market value of transactions) in order to comply with other requirements under CSDR and related technical standards.

<b>Option 2</b>	<i>See Option 2 in 'Specific Objective' table above</i>
	Description
<i>Benefits</i>	There are no direct benefits associated with this option. There would be less of a regulatory burden upon CSDs.
<i>Costs to regulator:</i>	The cost to the regulator is that there will be an increased risk of detriment occurring due to the decreased monitoring of the CSD's activity.
<i>Compliance costs:</i>	Compliance costs associated with this option will be non-existent as reporting of statistical data will not be required.

## **2.5 Cooperation Arrangements (Article 24 CSDR)**

As part of the process for drafting the CSDR technical standards ESMA received limited feedback from market participants that related to cooperation arrangements. Feedback received was in support



of ESMA's draft ITS, with respondents calling for ensuring a level playing field in the context of third country CSDs, in particular with regard to CSD recognition.

**What should the exchange of information include in the context of the cooperation between the competent authority of the home Member State and of the host Member State?**

<b>Specific Objective</b>	To streamline information sharing and cooperation between authorities where a CSD authorised in one Member State provides services in another Member State, including through setting up a branch.
Option 1	The exchange of information in the context of the cooperation between the competent authority of the home Member State and of the host Member State should reflect their respective responsibilities and information needs. To avoid unnecessary information flows, the exchange of information should be proportionate and risk-focused.
Option 2	The exchange of information in the context of the cooperation between the competent authority of the home Member State and of the host Member State should be more extensive, with the authorities sharing all information that they receive from the CSD, and internal assessment work they conduct relating to the CSD.
Preferred Option	<b>Option 1</b> - it would strike the right balance between achieving a coordinated supervision framework and proportionate costs for authorities and CSDs, as well as effective supervision of CSDs.

**Impact of the proposed technical options**

<b>Option 1</b>	<i>See Option 1 in 'Specific Objective' table above</i>
	Description
<i>Benefits</i>	It would strike the right balance between a coordinated supervision framework and an appropriate regulatory impact on CSDs, while still facilitating important benefits for the safety of financial markets, particularly in crisis situations.
<i>Costs to regulator:</i>	The authorities may incur costs in setting up such a cooperation framework (lower than the costs in the case of Option 2), however these costs are not likely to be significant as cooperation already exists in practice today in many cases.
<i>Compliance costs:</i>	The larger cross-border CSDs may incur costs in the context of such a cooperation framework, however these costs are not likely to be significant as cooperation already exists in practice today in many cases.

<b>Option 2</b>	<i>See Option 2 in 'Specific Objective' table above</i>
	Description
<i>Benefits</i>	Tight cooperation between authorities across borders would have important benefits for the safety of financial markets, particularly in crisis situations.
<i>Costs to regulator:</i>	The authorities would incur higher costs in setting up such a cooperation framework than in the case of Option 1.
<i>Compliance costs:</i>	The larger cross-border CSDs would incur higher costs in the context of such a cooperation framework than in the case of Option 1.

## 2.6 CSD Recognition (Article 25 CSDR)

When consulting with the industry it became apparent that respondents were almost completely in favour of the proposal included in the consultation paper, with one respondent calling for additional reporting and statistical requirements for third-country CSDs. Comments were also received which related to equivalence and additional requirements to allow EU CSDs to provide services in non-EU markets, ESMA noted that ESMA is not empowered in this respect.

### What is the best approach for determining the information to be sent by a third country CSD for recognition?

<b>Specific Objective</b>	To ensure that a third country CSD's application includes all relevant documents so that that ESMA may take an appropriate decision with respect to recognition.
Option 1	The applicant third country CSD shall certify that it is duly authorised and supervised in its home jurisdiction, that it effectively complies with the legal and supervisory arrangements in that third country, and that it is fully compliant with the third country requirements equivalent to the CSDR.
Option 2	The applicant third country CSD shall include evidence certifying that it is duly authorised and supervised in its home jurisdiction and that it effectively complies with the legal and supervisory arrangements in that third country. In addition, it should also provide information in relation to the main requirements under CSDR, while recognising that the supervision of the recognised CSD would be performed outside the EU, and ESMA would rely on cooperation with the home supervisor
Preferred Option	<b>Option 2</b> – it provides a proportionate approach which will ensure the most appropriate information is sent by a third-country CSD for recognition. This would follow the general principle of non-discrimination between EU and non-EU CSDs, and ensure a consistent treatment.

### Impact of the proposed policies

<b>Option 1</b>	<i>See Option 1 in 'Specific Objective' table above</i>
	Description
<i>Benefits</i>	Easier recognition approval process
<i>Costs to regulator:</i>	More limited costs to the third country authority and ESMA in providing and assessing the relevant information
<i>Compliance costs:</i>	Very limited compliance costs for the third country CSD.
<i>Indirect costs:</i>	<ul style="list-style-type: none"> <li>- The absence of scrutiny and simple reliance on the declaration by the CSD would allow no scrutiny and therefore potential risk imported in the EU.</li> <li>- Unlevel playing field between EU and third country CSDs.</li> </ul>

<b>Option 2</b>	<i>See Option 2 in 'Specific Objective' table above</i>
	Description
Benefits	- Ensure an adequate scrutiny; <ul style="list-style-type: none"> <li>- Limit the potential risk importation in the EU;</li> <li>- Ensure a more balanced approach between EU and third country CSDs.</li> </ul>
Cost to regulators	Higher costs for the third country authority and ESMA given the more extensive list of evidence to be provided and assessed.
Compliance costs	The costs will be higher than for Option 1, given the more extensive list of evidence to be provided.

## 2.7 Risk Monitoring Tools (Article 26 CSDR)

The below cost-benefit analysis was conducted to ensure effective risk monitoring requirements were included in the standards. This involved research and data analysis, primarily based on 31 CSDs' responses to external questionnaires.

### INTERNAL AUDIT FUNCTION

Of the 31 CSDs that provided feedback on their internal audit practices, all were already subject to regular internal audits.

#### Internal audit arrangements

- 29 CSDs had an internal audit function, either at group or CSD level, thus audits were performed through own resources
- 2 CSDs did not have an internal audit function, audits were performed by an external consultant

Below is a breakdown of the existing internal audit arrangements for each CSD respondent:

Internal audit function		Number of CSDs
CSD Level	Dedicated	7
	Not dedicated	5
	Shared by a group of CSDs	1
	Performs audit for other activities within CSD	1
	Performs audit for participations of CSD	2
	Performed by external consultant	2
At Group Level		13

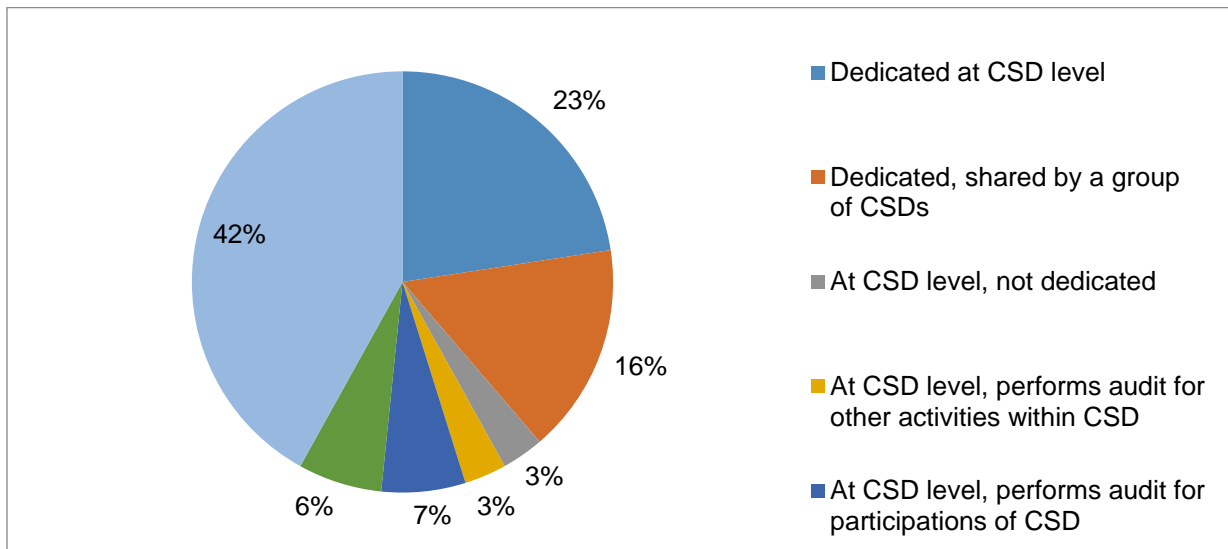


Chart created by external consultant, using information gathered from the previously mentioned questionnaires.

For some CSDs the local head of audit is shared between a group of CSDs with team members based locally. Considering the connections and operational proximities between CSDs in each group, we consider that this organisation is compliant with ESMA's proposals.

### Frequency of internal audits

The majority of CSDs perform internal audit at least once a year, as required by ESMA.

- 29 out of 31 CSDs internal audit practices are already compliant with ESMA's proposals:
  - o 8 CSDs undertake an internal audit at least twice a year
  - o 21 CSDs undertake an internal audit annually
- For the other 2 CSDs, an internal audit is undertaken less frequently than on an annual basis.

The two CSDs which undertake the internal audits less frequently than annually justify that internal audits are undertaken less than annually by invoking a group policy.

None of these CSDs make the results of the internal audits publicly available.

### External audits

An external financial audit was performed for all 31 of these CSDs, at least annually. For nine of these CSDs it was performed at least semi-annually. All but five of the 31 CSDs made those financial audits publicly available. No CBA was conducted in this area because all of the CSDs sampled were already compliant with CSDR.

There was no relevant data received as part of the consultation process that related to the availability to competent authorities.

### Cost estimates

19 CSDs indicated they do not have a dedicated internal audit function. Six CSDs provided an estimation of the on-going cost of implementing a dedicated internal audit function (no one-off cost). These answers were extrapolated to 13 other CSDs that do not have an internal audit division at CSD level.

Cost estimates provided by the six CSDs for implementing a permanent dedicated internal audit function ranged from EUR 50K to EUR 200K as initial one-off cost, without a firm indication of the size of the CSD. The average on-going cost of compliance amounts to EUR 142K.

Based on these assumptions, the total cost for the 19 CSDs without the dedicated function at the CSD level is estimated to be EUR 2.7M.

## INTERNAL AUDIT FUNCTION AT CSD LEVEL

### 2.7.1 What would be effective audit methods to which a CSD should be subject?

<b>Specific Objective</b>	Define effective audit methods to which a CSD should be subject.
Option 1	CSDs must have a dedicated internal audit function at CSD level.
Option 2	<p>To ensure an adequate control of the activity performed by CSDs, independent audits covering the operations of the CSD, risk management processes, compliance and internal control mechanisms, should be put in place and performed regularly. The independence of audits should not necessarily require the involvement of an external auditor, provided that the CSD demonstrates to the competent authority that the independence of its internal auditor is properly ensured. In order to ensure the independence of its internal audit function, the CSD should also establish an audit committee.</p> <p>Where the CSD belongs to a group the internal audit function may be carried out at group level provided that:</p> <ul style="list-style-type: none"> <li>- it is separate and independent from other functions and activities of the group;</li> <li>- it has a direct reporting line to the management body of the CSD;</li> <li>- the arrangement concerning the operation of the internal audit function does not prevent the exercise of supervisory and oversight functions, including on-site access to acquire any relevant information needed to fulfil those functions.</li> </ul>
Preferred Option	<b>Option 2</b> achieves the same objective as Option 1 by allowing the CSD to rely on shared resources. It would also allow for more flexibility in terms of allowing the CSD not to necessarily use an external auditor, provided that the CSD demonstrates to the competent authority that the independence of its internal auditor is properly ensured. The independence of the CSD's internal audit committee should also be

	ensured by the CSD's audit committee. The associated costs would be significantly lower than in the case of Option 1.
--	---

**Impact of the proposed policies**

<b>Option 1</b>	<i>See Option 1 in 'Specific Objective' table above</i>	
	Qualitative description	Quantitative description
<i>Benefits</i>	Simple, clear mechanism on internal audit which can provide a third line of defence for CSDs, from the perspective of a fully resourced internal function, set up specifically with that CSD in mind.	These benefits cannot be demonstrated in a quantitative fashion.
<i>Compliance costs:</i>	<p>CSDs who do not already comply with the requirement would have to:</p> <ul style="list-style-type: none"> <li>- dedicate part of their audit teams at Group level to the CSD</li> <li>- implement a new and costly internal audit function for those CSDs without an existing internal audit function</li> </ul>	<p>Out of the CSDs surveyed for the CBA, 20 CSDs would be impacted. Expected on-going costs for CSDs range from EUR 50k to EUR 265k per annum. For smaller CSDs, setting up an internal audit function could be costly compared to the benefits. For CSDs that do have an internal audit function, which also audits other activities within the company or audits companies in which the CSD has a participation (a CCP for instance), creating an internal audit function solely responsible for the CSD would involve increased costs. These would range from EUR 50k to EUR 200k per annum per CSD based on the evidence collected by ESMA.</p>

<b>Option 2</b>	<i>See Option 2 in 'Specific Objective' table above</i>	
	Description	
<i>Benefits</i>	The option enables the CSD to reduce costs via sharing resources whilst keeping internal audits independent of the services provided by the CSD. It would also allow for more flexibility in terms of allowing the CSD not use necessarily an external auditor, provided that the CSD demonstrates to the competent authority that the independence of its internal auditor is properly ensured. The independence of the CSD's internal audit committee should also be ensured by the CSD's audit committee. The associated costs would be significantly lower than in the case of Option 1.	
<i>Compliance costs:</i>	CSDs that do not have such arrangements currently in place for internal audits would have to implement the arrangements at a cost, arranging the required agreements and sourcing the appropriate resources. Based on the research conducted prior to the formulation of the technical standards, 2 EU CSDs are	

	currently in this position; therefore the overall cost to the industry should be limited.
<i>Indirect costs</i>	Potential conflicts of interests will have to be adequately identified and managed.

## FREQUENCY OF PERFORMANCE OF INTERNAL AUDITS

### 2.7.2 What should be the frequency of independent audits to ensure low risk for the CSD?

<b>Specific Objective</b>	Independent audits should be performed with reasonable frequency to ensure low risk for the CSD.
Option 1	Independent audits should be performed, at least on an annual basis.
Option 2	<p>A CSD's operations, risk management processes, internal control mechanisms and records shall be subject to independent internal or external audits to be performed at least every two years. The frequency shall be based on a documented risk assessment.</p> <p>A CSD's financial statement shall be prepared on an annual basis and be audited by statutory auditors or audit firms within the meaning of Directive 2006/43/EC of the European Parliament and of the Council.</p>
Preferred Option	<p>Although Option 1 would ensure that the CSD is subject to independent audits on an annual basis, Option 2 would be more proportionate as it would allow for both a regular frequency of audits and a focus on the risks involved in the activities of the CSD, with a risk assessment providing an effective measure of the appropriate timing for auditing specific areas of the business.</p> <p><b>Option 2</b> - in order to achieve a more balanced approach, with the individual frequencies for different elements based on a documented risk assessment.</p>

#### *Impact of the proposed policies*

<b>Option 1</b>	<i>See Option 1 in 'Specific Objective' table above</i>
	Description
<i>Benefits</i>	Most CSDs already comply with this requirement. The approach would ensure that the activities of the CSD are being regularly monitored by an independent reviewer.
<i>Compliance costs:</i>	<p>Most CSDs' existing practices are aligned with this approach and therefore additional compliance costs would be unlikely.</p> <p>On average, the cost of option 1 would be twice that of option 2 (review every year instead of every 2 years on average).</p>
<b>Option 2</b>	<i>See Option 2 in 'Specific Objective' table above</i>
	Description

<i>Benefits</i>	All CSDs already comply with this requirement to a certain extent, however the requirement would bring structure and turn the existing practices into an EU wide requirement for CSDs.
<i>Costs to regulator:</i>	This option would not create additional costs for regulators.
<i>Compliance costs:</i>	It appears that no CSD would be impacted by increased compliance costs, one slight cost may be the formalisation of CSDs' existing practices around internal audits.
<i>Indirect costs</i>	Smaller CSDs which currently perform internal audits annually could decide to do so less often which may lead to a lowering of the standard of their risk monitoring.

## 2.8 Record Keeping (Article 29)

### CONTENTS OF RECORD-KEEPING: ADEQUACY OF THE DATA RECORDED FOR THE AIM OF RECONSTRUCTION OF CSD OPERATIONAL PROCESS

#### DESCRIPTION OF THE EXISTING SITUATION

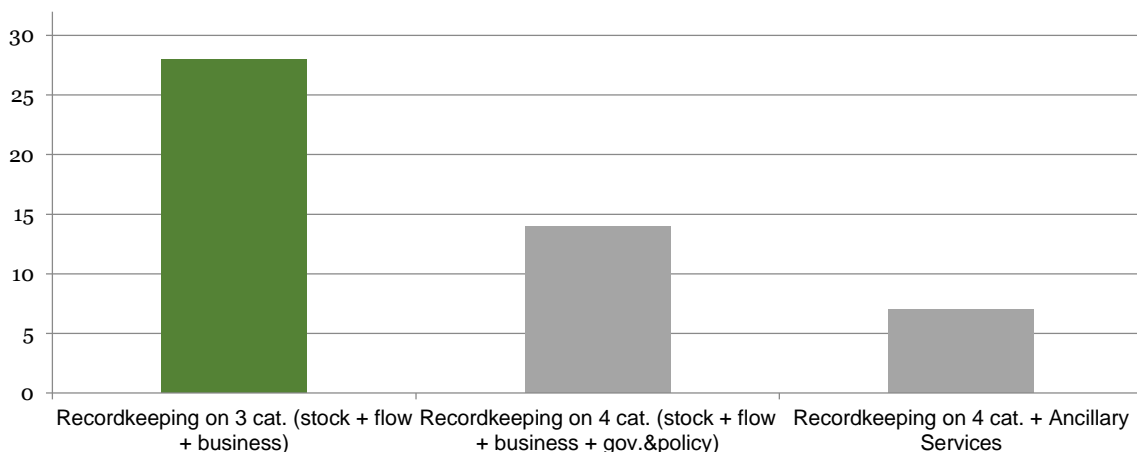
*Data collection methodology: specific studies made for the discussion paper, answers to the external consultant's questionnaire, CSDs' answers to external questionnaire, ESMA summary of CSDs' responses to the Discussion Paper on CSDR.*

#### **Contents of current CSD record-keeping**

A list of minimum requirements considered by ESMA includes the following categories of records:

1. stock (e.g. issuers, accounts, securities ID) ;
2. flow (e.g. moment of entry; trade date; currency; ...);
3. business (e.g. types of services offered; penalties; ...);
4. governance and policy (e.g. organisational charts; minutes of meetings; ...)

*Categories of records*



*Table prepared by the external consultant indicating current record-keeping arrangements at the 31 CSDs.*



28 of these CSDs declared that they keep records on the three first categories – stock, flow and business. 14 out of the responding CSDs declared keeping records on all 4 categories – stock, flow, business and governance & policy. Only seven CSDs declared that they keep records on the four categories and also on ancillary services.

### **Availability**

#### Format

Most CSDs keep records on media that allow the storage of information in a format accessible for future reference by the competent authorities. The table below prepared by the external consultant gives an indication of the different types of media used to store information for the 31 CSDs.

Type of Media	Computer File	Computer Tape	DLT/Magnetic Tape	Microfiche	Hard Copy	CD/DVD	Database
Number of CSDs holding records in each media	30	20	2	5	5	5	2

#### Reporting process

In terms of availability, 22 CSDs declared that they make records available for competent authorities. Out of these 22 CSDs, 12 have specified the format under which data is reported to competent authorities. The below table refers to the different formats currently in use, and shows that some CSDs make records available in more than one format.

Different Formats for reporting to CAs	Direct Data Feed	Online Queries	File Transfer	CD/DVD	Excel/Word	Paper
Number of CSDs using this format	1	3	10	2	5	3

### **Duration**

CSDR requires that all records are maintained for at least ten years. But some CSDs (10 out of 28 CSDs for which the information was available) only keep records for a shorter duration (five to seven years).

### **Costs estimation of implementing the proposed requirements**

The following study is based on information provided by ECSDA as part of the ad hoc study they conducted on this topic for the ESMA discussion paper. This study details the overall costs provided in ECSDA's answer to the discussion paper.

18 CSDs of various sizes were asked to provide their assessment of both one-offs and ongoing costs of implementing four different enhancements:

Cost	Definition
------	------------

#1	<b>Maintaining all proposed records in open, non-proprietary format</b>	Costs for maintaining all the proposed records in an open, non-proprietary format (as opposed to a proprietary format)
#2	<b>Direct Data feed</b>	Costs in case a direct data feed from the CSD to the competent authority is required
#3	<b>Mandatory use of LEIs</b>	Costs in case the use of LEIs for is made mandatory for CSD records on each settlement instruction, in the context of the reporting to authorities..
#4	<b>Others</b>	Other costs

*Table provided to ESMA by the external consultant*

18 CSDs have provided estimations on costs according the different options described in the Discussion Paper.

When data was not provided, costs were estimated based on figures provided by similar CSDs. For smaller CSDs, figures were usually not provided, and, when they were provided, they could be considered as outliers, leading to possible over- / under-estimations of the actual cost for those CSDs.

Costs are presented below for 18 CSDs, corresponding to the larger ones (over 6 million deliveries per year).

3 categories of costs related to different IT developments were considered:

1. Maintaining all the proposed records in an open, non-proprietary format
2. Mandatory use of LEIs
3. Direct data feed

Costs for maintaining all the proposed records in an open, non-proprietary format

Group of CSDs	A) Costs for maintaining all the required records in an open, non-proprietary format			
	One-off cost		Ongoing cost	
	Min	Max	Min	Max
<b>CSDs with &gt;20K deliveries and &lt;200K deliveries/day</b>	13 388 990	19 951 823	3 337 573	4 714 146
<b>CSDs with &gt;200K deliveries per day</b>	8 084 750	17 012 500	1 626 800	2 826 800
<b>TOTAL CSDs</b>	<b>21 473 740</b>	<b>36 964 323</b>	<b>4 964 373</b>	<b>7 540 946</b>

*Table provided to ESMA by the external consultant*

Mandatory use of LEIs

The costs provided correspond to the use of LEIs for reporting purposes. Only 1 CSD did estimate the cost of using the LEI in the overall platform (one-off cost being in that case EUR 15M instead of EUR 200K).

<b>B) Additional costs: mandatory LEIs for reporting purposes</b>				
Group of CSDs	One-off cost		Ongoing cost	
	Min	Max	Min	Max
CSDs with >20K deliveries and <200K deliveries/day	3 254 177	5 217 198	646 274	656 940
CSDs with >200K deliveries per day	1 544 750	3 072 500	226 800	226 800
<b>TOTAL CSDs</b>	<b>4 798 927</b>	<b>8 289 698</b>	<b>873 074</b>	<b>883 740</b>

Table provided to ESMA by the external consultant

Direct data feed

<b>C) Additional costs: direct data feed</b>				
Group of CSDs	One-off cost		Ongoing cost	
	Min	Max	Min	Max
CSDs with >20K deliveries and <200K deliveries/day	5 300 326	9 937 764	1 740 305	1 900 305
CSDs with >200K deliveries per day	3 480 550	6 930 500	907 200	907 200
<b>TOTAL CSDs</b>	<b>8 780 876</b>	<b>16 868 264</b>	<b>2 647 505</b>	<b>2 807 505</b>

Table provided to ESMA by the external consultant

One-off “costs for maintaining all the proposed records in an open, non-proprietary format” (based on CSDs’ answers and estimations) would represent a significant amount.

Total costs

<b>Total costs</b>				
Group of CSDs	One-off cost		Ongoing cost	
	Min	Max	Min	Max
CSDs with >20K deliveries and <200K deliveries/day	21 943 493	35 256 784	5 724 152	7 451 391
CSDs with >200K deliveries per day	13 110 050	27 015 500	2 760 800	3 960 800
<b>TOTAL CSDs</b>	<b>35 053 543</b>	<b>62 272 284</b>	<b>8 484 952</b>	<b>11 412 191</b>

Table provided to ESMA by the external consultant

### Impact of the overall cost on CSDs

The following table estimates impacts of the related costs by calculating the ratio between (i) estimated costs on CSD income, only for maintaining all the proposed records in an open, non-proprietary format and (ii) the total CSD income:

CSD	Costs for maintaining all the required records in an open, non-proprietary format		Total costs	
	One-off costs as % of CSD income	On-going costs as % of CSD income	One-off costs as % of CSD income	On-going costs as % of CSD income
CSD 9	8%	1,6%	10%	2,1%
CSD 22	8%	1,9%	10%	2,5%
CSD 11	6%	1,2%	9%	4,7%
CSD 12	6%	2,4%	7%	3,0%
CSD 16	3%	0,6%	4%	0,6%
CSD 17	3%	0,5%	3%	0,5%
CSD 19	2%	0,0%	2%	0,0%
CSD 21	2%	0,3%	2%	0,3%
CSD 23	2%	0,4%	4%	0,8%
CSD 26	1%	0,1%	4%	0,5%
CSD 27	1%	0,1%	3%	0,4%
CSD 20	0%	0,5%	1%	0,7%
CSD 32	0%	0,0%	1%	0,1%

Table provided to ESMA by the external consultant

In some cases, the investment tends to represent significant costs as compared to the income, especially for second-tier CSDs.

### **Data not stored today**

6 CSDs and one CSD group did mention the data that they do not have or store today, half of which not in T2S. The analysis below considers data proposed by ESMA in the Discussion Paper and shows records posing a problem to CSDs.

### Records on stock

Out of 20 records proposed in the Discussion Paper, 15 are neither available nor stored. Yet it should be noted that but for seven records which represent a difficulty for at least three CSDs, the other 13 records are already available or stored.

Records			Accessibility and storage	
			Difficulty on the record	Nb of CSDs (out of 6 + 1 group of CSDs)
SR	1	Issuers	Yes	1
SR	2	Country of establishment of Issuers	Yes	1
SR	3	Persons exercising control on Issuers	Yes	6
SR	4	Country of establishment of persons exercising control on issuers	Yes	7
SR	5	Issuers' securities' accounts	Yes	1
SR	6	Settlement banks used by Issuers	Yes	3
SR	7	Cash accounts used by Issuers	Yes	4
SR	8	Securities initially recorded in the CSD	Yes	1
SR	9	Securities maintained by the CSD	Yes	1
SR	10	Characteristics of the securities initially recorded in or maintained by the CSD	Yes	1
SR	11	Participants		0
SR	12	Country of establishment of Participants		0
SR	13	Persons exercising control on Participants	Yes	6
SR	14	Country of establishment of persons exercising control on Participants	Yes	7
SR	15	Participants' securities accounts		0
SR	16	Settlement banks used by Participants	Yes	1
SR	17	Cash accounts used by Participants		0
SR	18	Issuers' securities' accounts - end of day balances	Yes	1
SR	19	Participants securities accounts - end of day balances		0
SR	20	Participants cash accounts - end of day balances	Yes	4

*Table provided to ESMA by the external consultant*

Records representing a difficulty for almost all CSDs are SR3, SR4, SR13 and SR14. CSDs usually do not have the information on persons or entities who control their participants or the issuers.

### Records on flows

Out of the 31 proposed records:

14 records are already available and stored;

17 are neither available nor stored. Among these 17 records:

- 8 records represent a difficulty for at least three CSDs,
- The other 9 records only represent a difficulty for one to three CSDs.

Records			Accessibility and storage	
			Difficulty on the record	Nb of CSDs (out of 6 + 1 group of CSDs)
FR	1	Delivering participant		0
FR	2	Delivering participant settlement instruction (delivering instruction)		0
FR	3	Client of the delivering participant, where applicable	Yes	3
FR	4	Delivering participant securities account		0
FR	5	Delivering participant's settlement bank	Yes	1
FR	6	Delivering participant cash account		0
FR	7	Receiving participant		0
FR	8	Receiving participant settlement instruction (receiving instruction)		0
FR	9	Client of the receiving participant, where applicable	Yes	3
FR	10	Receiving participant securities account		0
FR	11	Receiving participant's settlement bank	Yes	1
FR	12	Receiving participant cash account		0
FR	13	Moment of entry timestamp of the delivering instruction		0
FR	14	Moment of entry timestamp of the receiving instruction		0
FR	15	Moment of irrevocability timestamp of the delivering instruction	Yes	5
FR	16	Moment of irrevocability timestamp of the receiving instruction	Yes	5
FR	17	End of validity date of the delivering instruction, where applicable	Yes	4
FR	18	End of validity date of the receiving instruction, where applicable	Yes	4
FR	19	Matching timestamp, where applicable	Yes	2
FR	20	Trade date		0
FR	21	Intended settlement date	Yes	1
FR	22	Securities object of the settlement instructions	Yes	1
FR	23	Currency		0
FR	24	Settlement amount		0
FR	25	Quantity/nominal amount		0
FR	26	Settlement: Yes/No	Yes	2
FR	27	Settlement timestamp	Yes	1
FR	28	Settlement agent of the cash leg	Yes	1
FR	29	System generated delivering instructions (in case of partial delivery, shaping)	Yes	3
FR	30	System generated receiving instructions (in case of partial delivery, shaping)	Yes	2
FR	31	Buy-in: Yes/No	Yes	6

Table provided to ESMA by the external consultant

Records representing a difficulty for almost all CSDs are: FR15, FR16 and FR17, that is the moment of irrevocability and the end of validity of the instructions, and the buy-in indicator.

#### Business/other records

Out of the 10 proposed records, five are neither available nor stored.

Records			Accessibility and storage	
			Difficulty on the record	Nb of CSDs (out of 6 + 1 group of CSDs)
BRO	1	Issuers' and Participants' details, including authorised signatures	Yes	1
BRO	2	Settlement agents for the cash legs	Yes	1
BRO	3	Types of services offered	Yes	1
BRO	4	Categories of Issuers accepted	Yes	1
BRO	5	Categories of securities initially recorded or maintained		0
BRO	6	Categories of Participants accepted		0
BRO	7	Types of securities' accounts offered		0
BRO	8	Volumes and values of settlement fails		0
BRO	9	Penalties	Yes	2
BRO	10	Major incidents in relation to core services (including summaries of incidents and of remedial actions)		0

Table provided to ESMA by the external consultant

No single record represents a difficulty for all CSDs.

Records in relation to governance and policy

Out of the 17 proposed records:

10 records are already available and stored;

7 are either not available or not stored. Among these records:

- 2 records represent a difficulty for at least three CSDs;
- The other 5 records only represent a difficulty for one or two CSDs.

Records			Accessibility and storage	
			Difficulty on the record	Nb of CSDs (out of 6 + 1 group of CSDs)
GP	1	Organisational charts for the management body and relevant committees, operational units, risk management unit and all other relevant units or divisions		0
GP	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	Yes	1
GP	3	CSD participations in other legal entities	Yes	1
GP	4	Documents attesting the policies, procedures and processes required under the relevant organisational requirements		0
GP	5	Minutes of management body meetings and, if applicable, of meetings of sub-committees of the management body and of senior management committees		0
GP	6	Minutes of meetings of the user committee	Yes	3
GP	7	Minutes of consultation groups with participants and clients, if any	Yes	2
GP	8	Internal and external audit, risk management, compliance reports, and reports by consultant companies, including management responses	Yes	1
GP	9	Major outsourcing contracts		0
GP	10	Business continuity policy and disaster recovery plan		0
GP	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	Yes	2
GP	12	Records of the results of the back and stress tests performed for the CSDs providing banking type of ancillary services	Yes	3
GP	13	Written communications with competent authorities, ESMA and relevant authorities		0
GP	14	Legal opinions received in accordance with provisions on organisational requirements		0
GP	15	Where applicable, legal documentation regarding link arrangements		0
GP	16	The most complete documents describing the development of new business initiatives		0
GP	17	Tariffs and fines that the CSD has in place AS Ancillary services		0

*Table provided to ESMA by the external consultant*

No single record represents a difficulty for all CSDs.

Ancillary services

Out of the 15 proposed records, no record is available and stored by all CSDs considered. Among these records:

5 records represent a difficulty for at least three CSDs

the other 10 records only represent a difficulty for one or two CSDs.

Records			Accessibility and storage	
			Difficulty on the record	Nb of CSDs (out of 6 + 1 group of CSDs)
AS	1	allocation and management of ISIN codes and similar codes (e.g. issuer/requesting party identification, securities type, securities characteristics, notional amount)	Yes	1
AS	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)	Yes	1
AS	3	cash accounts provided by the CSD (e.g. LEI of participant/investor using the cash accounts, credit limits, currency, deposits amounts)	Yes	5
AS	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)	Yes	4
AS	5	data and statistics services to market/census bureaus (e.g. entities served; data provided; purpose)	Yes	2
AS	6	general collateral management services as agent (e.g. entities served; purpose; value details)	Yes	5
AS	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)	Yes	4
AS	8	IT services provided (e.g. details on nature of services and how different from the core IT services)	Yes	2
AS	9	operations in relation to cash accounts (e.g. type; purpose; )	Yes	2
AS	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)	Yes	2
AS	11	regulatory reporting services (e.g. under which regulation; nature of service)	Yes	1
AS	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)	Yes	3
AS	13	services related to shareholders' registers (e.g. ISIN, relevant entities involved in the process, information flows)	Yes	2
AS	14	settlement matching, order routing, trade confirmation, trade verification operations	Yes	2
AS	15	the links established by the CSD	Yes	2

Table provided to ESMA by the external consultant

Records that represent a real issue for CSDs are: AS3, AS4, AS6 and AS7, that is records on collateral management and banking type of ancillary services which are provided only by a limited number of CSDs.

#### Conclusion – all records

As a conclusion, it appears a number of records are today either not available or not stored by CSDs:

34 records are available and stored by all CSDs considered;

59 records represent a difficulty for at least one CSD;

Among these 59, 22 records present a difficulty to a number of the CSDs considered (at least 3).

Especially when recordkeeping requirements apply to the daily activity (records on stocks and on flows), they may represent an issue and actually provide a first explanation on the costs provided in order to comply with ESMA's proposal on record keeping. Among these, 11 records are not available or not stored by almost any CSD.

Records on stock: SR3, SR4, SR13 and SR14

Records on flows: FR15, FR16 and FR17

Ancillary services: AS3, AS4, AS6 and AS7

### **2.8.1 What records should a CSD maintain so as to enable the competent authority to monitor the compliance with the requirements under CSDR?**



<b>Specific Objective</b>	To use a list of minimum requirements regarding the records that a CSD should maintain that allow competent authorities to monitor the compliance with the requirements under CSDR
Option 1	Require that a CSD maintains records, including for business continuity purposes, and that would enable the reconstruction of each operation
Option 2	Require that a CSD records the following information, without the requirement related to business continuity, and the enabling of the reconstruction of each operation: <ul style="list-style-type: none"> <li>a) Transaction/Settlement Instruction (Flow) Records covering records of all transactions, settlement instructions and orders concerning settlement restrictions that it processes.</li> <li>b) Position (Stock) records covering records of positions corresponding to all securities accounts that the CSD maintains.</li> <li>c) Ancillary services records covering each of the ancillary services provided by a CSD in accordance with Sections B and C of the Annex to Regulation (EU) No 909/2014, including the end of day balances of the cash accounts provided by the CSD or the designated credit institution for each currency.</li> <li>d) Business records covering records of activities related to the CSD's business and internal organisation.</li> </ul>
Preferred option	Option 1 would result in all CSDs needing to keep a large volume of records for 10 years including for business continuity purposes and allowing the reconstruction of each operation. This would be very costly and extremely difficult to achieve especially in the context of system changes. Option 2 would avoid requirements for CSD to maintain data that is very cumbersome and costly for a long period of time, and would focus on the most important elements that would allow the competent authority to monitor the compliance with the requirements under CSDR.  <b>Option 2</b> – it would create a common starting point from which competent authorities can conduct supervisory tasks and also limit record keeping costs for CSDs.

### **Impact of the proposed policies**

<b>Option 1</b>	<i>See Option 1 in 'Specific Objective' table above</i>
	Description
<i>Benefits</i>	Competent authorities will have access to a large volume of information from which they can reconstruct the operational processes of CSDs and ensure effective supervision based upon a wide ranging historical data.
<i>Costs to regulator:</i>	There will be limited one-off costs to the regulator. However there will be on-going costs that relate to the analysis of the broad range of data that is recorded.
<i>Compliance costs:</i>	The costs for CSDs to maintain records for including for business continuity purposes and that would enable the reconstruction of each operation would be very high.

<i>Indirect costs</i>	There will be costs for the CSD participants that would need to provide the CSD with relevant information.
<b>Option 2</b>	<i>See Option 2 in 'Specific Objective' table above</i>
	Description
<i>Benefits</i>	This option will ensure the availability of harmonised records across the EU, and it will avoid the significant costs of managing and storing information that is difficult to maintain for a CSD. The record keeping requirements that have been proposed are focused and clear, addressing the information and data that is most useful to CSDs and regulators.
<i>Costs to regulator:</i>	Costs to competent authorities would be lower when compared to Option 1. The information requested in option two is less detailed than that required under option one (which is a broader requirement). Therefore the analysis of the information will be slightly less costly for regulators.
<i>Compliance costs:</i>	Compliance costs should be significantly lower than for Option 1. The requirements are more aligned to records that CSDs already keep and the ISO standards.

## RECORD KEEPING FORMAT AND AVAILABILITY

### 2.8.2 How can the CSDR technical standards make it possible for competent authorities to have adequate access to accurate records maintained by CSDs?

Specific Objective	To allow the competent authorities to have adequate access to accurate records maintained by CSDs.
Option 1	Require data recording and availability as defined below: <ul style="list-style-type: none"> <li>- Records retained in a format that allows storage of information that is accessible for future reference by the competent authorities;</li> <li>- Require a direct data feed to the Competent Authority for flow and stock records maintained by a CSD.</li> <li>- A CSD shall use a legal entity identifier (LEI) or a bank identifier code (BIC) to identify in its records:               <ul style="list-style-type: none"> <li>(a) CSDs</li> <li>(b) CSD participants;</li> <li>(c) settlement banks;</li> <li>(d) issuers.</li> </ul> </li> </ul>
Option 2	Require data recording and availability as defined below: <ul style="list-style-type: none"> <li>- Records retained in a format that allows storage of information that is accessible for future reference by the competent authorities;</li> <li>- Require a direct data feed to the competent authority for flow and stock records, when requested by the competent authority; provided that the CSD is given sufficient time to implement the necessary facility to respond to such a request.</li> <li>- A CSD shall use a legal entity identifier (LEI) or a bank identifier code (BIC), with the obligation to convert to LEI for the purposes of reporting to authorities to identify in its records:               <ul style="list-style-type: none"> <li>(a) CSDs;</li> <li>(b) CSD participants;</li> <li>(c) settlement banks;</li> <li>(d) issuers.</li> </ul> </li> </ul>
Option 3	Require data recording and availability as defined below: <ul style="list-style-type: none"> <li>- Records retained in a format that allows storage of information that is accessible for future reference by the competent authorities;</li> <li>-Not require a direct data feed to the Competent Authority for flow and stock records maintained by a CSD;</li> <li>-Not require CSDs to use LEIs for their records.</li> </ul>
Preferred option	Option 1 would enable competent authorities to monitor compliance with the requirements under CSDR while also providing a high degree of harmonisation between CSDs. Option 2 would bring the same benefits, but, allowing for more flexibility, it would entail lower costs. Option 3 would be the most flexible, but would not bring any harmonisation in the practices of the CSDs and would not allow competent authorities to compare data across CSDs for the actual

	<p>identification of potential risks.</p> <p><b>Option 2</b> – is the preferred option as it is the most balanced approach, by providing a certain degree of harmonisation, while allowing for some flexibility in order to reduce the implementation costs.</p>
--	--

**Impact of the proposed policies**

<b>Option 1</b>	<i>See Option 1 in 'Specific Objective' table above</i>
	Description
<i>Benefits</i>	This option will enable competent authorities to monitor compliance with the requirements under CSDR while also providing a high degree of harmonisation between CSDs.
<i>Costs to regulator:</i>	Competent authorities will need to ensure access, storage and analysis of the information provided by CSDs.
<i>Compliance costs:</i>	The overall one-off costs (for the IT developments, such as for the use of LEIs and direct data feeds) for the industry will be significantly higher for this option than for Option 2.

<b>Option 2</b>	<i>See Option 2 in 'Specific Objective' table above</i>
	Description
<i>Benefits</i>	This option will have similar benefits to Option 1, but, allowing for more flexibility, it would entail lower costs.
<i>Costs to regulator:</i>	Lower costs than for Option 1, as the competent authorities will not need to ensure access to direct data feeds provided by CSDs.
<i>Compliance costs:</i>	Lower costs than for Option 1, as there will be fewer IT developments that would be necessary to be implemented by CSDs.

<b>Option 3</b>	<i>See Option 3 in 'Specific Objective' table above</i>
	Description
<i>Benefits</i>	This option will not entail changes in the current practices of the CSDs.
<i>Costs to regulator:</i>	Lower costs than for Option 1, as the competent authorities will not need to ensure access to direct data feeds provided by CSDs. Higher costs than Option 2, as, in the absence of the use of LEIs for reporting purposes, the competent authorities will have to develop alternative ways for aggregating and filtering data from different sources for supervisory purposes.
<i>Compliance costs:</i>	Potentially no costs

## 2.9 Reconciliation Measures (Article 37 CSDR)

### EXISTING RECONCILIATION PROCESSES

To conduct the cost-benefit analysis of options for reconciliations, data was collected using questionnaires. Nine CSDs provided information about the types of reconciliation that they currently conduct. Of the nine, seven conduct external reconciliations (with a third party), and eight conduct internal reconciliations (between internal accounts). In total 29 different reconciliations are carried out by the nine CSDs that responded to these questions and each CSD carries out at least one reconciliation. All but one CSD responded that they use double-entry accounting systems; the other CSD will begin to use this in 2015.

#### *Internal Reconciliations*

With regard to internal reconciliations the majority of the CSD respondents run a reconciliation comparing participants' end of day balances to issuer end of day balances within the CSD. There were also two CSDs which reconcile the previous end of day balance with the current day balance and settlements. Of the nine CSDs, only one runs an internal physical reconciliation, given that most markets now operate on a dematerialised basis.

#### *Corporate actions*

Only one CSD mentioned reconciliation processes specific to corporate actions, referring to an additional reconciliation for equities that compared (a) the number of issued shares submitted by the issuer for the corporate action event with (b) the number of registered shares at the local registration office. No CSD which responded to the questionnaire mentioned any existing post-corporate action reconciliations.

#### *External Reconciliations*

Of the nine CSDs involved in the research, seven have external reconciliations in place, however according to responses only one CSD of the nine reconciles with external registrars and one has reconciliations with participants' positions in its own books – required by local law.

With regard to reconciliations with ICSDs in the case of common depositaries, banks confirmed reconciliations in place with them daily for eligible new global note movements with one ICSD, and monthly in other cases.

#### *Existing reconciliation problems*

To consider the importance of reconciliation requirements it is necessary to recognise the issues that can arise with reconciliations, and the resultant effects for the settlement process.

Most of the CSDs which responded did not refer to specific historical or current issues with reconciliations. One CSD noted that there were normally a couple of issues with reconciliations per month that are solved within a few hours or within a business day. It was suggested by some respondents that solving problems with CSD links would take longer. Various reasons for reconciliation failures are mentioned, including system problems, incorrect bookings by operational units, inappropriate information provided by issuers and incorrect information from custodians.

Consequentially, when there are reconciliation problems there can be serious impacts on the settlement processes and reputational damage to the functioning of the market.

## INTERNAL RECONCILIATIONS

### 2.9.1 How can the CSDR technical standards ensure CSDs have the necessary controls and procedures in place to protect the integrity of the issue and to protect market participants and investors from the consequences of securities inflation or deletion?

<b>Specific Objective</b>	Ensure CSDs have the necessary procedures and controls to protect the integrity of the issue to help protect market participants and investors from the consequences of securities inflation or deletion
Option 1	<ul style="list-style-type: none"> <li>- A CSD shall use double-entry accounting, according to which for each credit entry made on a securities account maintained by the CSD, centrally or not centrally, there is a corresponding debit entry on another securities account maintained by the same CSD</li> <li>- Where the reconciliation process concerns securities subject to immobilisation, a CSD shall put in place adequate measures to protect the physical securities from theft, fraud, and destruction. Such measures shall at least include the use of vaults whose design and location ensure a high level of protection against floods, earthquakes, fire and other disasters.</li> <li>- Independent audit controls of the vaults, including physical inspections, shall be performed at least annually. The CSD shall share the results of those audit controls with the competent authority.</li> </ul>
Option 2	Same as Option 1, with the following additional measure: the CSD shall compare the previous end-of-day balance with all the settlements processed during the day and the current end-of-day balance for each securities issue and securities account centrally or not centrally maintained by the CSD.
Preferred Option	<b>Option 2</b> – it would ensure more thorough reconciliation measures and a higher accuracy of the process.

#### **Impact of the proposed policies**

<b>Option 1</b>	See Option 1 in 'Specific Objective' table above
	Description
<b>Benefits</b>	The proposed reconciliation measures would ensure that adequate controls are in place to ensure the integrity of the issue, both in the case of dematerialised securities, and in the case of physical securities.

<i>Compliance costs:</i>	<ul style="list-style-type: none"> <li>- The use of double-entry accounting should not imply additional costs, as this is a current practice for CSDs in the EU.</li> <li>- The independent audit controls of the vaults may trigger additional costs, though these measures will affect a limited number of CSDs.</li> </ul>
--------------------------	---

<b>Option 2</b>	<i>See Option 2 in 'Specific Objective' table above</i>	
	Qualitative description	Quantitative description
<i>Benefits</i>	The additional reconciliation would limit the risks of inflation/deletion of securities, as it would ensure a more thorough process.	
<i>Costs to regulator:</i>	There would be no specific costs to the regulator.	There would be no specific costs to the regulator.
<i>Compliance costs:</i>	All but one of the CSDs who were part of the nine CSD questionnaires would need to adapt existing reconciliation procedures to provide for the extra reconciliation proposed.	In addition to the costs generated by Option 1 for physical securities, additional costs for Option 2's extra reconciliation are estimated by CSDs to range from EUR 32K to over EUR 600K for each single CSD. The overall compliance cost is likely to be higher than for Option 1.

## THE SPECIFIC CASE OF CORPORATE ACTIONS

### 2.9.2 How can the CSDR technical standards ensure CSDs have the necessary controls and procedures in place to protect the integrity of the issue and to protect market participants and investors from the consequences of securities inflation or deletion in the specific case of corporate actions?

<b>Specific Objective</b>	Ensure CSDs have the necessary procedures and controls to protect the integrity of the issue to help protect market participants and investors from the consequences of securities inflation or deletion specifically in the case of corporate actions
Option 1	Propose additional reconciliation measures for corporate actions
Option 2	Do not propose any additional reconciliation measures for corporate actions.
Preferred Option	<b>Option 1</b> - it would ensure that corporate actions are accurately reflected, and moreover market practices already ensure that corporate actions are applied on reconciled positions.

### *Impact of the proposed policies*

<b>Option 1</b>	<i>See Option 1 in 'Specific Objective' table above</i>
	Description

<i>Benefits</i>	This option would bring additional security to the processing of corporate actions and would reduce the risks of errors.
<i>Costs to regulator:</i>	There would be no obvious costs to regulators.
<i>Compliance costs:</i>	Additional reconciliation measures would have an increased compliance cost for CSDs, higher than for option 2. This will be an on-going cost as reconciliations are carried out on a daily basis.

<b>Option 2</b>	<i>See Option 2 in 'Specific Objective' table above</i>
	Description
<i>Benefits</i>	The benefit would be the amount saved by not conducting additional reconciliations for corporate actions.
<i>Compliance costs:</i>	No additional compliance costs.

## EXTERNAL RECONCILIATIONS

### 2.9.3 How can the CSDR technical standards ensure CSDs have the necessary controls and procedures in place to protect the integrity of the issue and to protect market participants and investors from the consequences of securities inflation or deletion in case other entities are involved in the reconciliation process?

<b>Specific Objective</b>	Provide for CSDs to have the necessary procedures and controls to protect the integrity of the issue to help protect market participants and investors from the consequences of securities inflation or deletion in case other entities are involved in the reconciliation process.
Option 1	Require CSDs to have in place: <ul style="list-style-type: none"> <li>- A daily reconciliation of the total balance recorded on the securities accounts maintained by the CSD with the corresponding records of securities maintained by the relevant entity</li> <li>- An end of day reconciliation of the balance of each securities account maintained by the CSD where the securities have been transferred during a given business day, with the balance of the corresponding record of securities maintained by the relevant entity where the securities have been transferred during that business day</li> </ul>
Option 2	Require CSDs to have in place specific reconciliation measures depending on the entities involved in the reconciliation process (e.g. registrars, transfer agents, common depositories, CSD participants).
Preferred Option	<b>Option 2</b> - it would ensure that the reconciliation measures are tailored depending on the role of the other entities involved in the reconciliation process.

### *Impact of the proposed policies*



<b>Option 1</b>	<i>See Option 1 in 'Specific Objective' table above</i>
	Description
<i>Benefits</i>	The measures would ensure that reconciliation measures cover both stock and flows.
<i>Compliance costs:</i>	The costs should be similar to Option 2.

<b>Option 2</b>	<i>See Option 2 in 'Specific Objective' table above</i>
	Description
<i>Benefits</i>	This option would ensure that the reconciliation measures are tailored depending on the role of the other entities involved in the reconciliation process.
<i>Compliance costs:</i>	The costs should be similar to Option 1.

## RECONCILIATION PROBLEMS

### ***Suspension of settlement in a securities issue when undue creation or deletion of securities is detected***

<b>Specific Objective</b>	Ensure that reconciliation problems are solved as soon as possible, and that detrimental effects for the integrity of the issue are contained
Option 1	A CSD should analyse any mismatches and inconsistencies resulting from the reconciliation process and endeavour to solve them before the beginning of settlement on the following business day. Where the reconciliation process reveals an undue creation or deletion of securities, and the CSD fails to solve this problem till the end of the following business day, the CSD should suspend the securities issue for settlement until the undue creation or deletion of securities has been remedied.
Option 2	CSDs should have more flexibility regarding the suspension of settlement in case of reconciliation problems, under the control of the competent authority, and based on certain predefined thresholds.
Preferred Option	<b>Option 1</b> for the reasons explained in the cost and benefit section below.

### ***Impact of the proposed policies***

<b>Option 1</b>	<i>See Option 1 in 'Specific Objective' table above</i>
-----------------	---

	Description
<i>Benefits</i>	This option would ensure a higher degree of harmonisation, it would act as an incentive for CSDs to solve the reconciliation problems as quickly as possible and it would ensure that CSDs maintains correct records on the securities issued. The suspension of settlement would only apply in the case of severe reconciliation problems, in order to avoid the propagation of the errors through the holding chain. This option would ring-fence any breaks and would contain the risk to ensure that a serious discrepancy does not become unmanageable and the breaks become further blurred by new activity, especially in periods of market or participant stress.
<i>Costs to the regulator</i>	This option would have lower costs for the competent authorities than Option 2, though the competent authorities would need to monitor the cases when settlement is suspended.
<i>Compliance costs:</i>	The costs for the CSDs and the other entities involved in the reconciliation process may be higher than for Option 2, but only for those CSDs that experience severe reconciliation problems.
<i>Indirect costs</i>	This option may have costs for market participants that would be affected by the suspension of settlement. At the same time, it may also save costs for market participants and issuers, that may otherwise have been caused by the possible propagation of errors and discrepancies that would then need to be rectified.

<b>Option 2</b>	<i>See Option 2 in 'Specific Objective' table above</i>
	Description
<i>Benefits</i>	This option would allow for more flexibility. It may avoid potential market disruption leading to more settlement fails, though the propagation of reconciliation errors and discrepancies may also lead to market disruption and may have systemic effects.
<i>Costs to the regulator</i>	This option would have higher costs for the competent authorities than Option 1, given that they would need to monitor the application of the measures by the CSDs, and assess the discretionary decisions made by the CSDs.
<i>Compliance costs:</i>	The costs for the CSDs and the other entities involved in the reconciliation process may be lower than for Option 2, though this option also entails costs as the CSDs would need to monitor the reconciliation problems and decide on the measures to take.
<i>Indirect costs</i>	This option may have costs for market participants and issuers due to the possible propagation of errors and discrepancies that would then need to be rectified.

## 2.10 Operational Risk (Article 45 CSDR)

## **CSD OPERATIONAL RISK**

To address the below questions, ESMA considered the research it had conducted on the market (CPSS-IOSCO disclosure frameworks, answers to the external consultant's questionnaire) to establish the common position of CSDs and what options would be most appropriate for the technical standards. The following information breaks down the findings of the research and analysis.

All CSDs included in the data seem to have a business continuity policy (BCP) similar to the proposed ESMA requirements. BCPs are regularly tested by CSDs. From the 31 CSD respondents on operational risk, the wide majority (28 CSDs) run tests on their BCP at least once a year in similar ways to the ESMA requirements

Of the remaining 3 CSDs:

- 1 CSD runs tests on its BCP at random intervals, without further information
- 1 CSD runs tests on its BCP when systems are updated, without further information
- 1 CSD runs tests on its BCP regularly, without further information

6 CSDs confirmed they had been required to activate their disaster recovery plan in the previous 3 years. All but one of these found they experienced a recovery time of between 1 and 4 hours, and one found its recovery time to take 8-24 hours.

Only one CSD did not provide information on recovery times. Test results provide the following evidence on recovery times for critical functions:

- 16 CSDs follow recovery time of 2 hours or less, compatible with the ESMA proposed requirements
- 11 CSDs indicated that their recovery time ranged from 1 to 4 hours
- 2 CSDs indicated that their recovery time is 4 hours
- 1 CSD indicated that its recovery time is between 4 and 8 hours.

Out of 31 CSDs, the wide majority (27 CSDs) have a secondary processing site:

- 12 CSDs have at least one secondary business site and one secondary processing site, with business and processing sites being different sites
- 9 CSDs have secondary business and processing facilities, with no publicly available information on whether or not business and processing are on the same site
- 6 CSDs have one secondary site which regroups business and processing services

Of the remaining CSDs:

- 1 has a secondary processing site (mirroring the main processing site) but no information is publicly available on whether or not this site can support business operations
- 2 CSDs only have a secondary processing site

A cost analysis was carried out on the additional cost that would be incurred by CSDs in case they were required to have a secondary site in place (if they currently only had one site). The cost analysis was based on the following assumptions:

- the cost to maintain an additional back-up site (available on demand) as part of a BCP is estimated at EUR 3,000 per annum per critical employee with comprehensive workstations and an IT connection to the main site.
- It is important to note that this back-up facility does not belong to the financial institution; it is kept at its disposal in case of need by a company which offers that kind of service.

- It is assumed that the site would be ready to function and fully equipped, and potentially mutualised. In addition the overall population considered to be critical to maintain the activity was estimated based on a conservative estimate of 40% of staff, while BCPs usually consider 15-20% to be critical.

Based on this, the aggregated cost of having an additional site for all CSDs involved in the sample would amount to EUR 1,548,000 per annum per CSD.

Costs in the event of the BCP being activated (price per position per day) were excluded. Project costs were also excluded as they rely upon a starting point and an existing BCP.

## RESOURCES FOR MANAGING OPERATIONAL RISK

### 2.10.1 How can the CSDR technical standards ensure CSDs have the appropriate resources in place to manage operational risk?

<b>Specific Objective</b>	To ensure that a CSD has appropriately resourced operational risk management function.
Option 1	The operational risk management function should be separate and these individuals are not allowed to undertake any other tasks at the CSD.
Option 2	The operational risk management function may share staff with other functions of the CSD, provided that any conflicts of interest are adequately considered and addressed. (In line with Article 26 CSDR and RTS)
Preferred Option	<b>Option 2.</b> This is a more proportionate approach and will ensure that CSDs are able to function effectively, addressing the importance of operational risk whilst ensuring they do so without creating conflicts of interest.

#### *Impact of the proposed policies*

<b>Option 1</b>	<i>See Option 1 in 'Specific Objective' table above</i>
	Description
<i>Benefits</i>	Ensures an operational risk function that is purely focused on risk management from an operational perspective, without the risk of distractions coming from other responsibilities.
<i>Compliance costs:</i>	This option will involve higher compliance costs for the CSDs than Option 2 due to the requirement for individuals to be solely tasked with the responsibilities of operational risk management.

<b>Option 2</b>	<i>See Option 2 in 'Specific Objective' table above</i>
<i>Benefits</i>	This will ensure that the CSD has an appropriately staffed operational risk function while allowing for flexibility in terms of resource sharing, provided that potential conflicts of interests are adequately managed.
<i>Compliance costs:</i>	This option will have lower compliance costs than Option 1.

## RECOVERY TIME FOR A CSD'S SYSTEMS IN THE EVENT OF A DISRUPTION

## 2.10.2 How can the CSDR technical standards ensure CSDs have rapid and effective recoveries following events that cause disruptions?

<b>Specific Objective</b>	To ensure that critical IT systems can promptly resume operations from the time of disruption
Option 1	An exact time limit for the recovery of services for all systems
Option 2	An exact time limit for the recovery of critical IT systems only (in line with the CPSS-IOSCO PFMI)
Option 3	Flexible recovery time (discretion of the CSD) with a recovery time objective of no more than two hours for each critical function.
Preferred Option	<b>Option 3</b> allows for CSDs to determine appropriate recovery time objectives that are within a two hour time limit, ensuring critical functions are promptly recovered.

### *Impact of the proposed policies*

<b>Option 1</b>	<i>See Option 1 in 'Specific Objective' table above</i>
	Description
<i>Benefits</i>	This will ensure that there is a consistently rapid and effective response time that is proportionate to the CSD's responsibilities and the functions it carries out in the market
<i>Compliance costs:</i>	The compliance costs will depend upon the length of time that is agreed as the appropriate timescale for ensuring recovery. The shorter this timeframe, the larger the compliance costs. It will be a cost on an ad hoc basis, when there is a disaster incident warranting a recovery.
<i>Costs to other stakeholders</i>	Other stakeholders affected by the failure of the CSD experience detriment if they are unable to use the CSD services. Depending upon the length of time decided for disaster recovery, there will be varying degrees of costs for those parties.

<b>Option 2</b>	<i>See Option 2 in 'Specific Objective' table above</i>
	Description
<i>Benefits</i>	This option would allow for a faster recovery as it is focused upon the critical functions of the CSD in line with the PFMI.
<i>Compliance costs:</i>	Compliance costs will be smaller than for a requirement such as in Option 1 where a complete recovery is expected, as this option is focused on a quick recovery of the critical IT systems only. The compliance costs will however be higher than for Option 3.
<i>Costs to other stakeholders</i>	Other stakeholders affected by the failure of the CSD experience detriment if they are unable to use the CSD services. Depending upon the length of time decided for disaster recovery, there will be varying degrees of costs for those parties.

<b>Option 3</b>	<i>See Option 3 in 'Specific Objective' table above</i>
	Description
<i>Benefits</i>	Allows a CSD to focus resource on other areas when it suffers a disaster requiring a recovery exercise. The two hour window is in line with the PFMLs, and it ensures critical functions are recovered in a short timeframe, whereas less critical functions can be deprioritised accordingly.
<i>Compliance costs:</i>	The compliance costs related to this option would be lower than for Options 1 and 2.
<i>Costs to other stakeholders</i>	Other stakeholders affected by the failure of the CSD experience detriment if they are unable to use the CSD services. Depending upon the length of time decided for disaster recovery, there will be varying degrees of costs for those parties.

## SECONDARY SITES

### 2.10.3 How can the technical standards ensure that CSDs ensure the preservation of their services, the timely recovery of operations and the fulfilment of their obligations in the case of events that pose a significant risk of disrupting operations?

<b>Specific Objective</b>	Ensure the preservation of the CSD's 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
Option 1	A CSD shall maintain at least a secondary processing site with sufficient resources, capabilities, functionalities and staffing arrangements, which are adequate to the CSD's operational needs and risks that the CSD faces in order to ensure continuity of critical operations, at least in case the main location of business is not available.
Option 2	A CSD should have two secondary processing sites
Preferred Option	<b>Option 1</b> - it would meet the standard set in CSDR and it would be less costly than Option 2.

#### **Impact of the proposed policies**

<b>Option 1</b>	<i>See Option 1 in 'Specific Objective' table above</i>
	Description
<i>Benefits</i>	Easier and less costly solution to implement for CSDs, which would meet the standard set in CSDR.
<i>Indirect costs</i>	CSDs with 2 secondary sites (hence more security) could decide to keep only one, thus lowering security.

<b>Option 2</b>	<i>See Option 2 in 'Specific Objective' table above</i>
	Description

<i>Benefits</i>	Increased safety	
<i>Compliance costs:</i>	19 CSDs would need to adapt to ESMA's proposal. More costly than Option 1.	On-going costs would amount to EUR 1,548K per annum.

## FREQUENCY OF AUDIT ON A CSD'S IT SYSTEMS AND INFORMATION SECURITY FRAMEWORK

### 2.10.4 How can the CSDR technical standards ensure a CSD reviews its information technology systems and information security frameworks on a regular basis?

<b>Specific Objective</b>	To ensure that a CSD reviews its information technology systems and information security framework at appropriate intervals
Option 1	The IT systems and the information security framework in relation to the CSD core services shall be reviewed at least annually. They shall be subject to independent audit assessments. The results of such assessments shall be reported to the CSD's management body and to the competent authority.
Option 2	Less frequently than once a year
Preferred Option	<b>Option 1</b> - this option ensures a consistent approach to auditing IT systems and information security frameworks which will align with EMIR and result in a more robust CSD infrastructure.

#### **Impact of the proposed policies**

<b>Option 1</b>	<i>See Option 1 in 'Specific Objective' table above</i>
	Description
<i>Benefits</i>	This option will ensure that any updates are soon reviewed as part of the audit process and the CSD's management body and competent authority can be reasonably confident with the standards of the IT system and security provisions.
<i>Compliance costs:</i>	The compliance cost related to this option is higher than option two as there is a requirement for audit resource to be focused on IT and security frameworks on a more regular basis. It will be an ongoing cost to the CSD.

<b>Option 2</b>	<i>See Option 2 in 'Specific Objective' table above</i>
<i>Benefits</i>	Conducts audits, but without a regular timeframe. Allows the audit function to potentially focus on different areas of the CSD depending on the identified needs.
<i>Costs to regulator:</i>	There are no costs related to the regulator. There is potentially a cost related to the audit function not acting effectively and the regulator being required to intervene in instances where there is detriment that would not have been picked up had audits been more frequent.
<i>Compliance costs:</i>	The compliance costs related to this option would depend on the frequency of audits, and would certainly be lower than for option one.

<i>Indirect costs</i>	Indirect costs may arise for other stakeholders if the frequency of the audit was affecting the standard of a CSDs IT services and security systems. Without a regular check there is a risk that issues will arise which could have detrimental impacts upon the users of CSD services.
-----------------------	--

## 2.11 CSD Investment Policy (Article 46 CSDR)

Based on the available data (that which was collected by the external consultant by analysing the CSDs' annual reports and the CSDs' responses to an external questionnaire), the majority of CSDs maintain their assets in cash (11 CSDs have 100% of their assets in cash, 18 have more than 50% in cash and only six in financial instruments). Two CSDs amongst respondents to the questionnaire have more than 98% of their assets in financial instruments and one has more than 70%.

CSD cash is held in three different ways:

- Current bank account: only a few CSDs keep relevant cash volumes in their current bank accounts
- Term deposit: this is the most frequent approach taken by CSDs
- Reverse repo: only one CSD indicating it strongly invests in reverse repos

The majority of CSDs that invest in financial instruments invest in government bonds - and not in corporate bonds or in units of investment funds. Similarly to the way cash is held, different instruments have different risk profiles.

Sovereign debt is usually highly liquid, although it may have different credit, or liquidity risk levels depending on the issuer and the maturity of the bonds. Only one CSD seems to invest in 2y+ maturities.

One CSD invests 98% of its assets in the following securities:

- money market funds;
- treasury bills and bonds of its country of incorporation and activity;
- fixed-term deposits at commercial banks.

As regards derivatives, only six of the CSDs that took part in the survey use them. These CSDs suggest that derivatives are used for hedging purposes only. This is to hedge against interest rate risk and currency risk. The latter regards multicurrency CSDs.

Three CSDs indicated that they use FX derivatives to hedge their future income streams in currency and one indicated exposures to six different currencies, from EUR 10 bn to EUR 70 bn and in the case of one currency, almost EUR 300 bn.

One CSD stated that it has been entering into interest rate derivatives in order to hedge its exposure to interest rate risks. The table below demonstrates the asset mix of a number of CSDs.

CSD	Cash %	Financial Assets %
A	100	-



B	100	-
C	100	-
D	100	-
E	100	-
F	100	-
G	100	-
H	100	-
I	100	-
J	100	-
K	100	-
L	98.6	1.5
M	90.0	10.0
N	81.2	18.9
O	67.3	25.7
P	63.8	36.2
Q	62.8	37.2
R	56.3	43.7
S	2.0	98.0

Table created by external consultant

With regard to maturity, 15 CSDs invest in instruments maturing in less than 2 years and only one in instruments beyond a 2 year maturity.

**Timeframe for access to assets**

CSD	Confirmed timeframe to access 100% of assets	Estimation of assets accessible within hours
CSD 9	Immediately	-
CSD 17	Immediately	-
CSD 20	Within 3 hours	-
CSD 22	Within hours	-
CSD 6	Same day	-
CSD 1	Same day	-
CSD 4	Promptly	-
CSD 23	Promptly	-
CSD 18	Within 1-2 days	-
CSD 5	Within 2 days	-
CSD 7	Within hours	-
CSD 10	Within hours	-
CSD 13		90%
CSD 8		52%
CSD15		48.15%
CSD 2		40.00%
CSD 11		3.60%
CSD 21		2.00%
CSD 12		1.00%
CSD 19		0.20%
CSD 14		0.00%

CSD 3		0.00%
CSD 16		

Table created by the external consultant

Among the 31 CSDs considered:

- For 12 CSDs, 100% of assets could be rapidly accessible:
  - o For 6 CSDs, 100% of assets would be accessible within hours – including two CSDs for which 100% of assets is placed on current accounts at banks, deemed accessible immediately for the purpose of the analysis
  - o For 6 CSDs, 100% of assets would be accessible on the same day
- For 4 additional CSDs, 100% of assets would be accessible either promptly or within 1 or 2 business days
- For 1 additional CSD 90% of assets are deemed to be accessible immediately (current accounts at banks)
- For the 14 remaining CSDs, the timeframe to access 100% assets cannot be estimated
  - o For 3 of these CSDs over 40% of assets held on current accounts at banks, are deemed immediately accessible

In terms of accessibility of the assets, the following aspects should be considered:

- Assets held in current accounts at banks are deemed immediately accessible
- Local financial instruments held by the CSD itself are by generally accessible immediately;
- Foreign financial instruments are usually held through CSD links. In this particular case, direct links should allow for a more immediate access to assets;
- Bank term deposits (which are widely used by some CSDs) highly depend on the terms of the underlying contract with the financial institution, with some deposits less easily accessible.

### Concentration limits

CSD	Application of concentration limits	Description
CSD 2	Yes	No more than 25% in a given credit institution
CSD 10	Yes	Defined at group level
CSD 20	Yes	By country, counterparty, group of counterparties
CSD 3	Yes	Defined at group level
CSD 5	Yes	Defined at group level
CSD 6	Yes	Defined at group level
CSD 14	Yes	No more than 2/3 in a given credit institution
CSD 18	Yes	In case of unsecured investments: cash deposits held with counterparties other than the local central bank, debt instruments not issued or not guaranteed by the State Treasury, debt instruments not issued by the local central bank
CSD 4	No	
CSD 23	No	
CSD 8	No	In practice cash split between various institutions, although no formal policy applied
CSD 17	No	

CSD 1	NONE	100% of cash deposited at one bank
CSD 11	N/C	
CSD 19	N/C	
CSD 22	N/C	
CSD 13	N/C	
CSD 7	N/C	
CSD 9	N/C	

Table created by the external consultant

Among the CSDs consulted on concentration limits:

- 7 CSDs confirmed their use of concentration limits: existence of a policy and constant monitoring
- 5 CSDs confirmed the absence of concentration limits
- For 6 CSDs, all investments are in cash, deposited at one bank well-rated
- 8 CSDs did not provide the information

## HIGHLY LIQUID CSD ASSETS WITH MINIMAL MARKET AND CREDIT RISK

### 2.11.1 How can CSDs' assets be maintained as highly liquid with minimal market and credit risk?

<b>Specific Objective</b>	Keep CSDs' assets highly liquid and with minimal market and credit risk.
Option 1	<p>Allow a CSD to invest in financial instruments if:</p> <p>(a) they are issued or guaranteed by:</p> <ul style="list-style-type: none"> <li>(i) a government;</li> <li>(ii) a central bank;</li> <li>(iii) a multilateral development bank as listed under Article 117 of Regulation (EU) No 575/2013;</li> <li>(iv) the European Financial Stability Facility or the European Stability Mechanism;</li> </ul> <p>(b) the CSD can demonstrate to the competent authority that the financial instruments have low credit and market risk based upon an internal assessment by the CSD. In performing such an assessment the CSD shall employ a defined and objective methodology that shall not exclusively rely on external opinions and that takes into consideration the risk arising from the establishment of the issuer in a particular country;</p> <p>(c) they are denominated in any of the following currencies:</p> <ul style="list-style-type: none"> <li>(i) a currency in which transactions are settled in the securities settlement system operated by the CSD;</li> <li>(ii) any other currency the risks of which the CSD is able to manage.</li> </ul>

	<p>(d) they are freely transferable and without any regulatory constraint or third party claims that impair liquidation;</p> <p>(e) they have an active outright sale or repurchase market, with a diverse group of buyers and sellers, including in stressed conditions, and to which the CSD has reliable access;</p> <p>(f) reliable price data on these instruments are publicly available on a regular basis;</p> <p>In addition, no derivatives should be used.</p>
Option 2	<p>Same as Option 1, but allowing limited use of derivatives under the following conditions:</p> <p>(a) they are entered into for the purpose of hedging currency risk arising from the settlement in more than one currency in the securities settlement system operated by the CSD or interest rate risk that may affect CSD assets and, in both cases, qualify as a hedging contract pursuant to International Financial Reporting Standards (IFRS) adopted in accordance with Article 3 of Regulation (EC) No 1606/2002;</p> <p>(b) reliable price data is published on a regular basis for those derivative contracts;</p> <p>(c) they are concluded for the specific period of time necessary to reduce the currency or interest rate risk to which the CSD is exposed.</p>
Preferred option	<b>Option 2</b> appears to be the preferred to ensure highly liquid investments, and limited exposures to derivatives in well-defined circumstances.

### **Impact of the proposed policies**

<b>Option 1</b>	<i>See Option 1 in 'Specific Objective' table above</i>
	Qualitative description
<i>Benefits</i>	This option would ensure that CSDs only invest in financial instruments that have low credit and market risk.
<i>Compliance costs:</i>	<p>CSDs would need to review their portfolio of investments, notably on derivatives.</p> <p>Compliance costs could be significant related to the impossibility to hedge currency risk and interest rate risk, which would increase the risks for CSDs managing deposits and settlements in multiple currencies.</p> <p>In addition, replacing the current portfolio of investments would involve possible transaction costs.</p>
<i>Indirect costs</i>	CSDs will not be able to hedge their exposures to currency risk and interest rate risk.

<b>Option 2</b>	<i>See Option 2 in 'Specific Objective' table above</i>
	Description
<i>Benefits</i>	The benefits would be similar to Option 1. In addition, Option 2 would allow a better management of risks for CSDs enabling them to hedge currency risk and interest rate risk.
<i>Compliance costs:</i>	Compliance costs would be reduced as compared to Option 1

## APPROPRIATE TIMEFRAME FOR ACCESS TO ASSETS

### 2.11.2 How can the CSDR technical standards ensure CSDs have prompt access to their assets?

<b>Specific Objective</b>	Ensure prompt access by the CSD to its assets
Option 1	Require that: (a) a CSD that holds cash assets shall have immediate and unconditional access to such assets; (b) a CSD that holds financial instruments shall be capable of accessing them on the same business day when a decision to liquidate such financial instruments is taken
Option 2	Require that a minimal percentage of assets (to be defined) should be accessible on the same day, while access to the remaining assets may take place during a longer timeframe.
Preferred option	<b>Option 1</b> - this would ensure that the CSD has prompt access to financial instruments on the same business day when a decision to liquidate such financial instruments is taken, and immediate access to cash.

### **Impact of the proposed policies**

<b>Option 1</b>	<i>See Option 1 in 'Specific Objective' table above</i>
	Description
<i>Benefits</i>	This option would ensure prompt access to its assets by a CSD.
<i>Compliance costs:</i>	Consideration may need to be given to some types of assets held by the CSD where accessibility and liquidation may take a longer time. These assets would not be appropriate CSD investments and so should not be invested in. The cost of liquidating the assets may not be significant, but could be higher in case some securities were not liquid enough (or could not be put in repurchase agreements for a certain period of time), or depending on the closing conditions on term deposits.
<i>Indirect costs</i>	More limited pool of assets to invest in (highly liquid ones only) Reduced profitability of investments given the lower yields on high quality instruments.

<b>Option 2</b>	<i>See Option 2 in 'Specific Objective' table above</i>
-----------------	---

	Description
<i>Benefits</i>	This option would allow for greater flexibility in terms of the assets that a CSD may invest in.
<i>Compliance costs:</i>	This proposal will have lower costs than Option 1 as it would give, depending on the actual percentage, more flexibility to CSDs in their investment policy. CSDs may still need to adjust their investment policy, but to a lesser extent than for Option 1.
<i>Indirect costs</i>	Although not to the same extent as for Option 1 (due to the extra flexibility) - more limited pool of assets to invest in (highly liquid ones only) Reduced profitability of investments given the lower yields on high quality instruments.

## CONCENTRATION LIMITS

### 2.11.3 How can the CSDR technical standards ensure that a CSD's overall risk exposure to any individual authorised credit institution or authorised CSD with which it holds its financial assets remains within acceptable concentration limits?

<b>Specific Objective</b>	Ensure that a CSD's overall risk exposure to any individual authorised credit institution or authorised CSD with which it holds its financial assets remains within acceptable concentration limits
Option 1	<ul style="list-style-type: none"> <li>- Establish and implement policies and procedures to ensure that exposures to institutions will remain within acceptable concentration limits by applying sufficient diversification requirements.</li> <li>- 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</li> <li>- If and when concentration limits are surpassed, the CSD should take appropriate measures to bring the exposures within the limits, without any delay</li> </ul>
Option 2	<p>Same as option 1, with the following detailed obligations:</p> <ul style="list-style-type: none"> <li>- A CSD shall hold its financial assets in diversified authorised credit institutions or authorised CSDs</li> <li>- When considering these entities, the CSD shall take into account: <ul style="list-style-type: none"> <li>• their geographic distribution</li> <li>• interdependencies and multiple relationships that those entity or entities of the same group may have with the CSD</li> <li>• the level of credit risk of the entity holding the financial assets.</li> </ul> </li> </ul>
Preferred option	<p>Option 1 would meet the objective, yet without prescribing more details it may not ensure consistency across the EU, and may possibly lead to different interpretations of the requirements;</p> <p><b>Option 2</b> is preferred as it meets the objective more appropriately</p>

while ensuring consistency of application across the EU.
--

**Impact of the proposed policies**

<b>Option 1</b>	<i>See Option 1 in 'Specific Objective' table above</i>
	Description
<i>Benefits</i>	This option would allow a strong diversification of the risks.
<i>Compliance costs:</i>	This option will involve definition of concentration limit policies, and active monitoring with additional costs in this respect.

<b>Option 2</b>	<i>See Option 2 in 'Specific Objective' table above</i>
	Description
<i>Benefits</i>	This option would ensure a more consistent and harmonised approach across the EU.
<i>Compliance costs:</i>	This option may require some CSDs to change some of the entities with which they hold their assets, in order to ensure that they meet the requirements.

## 2.12 CSD Links (Article 48 CSDR)

Data was collected by reviewing ECSDA information on CSD links amongst members and also using the external consultant's analysis. Additionally, the CPSS-IOSCO disclosure frameworks were used.

### EXISTING CSD LINKS

The analysis is based on an ECSDA study on 25 CSDs.

In 2013, those 25 CSDs had links with other CSDs across the EU, for a total of 164 links (excluding relayed links). Four CSDs have links to just one other CSD. One CSD has links to 16 other CSDs; the remainder have links to numbers that vary between one and 16 CSDs.

In terms of methodology of the analysis conducted:

- The analysis only considered outbound links. This avoided any double-counting of the links
- The level of activity of these links is unknown – some of the links may be inactive
- The links may be DvP, FoP only, or both DvP and FoP. In the study which was used, the existence of both DvP and FoP processes between 2 CSDs for an outbound link is not considered separately, but as one single link.

In 2013, ECSDA noted that:

- there had been an 8% increase in the average number of CSD links per CSD since 2008;
- DvP links tend to be more numerous, as compared to FoP only links

It should also be considered that a significant number of new CSD links will be implemented with the implementation of T2S, as confirmed by various CSDs.

### **Typology of CSD links**

#### *Standard vs customised links*

This notion does not correspond to a standard definition, also due to the absence of data on the topic.

Applications by CSDs are of 2 kinds:

- **Standard agreements**, corresponding to usual terms and conditions applying to the participant of an issuer CSD;
- **Specific (or customised) agreements**, although the level of specificity of these agreements is not publicly available. Examples of the customisation of the CSD links mentioned tend to be operational: communication standards such as the use of ISO standards, specific reporting, or processes related to local specificities. Yet such specificities do not imply specific services when compared to other participants.

One stakeholder who responded to the questionnaire noted that CSDs may (with the same CSD) have both a specific agreement, and a regular agreement based on standard participation terms and conditions applying to all participants.

#### *Interoperable links*

An Interoperable link as defined by the CSDR is “a CSD link whereby the CSDs agree to establish mutual technical solutions for settlement in the securities settlement systems that they operate”.

Today, only the link between two ICSDs seems to qualify for such a definition. This link is also known as the “Bridge”.

#### *Direct vs indirect links*

CSD	Direct		Total direct	Indirect		Total indirect	Total
	DvP	FoP		DvP	FoP		
CSD 1	16	0	16	9	0	9	25
CSD 2	15	1	16	5	0	5	21
CSD 3	0	8	8	0	7	7	15
CSD 4	7	4	11	0	0	0	11
CSD 5	7	2	9	0	1	1	10
CSD 6	0	9	9	0	1	1	10



CSD 7	10	0	10	0	0	0	10
CSD 8	7	2	9	0	0	0	9
CSD 9	0	1	1	0	7	7	8
CSD 10	2	4	6	0	0	0	6
CSD 11	0	3	3	2	0	2	5
CSD 12	2	3	5	0	0	0	5
CSD 13	0	0	0	0	4	4	4
CSD 14	1	1	2	2	0	2	4
CSD 15	2	1	3	0	0	0	3
CSD 16	3	0	3	0	0	0	3
CSD 17	3	0	3	0	0	0	3
CSD 18	1	1	2	0	0	0	2
CSD 19	1	0	1	1	0	1	2
CSD 20	1	1	2	0	0	0	2
CSD 21	0	2	2	0	0	0	2
CSD 22	0	0	0	1	0	1	1
CSD 23	1	0	1	0	0	0	1
CSD 24	0	2	2	0	0	0	2
CSD 25	0	1	1	0	0	0	1
<b>TOTAL</b>	<b>79</b>	<b>45</b>	<b>124</b>	<b>20</b>	<b>20</b>	<b>40</b>	<b>164</b>

Table prepared by the external consultant

#### Direct links

The information above shows that direct links appear to be more numerous: 124 vs. 40. This excludes relayed links where access to a CSD gives access to other CSDs, as is the case when CSDs have an account at an ICSD, which allows them to settle domestic securities issued outside of the ICSD.

- Direct links are for a slight majority held by the ICSDs and CSDs who have a banking license. In this case, the links are for the vast majority DvP links (56 vs. 7);
- A slightly lower number are held by non-bank CSDs. In this particular case, FoP links are more significant (38 vs. 23). Yet it should be noted that a significant number of direct DvP links were implemented by non-bank CSDs, which represents a higher risk. For CSDs who displayed the information, it appears that the risks incurred are covered by ensuring no credit is made while processing the settlement (either of securities or cash).

Direct links are largely not intermediated. However some cases exist where the CSD uses the services of a custodian as operator ('operated direct links').

The use of an operator is frequent on certain markets. Main characteristics are:

- The investor CSD has an account in its name at the issuer CSD;
- The CSD does not process instructions itself to the CSD, but through the operator;
- The cash settlement can be operated through an account in the name of the CSD or through an account in the name of the operator.

These services can be considered as an outsourcing of the access to the market by the investor CSD, implying operational risks to be managed through a dedicated service level agreement (SLA).

#### *Indirect links*

- Only a limited number of CSDs use this kind of link (11 out of the 25 sampled). Among those, 5 CSDs account for 32 of the 40 indirect links;
- 8 non-bank CSDs use this kind of link, which bear a higher risk compared to a FoP link.

In the case of indirect links, banks participating in the CSD are used as sub-custodians (the case of middle CSDs being excluded as relayed links are excluded from this study).

### **TIME FOR IMPLEMENTING A CSD LINK**

Implementing a CSD link is the result of a risk and operational analysis conducted by CSDs. CSDs do not use criteria different from those criteria used for a regular participant. The following considerations are made:

- Determining the type of link (direct vs indirect, DvP vs FoP) (there is no indication that suggests the practicality of implementing DvP links is impossible);
- Determining the appropriate way to operate instructions transiting through the links and select an intermediary (for indirect links), the need for an operator (for direct links), or the possibility to operate directly (for direct links);
- Adjust processes and applications accordingly, including communication standards, reporting and reconciliation;
- Determining the level of risks implied.

Implementing a CSD link can take from 3 to 24 months, with substantive differences that appear to be in relation to the size of the investor CSD:

- It takes three to nine months for small size CSDs to implement a CSD link, from the initial assessment to actual implementation;
- It takes six to 24 months for large and very large size CSDs.

Two reasons were given to account for the variation in the time lapses; first, managing local regulation and legal framework requirements when implementing cross border relationships, particularly around the ownership of securities, and second the required IT developments.

No CSD mentioned the risk assessment process as a factor in the timing of the implementation, or the selection of an intermediary or operator as something which caused time delays.

### **RISKS CONSIDERED WHEN IMPLEMENTING A CSD LINK**

Generally speaking, CSDs confirm they subscribe to 3 sets of principles:

1. The rules imposed by CPSS-IOSCO as regards relations with other financial market infrastructures, as set in Principle 20. These rules notably consider that:
  - “an FMI should identify, monitor, and manage all potential sources of risk arising from the link arrangement”
  - “A link should have a well-founded legal basis”
  - “Linked CSDs should measure, monitor, and manage the credit and liquidity risks arising from each other”
  
2. The rules imposed by the ECB as regards links eligible to its credit operations, and the assessment it requires from the concerned SSSs on the following aspects:
  - legal soundness
  - settlement in central bank money
  - custody risk
  - regulation and/or control by competent authorities
  - transparency of risks and conditions for participation in a system
  - risk management procedures
  - intraday finality of settlement
  - operating hours and days
  - operational reliability of technical systems and availability of adequate backup facilities
  
3. The guidelines proposed by ECSDA (together with EACH and FESE) - Access and Interoperability Guideline - 28 June 2007

More specifically, in relation to ESMA’s proposal as regards the protection of the linked CSDs, the study below looks at 2 different aspects, although publicly available information does not always make a difference, which also reflects the fact that they tend to have consistent procedures in both cases:

- The set-up of outbound CSD links;
- The set-up of inbound CSD links.

*Risks considered in the set-up of outbound links*

Information was gathered for 19 CSDs, 5 of which have a banking license. Information provided is usually undetailed, although some specifics are available. It should be noted that apart from the case of the ICSDs, little reference is made to differences related to categories of links (DvP vs FoP, standard vs customised, direct vs indirect). Information provided usually covers all categories, including the specificities of each category.

CSD	Types of risks considered before entering a link arrangement		
	Legal risks	Operational risks	Financial risks
CSD 1	Yes	Yes	Yes
CSD 2	Yes	Yes	Yes
CSD 3	Yes	Yes	Yes
CSD 4	Yes	Yes	Yes

CSD 5	Yes	Yes	Yes
CSD 6	Yes	Yes	
CSD 7	Not specified	Yes	Yes
CSD 8	Yes	Yes	
CSD 9	Yes	Yes	
CSD 10	Yes	Yes	
CSD 11	CPSS-IOSCO & ECB principles	Yes	CPSS-IOSCO & ECB principles
CSD 12	Yes	Yes	
CSD 13	Yes	Yes	
CSD 14	Yes	Yes	Yes
CSD 15	Yes	Yes	
CSD 16	Yes	Yes	Yes
CSD 17	Yes	Yes	
CSD 18	Yes	Yes	
CSD 19	Yes	Yes	

Table created by the external consultant

Although the details of the assessment made on the various risks considered is usually not detailed:

- CSDs generally take into account in their assessment legal risks and operational risks;
- Financial risks are mainly considered by CSDs with a banking license. Although the other CSDs claim they abide by the principles set by CPSS-IOSCO, ECSDA and the ECB, and although some of them do have riskier relations with intermediaries for instance, in practice this category of risks appears to be less considered.

Moreover, it should be noted that some smaller CSDs who have a limited number of links (outbound or inbound) tend to not have a systematic procedure, but consider links requests on a case-by-case basis.

#### *Focus on legal risks*

Issues specifically stressed by CSDs greatly vary. In the assessment of legal risks, for those who give details, consideration is usually given to the protection of assets and related segregation set-ups and, for some of them, other issues related to the transfer of ownership and structures for holding assets.

Among other considerations, the existence of an insurance coverage for the links, mentioned by banks seems relevant to include in the proposal on the assessment of legal risks.

CSD	Legal Risks	
	Assessment carried out	Notable specifics
CSD 1	Yes	Conditions on transfer of ownership, status of nominee functions, Insurance coverage, control of a public supervisory authority, existence of an auditing

		company
CSD 2	Yes	Segregation of assets, tax issues, regulatory analysis
CSD 3	Yes	Control of a public supervisory body, status comparable to that of a CSD in the respective home Member State, segregation, insurance coverage
CSD 4	Yes	Segregation, insurance coverage
CSD 5	Yes	Undetailed (protection ensured via standard rules of the CSD)
CSD 6	Yes	Protection of assets
CSD 7	Not specified	No specifics
CSD 8	Yes	Undetailed
CSD 9	Yes	Undetailed
CSD 10	Yes	Protection of assets
CSD 11	CPSS- IOSCO & ECB principles	No specifics
CSD 12	Yes	Undetailed
CSD 13	Yes	Protection of assets
CSD 14	Yes	Managed by account operators, to which the CSD delegates this function. Account operators subject to due diligence.
CSD 15	Yes	Undetailed
CSD 16	Yes	On a case by case basis
CSD 17	Yes	Segregation
CSD 18	Yes	Undetailed
CSD 19	Yes	Undetailed

*Table created by the external consultant*

#### *Focus on operational risks*

Based on the information gathered in relation to operational risks, the CSDs that responded to the questionnaire mentioned in vague terms the operational readiness/operational reliability of the back-up capabilities and business continuity plans.

Some stakeholders notably mentioned the consideration to be given for instance to the means of communication (such as the use of ISO 15022 formats) and reporting. They indicated that this may lead to “customised” links in the sense that these may slightly differ from the service levels usually provided to regular participants.

CSD	Operational risks
-----	-------------------

	<b>Assessment Carried out</b>	<b>Notable specifics</b>
CSD 1	Yes	Undetailed
CSD 2	Yes	Ability to manage their operational risk, business continuity requirements
CSD 3	Yes	Undetailed
CSD 4	Yes	Operational efficiency (deadlines, turnaround times), connectivity and STP standards (ISO 15022 compliance)
CSD 5	Yes	Undetailed
CSD 6	Yes	Undetailed
CSD 7	Yes	Technical aspects (undetailed)
CSD 8	Yes	Technical aspects (undetailed)
CSD 9	Yes	Technical aspects (undetailed)
CSD 10	Yes	Undetailed
CSD 11	Yes	Undetailed
CSD 12	Yes	Undetailed
CSD 13	Yes	Undetailed
CSD 14	Yes	Managed by account operators, to which the CSD delegates this function. Account operators subject to due diligence.
CSD 15	Yes	Undetailed
CSD 16	Yes	On a case-by-case basis
CSD 17	Yes	Contingency and back up routines
CSD 18	Yes	Undetailed
CSD 19	Yes	Undetailed

Table created by the external consultant

*Focus on financial risk*

<b>CSD/SSS</b>	<b>Financial risks</b>	
	<b>Assessment Carried out</b>	<b>Notable specifics</b>
CSD 1	Yes	Undetailed
CSD 2	Yes	Credit and Liquidity analysis
CSD 3	Yes	Credit analysis
CSD 4	Yes	Credit & Liquidity analysis, notably credit lines, rating, industry rank
CSD 5	Yes	Undetailed
CSD 6	N/A	N/A
CSD 7	Yes	Existence of a financial supervision
CSD 8	N/A	N/A
CSD 9	N/A	N/A
CSD 10	N/a	N/A
CSD 11	CPSS-IOSCO & ECB principles	

CSD 12	N/A	N/A
CSD 13	N/A	N/A
CSD 14	Yes	Managed by account operators, to which the CSD delegates this function. Account operators subject to due diligence.
CSD 15	N/A	N/A
CSD 16	Yes	On a case-by-case basis
CSD 17	N/A	N/A
CSD 18	N/A	N/A
CSD 19	N/A	N/A

*Table created by the external consultant*

As evidenced by the table above, limited detailed information exists on financial risks. Usually, CSDs with a banking license mention that they conduct an extensive credit analysis.

In some cases, a financial risk assessment should be conducted whereas some of the CSDs who responded to the questionnaire do not mention the financial risk assessment occurring.

*Other considerations taken into account in the assessments*

A few CSDs mentioned additional considerations of interest:

- The compliance with anti-money laundering (AML)/know-your-customer (KYC) regulations;
- The eligibility of the securities at the requesting CSD;
- Reputation;
- Management competence.

The existence of sufficient client demand is rarely mentioned.

*Risks considered in the set-up of inbound links*

Most CSDs (18 CSDs out of 23 CSDs who explicitly refer to this case) consider other CSDs as being regular participants and do not have specific procedures in place. Risks considered thus do not differ from those considered for other participants as mentioned in the section later in this paper relating to reasons which may justify a refusal by a CSD of access to participants. The table below confirms the assessments that are carried out on other CSDs based on the responses to the questionnaire.

CSD	Assessment Carried out	Notable specifics
CSD 1	Specific Procedure	Undetailed
CSD 2	Specific Procedure	Specific Agreement
CSD 3	Specific Procedure	Undetailed
CSD 4	Specific Procedure	Undetailed
CSD 5	Specific Procedure	Undetailed
CSD 6	Regular participant	-
CSD 7	Regular participant	-
CSD 8	Regular participant	-

CSD 9	Regular participant	-
CSD 10	Regular participant	-
CSD 11	Regular participant	-
CSD 12	Regular participant	-
CSD 13	Regular participant	Possible specifications for other Group CSDs
CSD 14	Regular participant	-
CSD 15	Regular participant	-
CSD 16	Regular participant	-
CSD 17	Regular participant	-
CSD 18	Regular participant	-
CSD 19	Regular participant	-
CSD 20	Regular participant	Extensive analysis carried out
CSD 21	Regular participant	-
CSD 22	Regular participant	-
CSD 23	Regular participant	-
CSD 24	Not specified	Special liability clauses for certain CSDs
CSD 25	Not specified	-
CSD 26	Not specified	-
CSD 27	Not specified	-
CSD 28	Not specified	-
CSD 29	Not specified	-
CSD 30	Not specified	-

## DVP VS FOP LINKS

### 2.12.1 How can the CSDR technical standards ensure the protection of linked CSDs and their participants?

<b>Specific Objective</b>	Ensure the protection of the linked CSDs and their participants
Option 1	Distinguish the list of risks to be specified between FoP and DvP links.
Option 2	Do not distinguish the list of risks to be specified between FoP and DvP links.
Preferred Option	<b>Option 1</b> - it is more tailored according to the different types of risks entailed by the DvP links compared to FoP links, especially as many CSDs do not have DvP links.

#### **Impact of the proposed policies**

<b>Option 1</b>	See Option 1 in 'Specific Objective' table above
	Description



<i>Benefits</i>	This option would allow for a better framing, and a harmonisation of the assessment of risks involved in the case of DvP links, where risks considered are more specific than for FoP. It offers a requirement that takes into consideration the different settlement processes and tailored requirements appropriately.
<i>Compliance costs:</i>	This option may have lower compliance costs than Option 2, as the requirements for CSD links would be more adequately tailored to the risks entailed by the each type of link.

<b>Option 2</b>	<i>See Option 2 in 'Specific Objective' table above</i>
	Description
<i>Benefits</i>	This option would have no additional benefits.
<i>Costs to regulator:</i>	Potential impacts on investors in cases where a CSD does not make an adequate assessment of the risks it faces with a DVP settlement link may have an impact on the regulators costs if the risks crystallise later on.
<i>Compliance costs:</i>	This option may have higher compliance costs than Option 1, as the requirements for CSD links would not be adequately tailored to the risks entailed by the each type of link.

## INTEROPERABLE LINKS

### 2.12.2 How can the CSDR technical standards ensure the protection of linked CSDs and their participants in the case of interoperable links?

<b>Specific Objective</b>	Ensure the protection of the linked CSDs and their participants in the case of interoperable links.
Option 1	An interoperable link should be established and maintained under the following conditions: <ul style="list-style-type: none"> <li>a) the linked CSDs shall agree on equivalent standards concerning reconciliation, opening hours for the processing of the settlement and of corporate actions and cut-off times;</li> <li>b) the linked CSDs shall establish equivalent procedures and mechanisms for transmission of settlement instructions to ensure a proper, secure and straight through processing of settlement instructions;</li> <li>c) where an interoperable link supports DVP settlement, the linked CSDs shall reflect at least daily and without undue delay the results of the settlement in their books.</li> <li>d) the linked CSDs shall agree on equivalent risk management models;</li> <li>e) the linked CSDs shall agree on equivalent contingency and default rules and procedures referred to in Article 41 of Regulation (EU) No 909/2014</li> </ul>
Option 2	Do not prescribe specific requirements for interoperable links.
Preferred Option	<b>Option 1</b> - it would ensure that specific risks related to interoperable links are adequately taken into account.

**Impact of the proposed policies**

<b>Option 1</b>	<i>See Option 1 in 'Specific Objective' table above</i>
	Description
<i>Benefits</i>	This option would ensure that specific risks related to interoperable links are adequately taken into account when setting up an interoperable link, in order to foster the protection of the linked CSDs and of their participants..
<i>Compliance costs:</i>	The compliance costs would be higher than for Option 2.

<b>Option 2</b>	<i>See Option 2 in 'Specific Objective' table above</i>
	Description
<i>Benefits</i>	This option would not have any additional benefits.
<i>Costs</i>	None

**MONITORING AND MANAGING ADDITIONAL RISKS ARISING FROM INDIRECT LINKS AND THE USE OF INTERMEDIARIES**

**2.12.3 How can the CSDR technical standards ensure that the additional risks arising from indirect links and the use of intermediaries are managed effectively?**

<b>Specific Objective</b>	Ensure the CSDs effectively monitor and manage additional risks arising from indirect links and the use of intermediaries
Option 1	Distinguish between the requirements for indirect links and direct links operated by an intermediary.
Option 2	Do not distinguish between the requirements for indirect links and direct links operated by an intermediary.
Preferred Option	Option 1 is the preferred option as it would allow the application of tailored requirements based on the role of the intermediary in the case of indirect links compared to when a requesting CSD uses an intermediary to operate a CSD link, whereby this account operator operates the accounts of the requesting CSD on its behalf in the receiving CSD's books.

**Impact of the proposed policies**

<b>Option 1</b>	<i>See Option 1 in 'Specific Objective' table above</i>
	Description
<i>Benefits</i>	This option would allow the application of tailored requirements based on the role of the intermediary in the case of indirect links compared to when a requesting CSD uses an intermediary to operate a CSD link, whereby this account operator operates the accounts of the requesting CSD on its behalf in the receiving CSD's books.

<i>Compliance costs:</i>	Compliance costs should be lower than in the case of Option 2, as Option 1 is in line with current practices.
--------------------------	---

<b>Option 2</b>	<i>See Option 2 in 'Specific Objective' table above.</i>
	Description
<i>Benefits</i>	No specific benefits.
<i>Compliance costs:</i>	Compliance costs should be higher than in the case of Option 1.

#### 2.12.4 Reconciliation methods for linked CSDs

<b>Specific Objective</b>	Ensure that linked CSDs have robust reconciliation procedures to ensure that their respective records are accurate.
Option 1	Where intermediaries are involved in the operation of CSD links, such intermediaries shall establish appropriate contractual arrangements with the CSDs concerned in order to ensure compliance with reconciliation measures for linked CSDs.
Option 2	Where intermediaries are involved in the operation of CSD links, the intermediaries should not be required to facilitate compliance with the reconciliation measures for linked CSDs.
Preferred Option	<b>Option 1</b> - it would ensure the applicability of the reconciliation measures for linked CSDs in the case that intermediaries are involved in the operation of the CSD links.

#### *Impact of the proposed policies*

<b>Option 1</b>	<i>See Option 1 in 'Specific Objective' table above</i>
	Description
<i>Benefits</i>	This option would ensure the applicability of the reconciliation measures for linked CSDs in the case that intermediaries are involved in the operation of the CSD links.
<i>Compliance costs:</i>	CSDs would need to adapt their reconciliation procedures, as well as the intermediaries involved in the operation of CSD links.

<b>Option 2</b>	<i>See Option 2 in 'Specific Objective' table above</i>
	Description
<i>Benefits</i>	There are no identified benefits.
<i>Compliance costs:</i>	CSDs would need to adapt their reconciliation procedures, but intermediaries involved in the operation of CSD links would not be impacted.

#### 2.12.5 DvP settlement

<b>Specific Objective</b>	Establish criteria to determine in which cases DVP settlement through CSD links is practical and feasible
Option 1	DVP settlement shall be regarded as practical and feasible under the following circumstances: <ul style="list-style-type: none"> <li>(a) There is a market demand for DvP settlement evidenced through a request from any the User Committees of one of the linked CSDs.</li> <li>(b) The linked CSDs may charge a reasonable commercial fee for the provision of DvP settlement, on a cost-plus basis, unless otherwise agreed by the linked CSDs.</li> <li>(c) There is a safe and efficient access to cash in the currencies used by the receiving CSD for settlement of securities transactions of the requesting CSD and its participants.</li> </ul>
Option 2	Same as Option 1, without the need to consider point (a) regarding market demand.
Preferred Option	<b>Option 1</b> - it would ensure costs are engaged only when necessary to meet market needs.

#### ***Impact of the proposed policies***

<b>Option 1</b>	<i>See Option 1 in 'Specific Objective' table above</i>
	Description
<i>Benefits</i>	This option would ensure that market needs are taken into account when considering whether to set up a DvP link.
<i>Compliance costs:</i>	This option would have lower compliance costs than Option 2, as it would take into account market needs.

<b>Option 2</b>	<i>See Option 2 in 'Specific Objective' table above</i>
	Description
<i>Benefits</i>	This option would not bring additional benefits.
<i>Compliance costs:</i>	This option would have higher compliance costs than Option 1, as it may trigger the setting up of DvP links without taking into account market needs.

## **2.13 Access (Articles 33, 49, 52 and 53 CSDR)**

### **2.13.1 Access of Participants to CSDs (Article 33 CSDR)**

#### **DESCRIPTION OF THE EXISTING SITUATION**

*Data collection methodology: published information in line with the CPSS-IOSCO Disclosure frameworks, CSD rules, answers to the external consultant's questionnaire.*

For the purpose of this section, 32 CSDs were considered by the external consultant.

Out of 32 CSDs for which data was collected by the external consultant, 31 CSDs have a formalised application procedure for requesting participants.

### ***Risk categories***

In order to collect data on risk analysis as part of CSDs application procedures, 4 main admission criteria were used by the external consultant:

Legal considerations

Financial considerations

Internal control / risk management considerations

Operational and technical considerations

First, it should be mentioned that for one CSD no information was publically available regarding the details of the application procedure. Therefore the following analysis is based on 30 CSDs.

### *Legal considerations*

When assessing legal risks regarding requesting participants, CSDs first have to comply with the rules in place in their country of incorporation, whether or not the requesting participants are subject to a specific regulation and if they are properly licensed.

Moreover, some CSDs look at the existence of anti-money laundering measures within the participant's organisation.

Out of 30 CSDs:

25 CSDs take legal considerations into account when analysing a participant's application

5 CSDs do not specifically mention legal considerations as part of their analysis

### *Financial considerations*

When assessing financial risks, CSDs look at a requesting participant's resources, through annual reports for instance, in order to determine the stability of the participant in the future.

Out of 30 CSDs:

20 CSDs take financial considerations into account when analysing a participant's application

10 CSDs do not specifically mention financial considerations as part of their analysis

### *Internal control / risk management considerations*

When assessing internal control and risk management considerations of requesting participants, CSDs can look at the effective management of the risks they undertake in the course of their activities and the monitoring of their clients' obligations to them and their own obligations. They can also ask for proof that internal audits are properly performed.

Out of 30 CSDs:

9 CSDs take internal control / risk management considerations into account when analysing a participant's application

21 CSDs do not specifically mention internal control / risk management considerations as part of their analysis

#### *Operational and technical considerations*

When assessing operational and technical aspects, CSDs will look at the requesting participant's ability to be connected to and use its information system, at the operation and maintenance of an adequate communication platform, at the existence of a business continuity policy.

Out of 30 CSDs:

26 CSDs take operational and technical considerations into account when analysing a participant's application

4 CSDs do not specifically mention operational and technical considerations as part of their analysis

In addition to legal, financial, internal control / risk management and operational /technical criteria, several CSD's take other types of risks into consideration when assessing a participant's application.

#### *Considerations on reputation*

In order to ensure that accepting a participant's application will not negatively impact their business, some CSDs ask participants to demonstrate in particular that, beyond the implementation of anti-money laundering (AML) or Know Your Customer (KYC) measures, their management's reputation has not been impaired by any problems within the company.

#### *Liquidity and credit risk*

CSDs that hold a banking license, given this status, can assess a requesting participant's liquidity and credit situation and whether or not it complies with its capital requirements, in order to make sure that the CSD's activities will not be endangered by accepting that participant.

Most CSDs agree with the risk categories defined by ESMA to be taken into account when evaluating participants' applications. However, while legal, financial and operational risks are important categories, several CSDs believe that the risk analysis should not necessarily be limited to these categories and that these categories should not be limited to the list of examples presented in ESMA's Discussion Paper.

#### **Cases of refusal**

*Data collection methodology: answers to the external consultant's questionnaire (19 CSDs)*

Out of 19 CSDs for which data was available:

12 CSDs have not refused access to a participant in the past 5 years;

7 CSDs have stated that cases of refusal are rare and in line with the CSDs' admission criteria.

#### **Justification of the refusal**

Data collection methodology: CSD rules.

Out of 32 CSDs:

12 CSDs mention that they are required to justify refusal of access to a participant

1 CSD explicitly mentions that it is not required to justify refusal of access to a participant

No data was publicly available for the remaining 19 CSDs

CSDs generally agree with the timeframes proposed by ESMA for the procedure to be applied in the case of refusal of access.

**What risks should be taken into account by CSDs when carrying out a comprehensive risk assessment, and by competent authorities when assessing the reasons for refusal of access?**

<b>Objective</b>	Establish the risks to be taken into account by CSDs when carrying out a comprehensive risk assessment, and by competent authorities when assessing the reasons for refusal of access of participants to a CSD
Option 1	The following types of risks: legal, financial and operational.
Option 2	Additional risks may be considered that do not fall into one of the categories: legal, financial and operational.
Preferred Option	<b>Option 1</b> appears to be preferable, as it would ensure a level playing field across CSDs in the EU.

**Impact of the proposed policies**

<b>Option 1</b>	<i>See Option 1 in 'Specific Objective' table above</i>
	Description
<i>Benefits</i>	This option would ensure a level playing field across CSDs in the EU, with a higher degree of transparency and certainty regarding the criteria to be used, and would potentially reduce the likelihood of complaints where access is not granted.
<i>Compliance costs:</i>	The overall compliance costs both for CSDs and participants may be lower than for Option 2, as it would ensure harmonised and standardised criteria across the EU.

<b>Option 2</b>	<i>See Option 2 in 'Specific Objective' table above</i>
	Description
<i>Benefits</i>	This may imply fewer changes in the current practices of CSDs, as it would allow for a more flexible approach.
<i>Compliance costs:</i>	The overall compliance costs both for CSDs and participants (especially participants active in more than one market) may be higher than for Option 1, as the criteria would vary across CSDs.

### 2.13.2 Access of Issuers to CSDs (Article 49 CSDR)

*Data collection methodology: published information in line with the CPSS-IOSCO Disclosure framework, CSD rules, answers to the external consultant's questionnaire.*

For the purpose of this section, 32 CSDs were considered.

Out of 32 CSDs for which data was collected, 31 CSDs have a formalised application procedure for issuers.

#### **Risks considered by CSDs for the participation of issuers**

Publicly available information that was accessible in the course of this study did not provide details on risks specifically weighing on issuers.

- Issuers are considered in assessing the eligibility of a security for operations at the CSD. Yet no details are provided on specific criteria applicable to issuers themselves, beyond those applying to the security, its characteristics, and the existence of relevant documentation and regular provision of information as required by local laws;
- Issuers are considered as “participants”, but for those firms acting as Issuing and Paying Agents, who are not the actual issuers of the securities and thus do not qualify for this designation.

Only one CSD mentioned that it considers the following when assessing issuers for access:

- Legal risks: due foundation of the issuer, proper issue of the securities, fulfilment of obligations regarding information documents (prospectus or other) including the formal requirements;
- Operational risks: need for a link to a foreign CSD and related risks.

#### **Refusal by a CSD to provide services to an issuer**

Only one CSD mentioned a refusal to provide services to issuers in the past five years. In the cases mentioned, this CSD refused to provide services for the following reasons:

- the issuer did not fulfil the legal obligation to publish documentation (prospectus or other information documents);
- the issuer had violated provisions on the issuance of securities.

#### **How can the technical standards ensure that appropriate checks are performed on the financial risks of an issuer requesting to have its securities recorded in a CSD?**

<b>Specific Objective</b>	Ensure that a CSD is not exposed to unnecessary financial risks and the requesting issuer holds sufficient financial resources to fulfil its contractual obligations towards the CSD
Option 1	Assess the financial risks following an issuer's request for recording its securities in the CSD, taking into account whether the requesting issuer holds sufficient financial resources to fulfil its contractual obligations towards the CSD.
Option 2	Do not perform a detailed assessment of the financial capabilities of the requesting issuer to meet its contractual obligations towards the CSD.



Preferred Option	<b>Option 1</b> – this option is the most appropriate as it mitigates the likelihood of a CSD being placed under unexpected financial stress due to the actions of a potential issuer.
------------------	--

### **Impact of the proposed policies**

<b>Option 1</b>	<i>See Option 1 in 'Specific Objective' table above</i>
	Description
<i>Benefits</i>	It is important for a CSD to assess whether the requesting issuer holds sufficient financial resources to fulfil its obligations towards the CSD e.g. payments in connection to corporate actions or CSD fees. This approach will ensure that the risks of these obligations not being met are addressed before access is authorised, reducing the risks for the CSD.
<i>Compliance costs:</i>	There will be compliance costs for the CSD that relate to the financial assessments being made on the requesting issuer.

<b>Option 2</b>	<i>See Option 2 in 'Specific Objective' table above</i>
	Description
<i>Benefits</i>	It will be easier for issuers to record securities in a CSD because of the less stringent requirements in relation to an issuer's financial resources.
<i>Compliance costs:</i>	There would be no initial cost for the CSDs, however if issuers were granted access to a CSD and then later were unable to meet specific financial commitments then there would be an associated cost for the CSD linked to trying to remediate potential impacts.

### **2.13.3 Access between CSDs (Article 52 CSDR)**

**What risks should be taken into account by CSDs when carrying out a comprehensive risk assessment, and by competent authorities when assessing the reasons for refusal of access?**

<b>Objective</b>	Establish the risks to be taken into account by CSDs when carrying out a comprehensive risk assessment, and by competent authorities when assessing the reasons for refusal of access from another CSD
Option 1	The following types of risks: legal, financial and operational.
Option 2	Additional risks may be considered that do not fall into one of the categories: legal, financial and operational.
Preferred Option	<b>Option 1</b> appears to be preferable, as it would ensure a level playing field across CSDs in the EU.

### **Impact of the proposed policies**

<b>Option 1</b>	<i>See Option 1 in 'Specific Objective' table above</i>
	Description
<i>Benefits</i>	This option would ensure a level playing field across CSDs in the EU, with a higher degree of transparency and certainty regarding the criteria to be used, and would potentially reduce the likelihood of complaints where access is not granted.
<i>Compliance costs:</i>	The overall compliance costs for CSDs may be lower than for Option 2, as it would ensure harmonised and standardised criteria across the EU.

<b>Option 2</b>	<i>See Option 2 in 'Specific Objective' table above</i>
	Description
<i>Benefits</i>	This may imply fewer changes in the current practices of CSDs, as it would allow for a more flexible approach.
<i>Compliance costs:</i>	The overall compliance costs for CSDs may be higher than for Option 1, as the criteria would vary across CSDs.

#### **2.13.4 Access between CSDs and another market infrastructure (Article 53 CSDR)**

##### **DESCRIPTION OF THE EXISTING SITUATION**

*Data collection methodology: published information in line with the CPSS-IOSCO Disclosure framework, CSD rules, answers to external consultant's questionnaire.*

For the purpose of this section, 32 CSDs were considered. 31 CSDs have formalised the application procedure and are considered below.

##### ***Reasons which may justify a refusal by a CSD to grant access to other market infrastructures***

First, it is important to point out that admission criteria for other market infrastructures are very similar to those for participants.

In the case of CSDs holding a banking license, all participants, including other market infrastructures, are considered customers. Thus, their status does not make a difference regarding the criteria that will be assessed in order to decide if their request will be granted.

As for CSDs without a banking license, most do not have a separate application procedure for other market infrastructures either. In most cases, CSDs will give a list of eligible entities (including participants and other market infrastructures) and the requirements for these entities as a group.

Certain documents that have to be provided by a requesting market infrastructure, as part of the application file, can be different from the documents asked from participants but the criteria themselves are the same for a participant and a market infrastructure.

*As a result, the external consultant found no significant differences between admission criteria for other market infrastructures and criteria for participants.*

### ***Risk categories***

In order to collect data on risk analysis as part of CSDs application procedures, 4 main admission criteria were used:

Legal considerations

Financial considerations

Internal control / risk management considerations

Operational and technical considerations

As for participants, no information was publically available regarding the details of the application procedure used by one CSD. 31 CSDs only will thus be part of the following analysis.

#### *Legal considerations*

When assessing legal risks regarding requesting market infrastructures, CSDs look at their proper incorporation in their country, whether or not they are subject to a specific regulation and if they are properly licensed. Moreover, some CSDs look at the existence of anti-money laundering measures within the other market infrastructure's organisation.

Out of 31 CSDs:

26 CSDs take legal considerations into account when analysing a market infrastructure's application

5 CSDs do not specifically mention legal considerations as part of their analysis

#### *Financial considerations*

When assessing financial risks, CSDs look at a requesting market infrastructure's resources, through annual reports for instance, in order to determine the stability of the other market infrastructure in the future.

Out of 31 CSDs:

20 CSDs take financial considerations into account when analysing a market infrastructure's application

11 CSDs do not specifically mention financial considerations as part of their analysis

#### *Internal control / risk management considerations*

When assessing internal control and risk management considerations of requesting market infrastructures, CSDs can look at the effective management of the risks they undertake in the course of their activities and the monitoring of their clients' obligations to them and their own obligations. They can also ask to be demonstrated that internal audits are properly performed.

Out of 31 CSDs:

9 CSDs take internal control / risk management considerations into account when analyzing a market infrastructure's application;

22 CSDs do not specifically mention internal control / risk management considerations as part of their analysis.

#### *Operational and technical considerations*

When assessing operational and technical aspects, CSDs will look at the requesting market infrastructure's ability to be connected to and use its information system, at the operation and maintenance of an adequate communication platform, at the existence of a business continuity policy.

Out of 31 CSDs:

27 CSDs take operational and technical considerations into account when analyzing a market infrastructure's application;

4 CSDs do not specifically mention operational and technical considerations as part of their analysis.

In addition to legal, financial, internal control / risk management and operational/technical criteria, several CSD's take other types of risks into consideration when assessing a market infrastructure's application.

#### ***Considerations on reputation***

In order to make sure that accepting a market infrastructure's application will not negatively impact their business, some CSDs ask market infrastructures to demonstrate in particular that, beyond the implementation of anti-money laundering or KYC measures, their management's reputation has not been impaired by any problems within the company.

#### *Liquidity and credit risk*

CSDs that hold a banking license, given this status, can assess a requesting market infrastructure's liquidity and credit situation and decide whether or not it complies with its capital requirements, in order to make sure that the CSD's activities will not be endangered by accepting an application.

Most CSDs agree with the risk categories that were previously defined by ESMA to be taken into account when evaluating a market infrastructure's application. However, while legal, financial and operational risks are important categories, several CSDs believe that the risk analysis should not necessarily be limited to these categories and that these categories should not be limited to the list of examples presented in ESMA's Discussion Paper.

### ***Elements of the procedure where a CSD refuses to provide access to another market infrastructure***

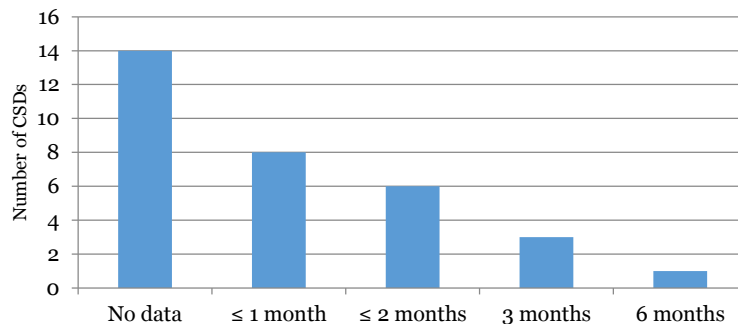
#### Deadline for answering participants regarding their application

Out of 31 CSDs:

18 CSDs clearly state that there is a formal deadline to accept or refuse access to another market infrastructure

13 CSDs do not mention such deadline

Below is a breakdown of the number of months after which CSDs must give an answer to other market infrastructures regarding their application:



*Table created by the external consultant*

Out of 18 CSDs for which data was found regarding the existence of a deadline, 10 CSDs have a deadline that is longer than a month after they received the application.

#### Cases of refusal

Out of 32 CSDs:

Data was collected for 19 CSDs through the external consultant's questionnaire on whether or not another market infrastructure had been refused access to the CSD in the past 5 years

Data was not publicly available on that matter for 14 CSDs

Out of 19 CSDs for which data was available:

12 CSDs have not refused access to another market infrastructure in the past 5 years

The remaining 7 CSDs state that cases of refusal are rare and in line with the CSDs' admission criteria

#### Justification of the refusal

Out of 32 CSDs who have a formalised procedure:

12 CSDs mention that they are required to justify refusal of access to another market infrastructure

1 CSD explicitly mentions that it is not required to justify refusal of access to another market infrastructure

No data was publicly available for the remaining 19 CSDs

CSDs generally agreed with ESMA's proposed timeframes for the procedure to be applied in the case of refusal of access.

**How can the CSDR technical standards clearly identify the risks related to the different entities that may have access to CSDs?**

<b>Specific Objective</b>	To ensure that the risks are clearly presented in relation to the different entities that may have access to a CSD
Option 1	Apply the same requirements regardless of the type of entity that may have access to a CSD.
Option 2	Include tailored requirements for issuers, participants, CSDs, CCPs and trading venues based on the specificities of each type of entity
Preferred Option	<b>Option 2</b> – CP feedback supported the idea of separating the requirements for issuers, participants, CSDs, CCPs and trading venues to ensure clarity and to enable a tailored approach.

***Impact of the proposed policies***

<b>Option 1</b>	<i>See Option 1 in 'Specific Objective' table above</i>
	Description
<i>Benefits</i>	The benefits of this option are limited, it would require less risk specific assessments by CSDs.
Compliance costs:	The compliance costs for CSDs are likely to be smaller in the short term as the same assessment process would need to be followed for each type of request for access. However in the longer term the compliance costs facing the CSD would potentially be larger than in Option 2. This is because a less focused risk assessment that is carried out on requesting entities would not be tailored to the risks of a specific type of entity.

<b>Option 2</b>	<i>See Option 2 in 'Specific Objective' table above.</i>
	Description
<i>Benefits</i>	This approach will ensure the requirements are clear and proportionate, taking into account the different roles and responsibilities of the different entities that may have access to CSDs.
<i>Costs</i>	The overall compliance costs may be lower than for Option 1 in the long term, as the risk assessments would be tailored according to the roles of the different types of entities.

## 2.14 Authorisation to provide banking-type ancillary services (Article 55 CSDR)

Should the competent authority rely on documentation that it already possesses when making a decision on whether to authorise a CSD to designate a credit institution or to provide any banking-type ancillary service?

<b>Specific Objective</b>	To ensure that the competent authority has the appropriate information to make a decision on whether to authorise a CSD to designate a credit institution or to provide any banking-type ancillary service, whilst not imposing undue costs on applicants.
Option 1	The applicant should provide all necessary information to the competent authority in its application to designate a credit institution or to provide any banking-type ancillary services, including the information provided under Article 17 for the general authorisation to perform CSD services.
Option 2	The applicant should only provide information to designate a credit institution or to provide any banking-type ancillary service and not re-submit any elements that had previously been provided to the competent authority in accordance with Articles 17 or 22 CSDR, provided that there is no material change arising from that information.
Preferred Option	<b>Option 2</b> – this is a proportionate approach which will ensure that submissions of information are not duplicated and resource is not unnecessarily directed toward providing information that has been submitted previously.

### *Impact of the proposed policies*

<b>Option 1</b>	<i>See Option 1 in 'Specific Objective' table above</i>
	Description
<i>Benefits</i>	Very clear, standardised set of information to be provided by all applicants, ensures all the necessary information is received allowing competent authorities to make considered decisions.
<i>Compliance costs:</i>	Additional costs may arise, since information that may have been submitted previously may need to be re-submitted.
<i>Costs to other stakeholders</i>	There may be costs to other stakeholders in events where information that is requested has been sourced by the applicant CSD from another stakeholder and so needs to be produced again by that stakeholder.

<b>Option 2</b>	<i>See Option 2 in 'Specific Objective' table above</i>
	Description
<i>Benefits</i>	Applicants would not need to re-submit previously sent information and so the process for assessments would be smoother and more efficient.
<i>Costs to regulator:</i>	Regulators would have to ensure they have well organised recordkeeping abilities and triage of the incoming applications so that there are no gaps between the required details under CSDR and the technical standards under

	Article 55 of CSDR and the details provided by the applicants and those already held by the competent authorities.
<i>Compliance costs:</i>	Applicants would have to ensure they have effectively recorded the information previously submitted to regulators so that they know at all times the details sent already to the competent authorities in order not to send unnecessary documents or miss documents that the competent authorities had not yet received but should receive according to the CSDR and relevant technical standards.

### 3 INTERNALISED SETTLEMENT (ARTICLE 9 CSDR) – DRAFT RTS AND ITS

To consider the costs and benefits of different approaches for monitoring internalised settlement ESMA based its analysis on various pieces of information provided by financial institutions.

Pre-CSDR the internalisation of settlement by custodians is fundamentally based on two situations. The first involves cases where a client transfers securities from one account to another within the custodian’s books, without a need for actual settlement at CSD level. The second involves custodians providing services to buy-side and sell-side players, where custodians can book trades themselves. There are effectively two types of institutional custodians relevant to this analysis: those who serve both buy-side and sell-side clients (especially on some specific markets), and those who serve only buy-side clients.

Below is a summary of the existing arrangements at firms which conduct internalised settlement. Five participants provided information that related to their actual internalised settlements.

All five participants conducted different processes:

- Bank 1 did not provide internalised settlement, although “intra-account” settlement (booking between two accounts of the same client) may not have been considered in their response;
- Bank 2, served both sell-side and buy-side clients, with a significant internalised settlement rate (above 10%);
- Bank 3’s activity reflected a low level of internalised settlement (<1%);
- Bank 4 had a very limited amount of internalised settlement (<1%), although figures provided do not show intra-account settlement (settlement between accounts of the same client);
- Bank 5 reported a significant level of internalised settlements;
- One other stakeholder confirmed a 4% share of internalised settlements.

In general the level of internalised settlement appeared to be relatively low except for Bank 2 and Bank 5.



## Internalised settlement reporting

None of the stakeholders involved in the research provided input on the current existence of reporting to competent authorities on internalised settlement.

It appears that for some players the identification of internalised settlements may represent a cost. Initial estimations based on interviews suggested that this cost may be around EUR 1M for each settlement internaliser.

Respondents to the CP felt that it was important to achieve a level playing field with regard to the scope and granularity of the reporting of internalised settlement, with some saying that reporting on internalised settlement should mirror the requirements CSDs are subject to.

Other respondents felt that a reporting breakdown beyond aggregated volume and value would be beyond the Level 1 mandate and too costly for settlement internalisers.

The key objective of internalised settlement reporting is to ensure that NCAs are provided with useful, up to date information on the activities of settlement internalisers which can be used to identify any potential risks.

ESMA is aware that the implementation of certain requirements (such as aggregation by Issuer CSD, or transaction type) will require time for the respective market practices to be developed. At the same time, competent authorities will need time to build their IT solutions to be able to receive, process and analyse the reports, while the settlement internalisers will have to develop their own internal IT solutions to be able to meet the reporting requirements. This process can only start after all exact details of the reporting requirements have been agreed. Due to the reasons mentioned above, ESMA proposes that the requirements on internalised settlement reporting should become applicable 24 months after the publication of the technical standards in the Official Journal.

## DETAILS OF INTERNALISED SETTLEMENT REPORTING

**How can the CSDR technical standards enable competent authorities to have adequate data regarding internalised settlement to enable them to identify potential risks?**

<b>Specific Objective</b>	Enable competent authorities to have adequate data regarding internalised settlement to enable them to identify potential risks
Option 1	Reporting of aggregate volumes and values of internalised settlement
Option 2	The reports on internalised settlement should provide detailed information on the aggregated volume and value of settlement instructions settled by settlement internalisers outside securities settlement systems specifying asset class, type of securities transactions, type of clients, and issuer CSD, as well as data on failed internalised settlement instructions.

Preferred Option	<b>Option 2</b> is preferable because it would provide a more detailed insight into the activity of settlement internalisers. The reports would be useful when considering where internalisers experience the most fails, and also provide data that would be useful for spotting trends which could lead to risks for investors and the orderly functioning of financial markets.
------------------	--

**Impact of the proposed policies**

<b>Option 1</b>	<i>See Option 1 in 'Specific Objective' table above</i>	
	Qualitative description	Quantitative description
<i>Benefits</i>	This option would allow competent authorities to have a quick view of the activity on internalised settlement compared to CSD settlement, based on a simple view of value and volumes	
Costs to regulator:	Competent authorities would have an on-going cost related to the collection and analysis of the reported data. (lower than for Option 2) The authorities will not be able to easily identify potential risks arising from internalisation of settlement.	
Compliance costs:	The setting up of the necessary procedures for the reporting would be a one-off cost for those entities providing internalised settlement. On-going costs will exist for providing the regular reporting however they should be lower than for Option 2.	Some banks mentioned an estimation of a EUR 1M one-off cost per custodian. Considering only a limited number of market players service at the same time sell-side and buy-side clients, thus having the opportunity to provide internalised settlement, only the global custodians are likely to be impacted.

<b>Option 2</b>	<i>See Option 2 in 'Specific Objective' table above</i>	
	Description	
<i>Benefits</i>	This option would provide a more detailed insight for competent authorities into the activity of settlement internalisers. The reports would be useful when considering where internalisers experience the most fails, and also provide data that would be useful for spotting trends which could lead to risks for investors and the orderly functioning of financial markets. As proved by the lack of evidence provided to ESMA under current market practices, there is a need to enhance transparency on this activity.	

<i>Costs to regulator:</i>	<p>The costs for competent authorities would be of a similar nature to Option 1, with the main cost for the implementation of a process to analyse new data (higher than for Option 1).</p> <p>The reputational cost for competent authorities of not identifying risks related to this activity will be much lower than under Option 1.</p>
<i>Compliance costs:</i>	<p>Compliance costs would be of a similar nature to Option 1, but higher due to the additional details that must be reported using this option.</p>