ECSDA
European Central Securities Depositories Association

22 May 2014

"A new framework for CSD authorisation and supervision":

ECSDA comments on the ESMA Discussion Paper on CSDR technical standards (Part 2)

This paper constitutes the second part of ECSDA's comments on the ESMA Discussion Paper of 20 March 2014 on draft technical standards for the CSD Regulation ("CSDR"). It covers questions 21 to 54 of the consultation, which primarily relate to the authorisation framework for CSDs.

Table of contents

ECSDA aisbl (European Central Securities Depositories Association), Rond-Point Robert Schuman 6, bte 9, B-1040 Brussels
Phone: +32 2 230 99 01 Email: info@ecsda.eu Website: www.ecsda.eu

Executive Summary

- Technical standards under the CSD Regulation should not be considered as 'minimum requirements' for competent authorities. **The imposition of additional requirements ('on top of' the European rules) by national regulators should be avoided as much as possible** to ensure truly equal conditions of competition for CSDs and truly harmonised safety standards across EU markets. National regulators should not be allowed to 'gold-plate' technical standards and require CSDs to maintain, for example, additional data items as part of their record-keeping obligation compared to CSDs operating similar activities in other EU countries.

- That said, **harmonised standards do not equal a "one-size-fits-all" approach and it should be possible for European technical standards to be implemented proportionately, taking into account the diversity in CSD business models, activities and size.** For instance, requirements covering the compliance function, the audit function, and the risk function in CSDs, should not mean that smaller CSDs have to appoint a staff member exclusively dedicated to each of these functions. It should be possible, instead, for these functions to be combined with other roles. For example, the same person will often act both as legal counsel and compliance officer for the CSD. In the case of corporate groups, it should be possible for an individual to perform these functions for different entities within the group.

- **The ongoing supervisory assessments to be carried out based on the CSDR technical standards should build on, and avoid duplication with, assessments under the CPSS-IOSCO Principles for financial market infrastructures, and Eurosystem assessments, including for CSD links.** ECSDA also expects that the former ESCB-CESR standards will be discontinued and replaced by the CSDR technical standards.

- **CSDs should only be allowed to hold participations in other legal entities if such participations do not substantially alter their risk profile.** In practice, (i) CSDs should not assume unlimited liability for such participations, (ii) the activities of subsidiaries should be complementary to or support the activities of the CSD (without necessarily being restricted to other entities in the securities chain), (iii) services authorised under the CSD Regulation, including when they are performed by a subsidiary of the CSD, should constitute the main source of revenues for the CSD, and (iv) CSDs should be required to take into account the risks related to their participations in their recovery plan. CSDs should however be allowed to assume control over other entities where such control contributes to a better management of the risks to which the CSD is exposed.

- **The recordkeeping requirements currently envisaged by ESMA are unnecessarily extensive and should be substantially scaled down to avoid imposing unnecessarily high costs on CSDs and their users.** Based on information collected from 18 European CSDs, and assuming that the proposed ESMA requirements would all have to be implemented, ECSDA estimates that the system development costs for the 33 CSDs in the European Economic Area would exceed EUR 75 million, possibly even EUR 115 million. The mandatory use of Legal Entity Identifiers (LEI) and of non-proprietary format for CSD records, in particular, would be extremely costly to implement.

- **Moreover, the purpose of CSD recordkeeping requirements should be clarified and CSDs should not be confused with "trade repositories".** In line with the CSD Regulation, rules on recordkeeping should primarily aim at allowing regulators to assess compliance with CSDR. They are not meant to provide regulators with transaction data allowing them to oversee the activities of market participants. The list of compulsory recordkeeping items should be reduced accordingly, and a more balanced approach must be found.

- CSDs will have to make important technical adaptations to their systems in order to comply with

some of the most complex technical standards. It is thus indispensable for ESMA to recognise that CSDs will not realistically be able to demonstrate compliance with all technical standards during the initial authorisation process. **An appropriate transition period must be foreseen, at least for the following standards:**

- **Settlement discipline:** CSDs, market participants and other infrastructures should be given up to three years to comply with the new rules on buy-ins and penalties for late settlement, to be adopted under CSDR article 7;

- **Recordkeeping:** Depending on the scope of the final requirements, a transition period of at least 14 months will have to be determined to allow CSDs to develop the required functionalities;

- **Requirements on a secondary processing site:** CSD having to set up a new secondary processing site should be given at least 6 months after the entry into force of the technical standards to achieve compliance.

▪ **Technical standards should ensure that the recognition of third country CSDs under CSDR is not just a one-off approval, but an ongoing process.** Once a third country CSD is recognised, follow-up arrangements should be in place to ensure ongoing supervisory equivalence.

▪ **Finally, for CSDs with a banking licence, ESMA should anticipate possible overlaps and avoid whenever possible inconsistencies between CSDR technical standards and applicable banking legislation (CRD IV and CRR in particular[1]).**

[1] CRD IV refers to the Directive 2013/36/EU and Regulation (EU) No 575/2013 on capital requirements for banks.

1. Internalised settlement - Article 9(2), (3)

WHAT THE LEVEL 1 REGULATION SAYS:
Article 9(1): **"**Settlement internalisers shall report to the competent authorities the aggregated volume and value of all securities transactions that they settle outside securities settlement systems on a quarterly basis. Competent authorities shall without delay transmit the information received under the first subparagraph to ESMA and shall inform ESMA of any potential risk resulting from that settlement activity."

WHAT THE LEVEL 2 TECHNICAL STANDARDS SHOULD SPECIFY:
Article 9(2): RTS on "the content of such reporting"
Article 9(3): ITS "to establish standard forms, templates and procedures for the reporting and transmission of information referred to in paragraph 1"

ANNUAL REPORTING BY ESMA ON INTERNALISED SETTLEMENT:

Article 74(1): "ESMA, in cooperation with EBA and the authorities referred to in Articles 10 and 12, shall submit annual reports to the Commission (...) [including] at least an assessment of the following:
(c) measuring settlement which does not take place in the securities settlement systems operated by CSDs based on the number and volume of transactions and any other relevant criteria based on the information received under Article 9".

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

ECSDA does not comment on the requirements for "settlement internalisers" since CSDs are not in the scope of internalised settlement and are subject to more detailed reporting requirements on all their settlement activities, including settlement via CSD links.

2. Information provided to the authorities for authorisation - Article 17(8), (9)

WHAT THE LEVEL 1 REGULATION SAYS:
Article 17(1): "The applicant CSD shall submit an application for authorisation to its competent authority."
Article 17(2): "The application for authorisation shall be accompanied by all information necessary to enable the competent authority to satisfy itself that the applicant CSD has established, at the time of the authorisation, all the necessary arrangements to meet its obligations set out in this Regulation. The application for authorisation shall include a programme of operations setting out the types of business envisaged and the structural organisation of the CSD."
Article 17(3): "Within 30 working days from the receipt of the application, the competent authority shall assess whether the application is complete. If the application is not complete, the competent authority shall set a time limit by which the applicant CSD has to provide additional information. The competent authority shall inform the applicant CSD when the application is considered to be complete."

WHAT THE LEVEL 2 TECHNICAL STANDARDS SHOULD SPECIFY:
Article 17(8): RTS on "the information that the applicant CSD shall provide to the competent authority in the application for authorisation"
Article 17(9): ITS on "standard forms, templates and procedures for the application for authorisation."

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

ECSDA agrees with the general 'building blocks' contained in Annex 1 of the ESMA Discussion Paper, while noting that the information that CSDs are required to provide for authorisation is very extensive. We agree with ESMA's statement, in paragraph 79, that the application of a CSD *"should include all details needed to demonstrate compliance with all CSDR and relevant technical standards"*.

However, we do not think that CSDs can realistically be expected to comply with the technical standards under Title II of the CSD Regulation, especially as regards settlement discipline measures (CSDR article 7) by the time they file their application with their competent authority. Indeed, as outlined in part 1 of our comments on the ESMA Discussion Paper[2], and in line with the joint industry letter sent to the co-legislators on 4 November 2013[3], details of the future settlement discipline regime will not be known until Level 2 legislation is adopted in 2015 and the changes required of CSD systems will take months to implement. Moreover, these changes will have to be reflected by CSD participants so that they can pass on fines to their own clients, if appropriate. Given the additional complexity of having to implement these changes in parallel with the migration to TARGET2-Securities for many EU CSDs participating in the project, a transition period is necessary to make the necessary adaptations. **We thus ask ESMA to clarify that the items listed under points E2 and E3 of Annex I of the Discussion Paper (intended settlement dates, preventing fails and measures to address settlement fails) will not be required for a CSD to obtain authorisation, at least in the first three years after the Level 2 standards on settlement discipline have been adopted.**

A similar approach, but with a presumably shorter transition period, should be adopted for points C7 on recordkeeping and F3(2) as regards CSD secondary processing sites (see more detailed explanations in our responses to questions 28 and 39).

We also suggest that points 8 and 9 under C2.8 (Internal Control Mechanisms) in Annex I could be removed as they seem to duplicate with the information required under A2.2 (Policies and procedures).

Furthermore, **we do not think that the information specified by ESMA under article 17(8) and detailed in Annex 1 of the Discussion Paper should be described as "minimum requirements".** Given that the proposed requirements are already very detailed and extensive, and given the need to ensure a consistent and fair application process for all CSDs across the European Union, the contents required of CSD applications should be the same in all jurisdictions, and it should not be possible for national regulators in certain countries to 'gold-plate' the ESMA requirements and ask for more information than would have been required by another national regulator in a different jurisdiction. Since the Level 1 text does not refer to "minimum" requirements, we suggest that ESMA should avoid this term in the technical standards and design instead a single, harmonised list of elements to be contained in CSDs' application documents.

That said, given the diversity of CSD business models and service offers, ECSDA note that not all the required items listed in Annex I will be relevant and appropriate for all CSDs, in particular given that not all CSDs will be authorised for the full set of core and ancillary services. The technical standards should thus recognise that, if a CSD does not intend to provide a specific service (or e.g. if it does not plan to establish any link with other CSDs), it should not be required to provide the corresponding information to the competent authority.

ECSDA also believes that CSDs should be allowed to leverage, where appropriate, on the extensive information provided as part of their yearly disclosure or self-assessment reports under the CPSS-IOSCO Principles for financial market infrastructures (PFMI) in order to demonstrate compliance with the CSDR. We recognise that the CSDR authorisation process will be

[2] See http://www.ecsda.eu/position_papers.html
[3] See http://www.ecsda.eu/joint_papers.html

a one-off exercise, separate from the ongoing supervisory assessment of CSDs, but we also believe that existing assessments and disclosure reports can form a valuable basis for demonstrating compliance with the authorisation requirements under CSDR. Allowing CSDs to refer to, or to re-use part of these existing assessments will not only avoid unnecessary duplications, it will also promote consistency. This is particularly relevant for section F of Annex I (prudential requirements). Alternatively, ESMA could consider allowing competent authorities not to request applicant CSDs to provide information on some of the items listed in in Annex 1 of the ESMA Discussion Paper if these competent authorities are confident that the CSD(s) under their jurisdiction comply with the specified items, based on the outcome of recent supervisory assessments.

More generally, CSDs should be allowed to provide hyperlinks (rather than actual paper copies) of publicly available documents in their application file, as is explicitly mentioned under EMIR technical standards.

In the case of CSD links (section G of Annex I in the ESMA Discussion Paper), it should be possible for CSDs and competent authorities to refer to and to rely on existing link assessments, whenever this is applicable. A complete re-assessment of CSD links for the purpose of CSDR authorisation should be avoided, especially given the resources involved in the exercise, notably as part of the ongoing and upcoming Eurosystem link assessments in preparation for CSDs' migration to T2S. In this context it is also important for ESMA to take into account that CSDs face different timelines in relation to T2S migration.

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

ECSDA agrees with the template proposed in Annex II.

Regarding the practical organisation of documentation exchange and reference numbering, we believe that flexibility is needed and that CSDs and their regulators should be able to build on existing processes or reporting mechanisms, whenever these are compatible with the technical standards. For example, we believe it should be up to the competent authority to keep the reference numbering, taking into account the documents that it already possesses. Any provision of new or updated documents to the competent authority would otherwise require a cumbersome and unnecessary update of the list of the documents.

As an additional argument in favour of sufficient flexibility, we note that CSDs that have a banking licence are subject to a different communication and reporting mechanism with their competent authority. Their application for authorisation under CSDR may therefore re-use some of the elements of the banking authorisation.

3. Conditions for CSD participations in other entities - Article 18

WHAT THE LEVEL 1 REGULATION SAYS:

Article 18(4): "An authorised CSD may only have a participation in a legal person whose activities are limited to the provision of services set out in Sections A and B of the Annex, unless such a participation is approved by its competent authority on the basis that it does not significantly increase the risk profile of the CSD."

WHAT THE LEVEL 2 TECHNICAL STANDARDS SHOULD SPECIFY:

Article 18(5): RTS on "the criteria to be taken into account by the competent authorities to approve participations of CSDs in legal persons other than those providing the services listed in Sections A and

B of the Annex. These criteria may include whether the services provided by that legal person are complementary to the services provided by a CSD, and the extent of the CSD's exposure to liabilities arising from that participation."

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

ECSDA does not agree with all the restrictions suggested by ESMA in relation to CSDs' participations in other entities. We recognise the need for technical standards to ensure that participations in other businesses do not put CSD activities at risk, but we believe that some of the proposed restrictions are not justified and could actually prevent CSDs from strengthening and diversifying their market infrastructure activities, which in fact contribute to reduce the overall business risk for the CSD. In a rapidly changing environment, CSDs are increasingly expected to develop innovative solutions to problems faced by market participants. One way of developing such solutions is for a CSD to establish subsidiaries or to have participations in complementary businesses. In smaller markets in particular, the know-how and capital for building new infrastructure institutions is often concentrated in the existing market infrastructures, such as CSDs. Preventing CSDs from holding participations in new business ventures would in such cases hamper market development or it would force small or mid-size CSDs to create multi-layer capital groups, which would increase their functioning costs without any actual benefits.

On the individual proposals more specifically:

1. **On guarantees:**

ESMA suggests prohibiting CSDs from assuming guarantees leading to unlimited liability and allowing limited liability only where the resulting risks are fully capitalised. ECSDA agrees with ESMA that this requirement is appropriate.

2. **On limiting control:**

The proposed prohibition for CSDs to hold participations where they assume control unless covered by liquid capital is not without problems. First, it is not clear how such a requirement could be implemented in practice. Second, assuming control of an entity in which it holds a participation can be a way for the CSD to better manage the risks resulting from this participation. **ECSDA thus recommends that this requirement should be further clarified and should not prevent CSDs from exercising effective control over subsidiaries when competent authorities are confident that the risks resulting from the activities of the subsidiary are properly managed.**

In the UK for example, Euroclear UK and Ireland (EUI) has some nominee companies as subsidiaries which hold international securities for the purpose of EUI's links, and other nominees companies that hold stamp duty monies. None of these entities have a regulated status given their nature. These are used to reduce risks and are essential to provide EUI's services in a safe and efficient way. EUI fully takes responsibility for the position of these entities in its contracts with participants, otherwise participants would have limited recourse against a nominee company with no substance, which would not be acceptable from a systemic point of view.

Whilst a more flexible approach is needed on the 'control' exercised by CSDs over other entities, ECSDA believes that CSDs could legitimately be expected to take into account the risks related to their participations in other entities in their recovery plan. In fact, we note that such considerations are already

expected of CSDs under global principles[4] and might be further specified in future EU legislation on the recovery of financial infrastructures. **Whereas we support a general requirement for CSDs to include the risks related to their participations in other entities in their recovery plans, we do not think that ESMA should aim to specify further details on the contents and structure of recovery plans, in order not to pre-empt future EU legislation.**

3. **<u>On limiting revenues generated by CSD participations to a certain percentage of total revenues:</u>**

ECSDA does not agree with the proposal to limit revenues from participations to 20% of the overall revenues of the CSD.

First, the proposed threshold appears rather arbitrary and does not take into account the nature of the risks involved in the participations.

Second, such a nominal threshold would be cumbersome to implement, especially given the uncertainty about annual revenues. In practice, a CSD might have revenues different from its initial forecast, and find itself in a difficult situation if the revenues from its participations unexpectedly exceed 20% of its total revenues, thereby forcing it to dispose of its participation, possibly at a loss, at a moment where the extra revenues actually contributes to maintaining the financial strength and resilience of the CSD. Managing a fixed cap on revenues would be difficult for CSDs to manage and could expose them to legal uncertainty in relation to participations. It is unclear whether the calculation of revenues over three years would be sufficient to smoothen eventual negative or positive shocks to the CSD's or the external entity's revenues.

Third and perhaps most importantly, such a restriction would in some cases no longer allow CSDs to outsource the performance of some of their ancillary services (as authorised under Section B of the CSD Regulation, for instance) to a separate entity in which they hold a participation, usually with the aim of reducing the risks stemming from the provision of these services to the CSD core activities. In Denmark for example, VP holds participations in a trustee company and a company that provides different ancillary services to the CSD. A general cap on revenues from participations could require CSDs to insource these additional risks back into the CSD and could thus actually increase the risk profile of the CSD, contrary to the objective of CSDR.

ECSDA is thus convinced that technical standards should not prescribe a fixed cap on revenues from CSD participations. If the ultimate objective of regulators is to ensure that authorised CSD services remain the core and dominant activity of the CSD, then **technical standards should clearly state this principle, e.g. stating that CSDR-authorised services, including when they are performed by a subsidiary of the CSD, should constitute the main source of revenues of a CSD.** Without imposing a quantitative threshold, such a requirement would force national competent authorities to ensure that CSDs' activities remain focused on their role as financial market infrastructure.

4. **<u>On limiting participations to other entities in the securities chain (trading venue, CCP, trade repository):</u>**

ECSDA does not agree with ESMA's proposal, in paragraph 96 of the Discussion Paper, to limit CSD participations to other entities in the securities chain. Indeed, **a CSD can have very legitimate reasons to hold participations in other types of entities which are not directly part of the securities chain, but still offer complementary services to the CSD's activities, such as IT companies or financial**

[4] Recovery of CSDs is covered by the CPSS-IOSCO Principles for financial market infrastructures of April 2012, and further clarifications are to be provided in a follow-up report to the CPSS-IOSCO Consultative Report of August 2013 on the Recovery of financial market infrastructures.

information providers/data vendors. In Norway for instance, VPS holds participations in a network provider and IT company that offers services to management companies for mutual funds. It should also be possible for CSDs to operate a subsidiary offering registrar services (this is for instance the case in Switzerland today, where SIX SIS operates a separate company subsidiary, called SIX SAG Ltd, for share register services). Another good example for such complementary participations that should remain possible are CSD participations in real estate companies which own the offices of the CSD. **ECSDA thus recommends removing the requirement "limiting participations to securities chain" from the draft technical standards. Instead, ESMA should require CSDs to hold participations in entities providing "complementary" services to their CSDR-authorised activities.**

In conclusion, we believe that the following restrictions on CSD participations would be faithful to the spirit and the letter of the Level 1 text of the CSD Regulation, thereby ensuring that CSDs maintain a low risk profile:

1) Prohibiting CSDs from assuming guarantees leading to unlimited liability and allowing limited liability only where the resulting risks are fully capitalised;
2) Requiring competent authorities to ensure that the activities of the entities in which a CSD holds participations are complementary to or support the activities of the CSD;
3) Ensuring that CSDR-authorised services, including when they are performed by a subsidiary of the CSD, constitute the main source of revenues of the CSD;
4) Allowing CSDs to assume control over other entities where such control contributes to a better management of the risks to which the CSD is exposed as a result of these participations;
5) Requiring CSDs to take into account the risks related to their participations in other entities in their recovery plan.

4. Review and evaluation - Article 22(10), (11)

WHAT THE LEVEL 1 REGULATION SAYS:

Article 22(1): "The competent authority shall, at least on an annual basis, review the arrangements, strategies, processes and mechanisms implemented by a CSD with respect to compliance with this Regulation and evaluate the risks to which the CSD is, or might be, exposed or which it creates for the smooth functioning of securities markets.

Article 22(7): "The competent authority shall regularly, and at least once a year, inform the relevant authorities referred to in Article 12 and, where applicable, the authority referred to in Article 69 of Directive xxxx/xxxx/EU [new MiFID] of the results, including any remedial actions or penalties, of the review and evaluation referred to in paragraph 1."

Article 22(8): "When performing the review and evaluation referred to in paragraph 1, the competent authorities responsible for supervising CSDs which maintain the types of relations referred to in points (a), (b) and (c) of the first subparagraph of Article 17(6) shall supply one another with all relevant information that is likely to facilitate their tasks."

WHAT THE LEVEL 2 TECHNICAL STANDARDS SHOULD SPECIFY:

Article 22(10): RTS on "(a) the information that the CSD shall provide to the competent authority for the purposes of the review referred to in paragraph 1;

(b) the information that the competent authority shall supply to the relevant authorities referred to in paragraph 7;

(c) the information that the competent authorities referred to in paragraph 8 shall supply one another."

Article 22(11): ITS on "standard forms, templates and procedures for the provision of information referred to in the first subparagraph of paragraph 10."

Q25: Do you consider the approach outlined above adequate, in particular as regards the scope and frequency of information provision and the prompt communication of material changes? If

not, please indicate the reasons, an appropriate alternative and the associated costs.

ECSDA generally agrees with the proposed approach, and we note that CSDs mostly already provide the information listed in §105 of the Discussion Paper today. That said, we believe that **the notion of "materiality" could be further stressed** to ensure that a CSD's supervisors focus on changes and processes that truly have a potential impact on a CSD's risk profile. We fully support ESMA's statement in §100 of the Discussion Paper that *"authorities should, in a post-crisis context, increase their capabilities of ongoing supervision rather than over-relying on ad-hoc supervision"*. And we note that CSDs will be required under CSDR article 16(3) to *"inform competent authorities without undue delay of any material changes affecting the conditions for authorisation".* Technical standards should thus acknowledge that there is already an efficient ongoing supervisory regime in place, and that additional ad hoc reviews should focus on material changes affecting the CSD's risk profile, without duplicating with the information provided in the context of the ongoing supervisory assessments. Focusing on relevant updates would considerably facilitate the work of competent authorities and thus contribute to the efficiency of the supervision process. ECSDA supports ESMA's intention expressed in § 104 to focus on the quality of the documentation rather than on the quantity and that *"only relevant documents should be provided".* This principle should be clearly reflected in the draft technical standards.

For example, we share the opinion that the minutes of meetings of the management body of the CSD might sometimes provide relevant information in the course of a supervisory review, but this will not generally be the case. Thus we believe that an obligation for CSDs to provide copies of the minutes of meetings of their management body to competent authorities should be sufficient, and that it is not necessary to require all meetings minutes to be provided by CSDs as part of the annual review process.

As for the annual review of CSD's compliance with the regulation, it should rely as much as possible on information already provided by the CSD. CSDs should only be required to provide information where such information is not yet available to the competent authorities. CSDs should for instance not be required to prepare extensive additional reports summarising information that was already sent to the competent authorities.

ECSDA expects that the annual review according to article 22 of CSDR will replace the previous reviews carried out using the ESCB-CESR framework. Given that the CSDR requirements go beyond the former ESCB-CESR standards (they also go beyond the CPSS-IOSCO Principles for financial market infrastructures), ECSDA considers that the former, non-binding, ESCB-CESR standards should be discontinued once they have been replaced by binding technical standards assessing CSD's compliance with the CSDR requirements.

The annual review exercise should also leverage as much as possible on CSDs' assessments against the CPSS-IOSCO Principles, which cover most of the information required for the review.

5. Recognition of third country CSDs - Article 25

WHAT THE LEVEL 1 REGULATION SAYS:

Article 25(6): "6. The third country CSD referred to in paragraph 1 shall submit its application for recognition to ESMA.

The applicant CSD shall provide ESMA with all information deemed necessary for its recognition. Within 30 working days from the receipt of the application, ESMA shall assess whether the application is complete. If the application is not complete, ESMA shall set a time limit by which the applicant CSD has to provide additional information.

The competent authorities of the Member States in which the third country CSD intends to provide CSD services shall assess the compliance of the third country CSD with the laws referred to in point (d) of

paragraph 4 and inform ESMA with a fully reasoned decision whether the compliance is met or not within three months from the receipt of all the necessary information from ESMA.
The recognition decision shall be based on the criteria set out in paragraph 4.
Within six months from the submission of a complete application, ESMA shall inform the applicant CSD in writing with a fully reasoned decision whether the recognition has been granted or refused."

WHAT THE LEVEL 2 TECHNICAL STANDARDS SHOULD SPECIFY:
Article 25(12): RTS on "the information that the applicant CSD shall provide ESMA in its application for recognition under paragraph 6".

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

ECSDA agrees with ESMA that *"the definition of the items that a non-EU CSD could provide for EU recognition purposes could be similar to the elements required for the registration of an EU CSD"* and we expect ESMA to further define the necessary adaptations, if any, in technical standards. Indeed, as is the case in EMIR technical standards, we believe that the CSDR technical standards should include a list of all requirements for third country CSDs to apply for recognition.

Unlike in the case of EMIR however, the scope of the third country provisions in the Level 1 text of the CSD Regulation is not entirely clear and could require further clarifications in Level 2 standards. One important difference with EMIR is for instance that CSDR does not provide recognised third country CSDs with an EU 'passport' but rather seems to follow a market-by-market approach.

Furthermore, **the current recognition procedure seems to be designed as a one-off exercise, whereas it should be an ongoing process.** Once a third country CSD is recognised, there should be follow-up arrangements and requirements in place to ensure ongoing supervisory equivalence. ECSDA thus encourages ESMA to adopt a 'dynamic approach' in the technical standards on third country CSDs in order to ensure continued equivalence.

Finally, we believe that ESMA should consider reciprocity in market access. It is well known that many non-EU countries do not share the EU's policy of increasing competition between CSDs and favour instead monopoly provision of CSD services. This difference should be reflected in the recognition and supervision process for third country CSDs to ensure that CSDs can only compete in the EU if the respective EU CSDs can also enter that third country's CSD market.

6. Monitoring tools for the risks of CSDs, responsibilities of key personnel, potential conflicts of interest and audit methods - Article 26

WHAT THE LEVEL 1 REGULATION SAYS:
Article 26(1): "A CSD shall have robust governance arrangements, which include a clear organisational structure with well-defined, transparent and consistent lines of responsibility, effective processes to identify, manage, monitor and report the risks to which it is or might be exposed, and adequate remuneration policies and internal control mechanisms, including sound administrative and accounting procedures."
Article 26(3): "A CSD shall maintain and operate effective written organisational and administrative arrangements to identify and manage any potential conflicts of interest between itself, including its managers, employees, members of the management body or any person directly or indirectly linked to them, and its participants or their clients. It shall maintain and implement adequate resolution procedures whenever possible conflicts of interest occur."
Article (6): "A CSD shall be subject to regular and independent audits. The results of these audits shall

be communicated to the management body and made available to the competent authority and, where appropriate taking into account potential conflicts of interest between the members of the user committee and the CSD, to the user committee."

WHAT THE LEVEL 2 TECHNICAL STANDARDS SHOULD SPECIFY:
Article 26(8): RTS on:
(a) "the monitoring tools for the risks of the CSDs referred to in paragraph 1, and the responsibilities of the key personnel in respect of those risks"
(b) "the potential conflicts of interest referred to in paragraph 3"
(c) "the audit methods referred to in paragraph 6 at the CSD level as well as at the group level and the circumstances in which it would be appropriate, taking into account potential conflicts of interest between the members of the user committee and the CSD, to share audit findings with the user committee in accordance with paragraph 6."

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

(a) Monitoring tools and responsibilities of key personnel:

- **Monitoring tools**

ECSDA does not agree with the proposal made by ESMA in §110 of its Discussion Paper which would require CSDs to monitor not only their own risks, but also to the risks they pose to participants and other entities. This is not consistent with and goes beyond Article 26(1) in the Level 1 text of the CSD Regulation, which requires CSDs to *"identify, manage, monitor and report the risks to which it is or might be exposed".*
Besides, it is not clear how a CSD would be able to identify, manage, monitor and report risks in relation to participants' clients. In our view, it is the responsibility of the respective participant to assess and manage the risks in relation to its clients.
Therefore we recommend that **technical standards on monitoring tools should be limited to the risks faced by CSDs.**

- **Responsibilities of key personnel**

ECSDA agrees with the lists of responsibilities of key personnel suggested by ESMA.

However, we would like ESMA to bring some clarifications to the **notion of "dedicated functions"**. Indeed, the requirement to have several dedicated functions (chief risk officer, compliance officer, chief technology officer and independent internal audit) should be interpreted flexibly taking into account the principle of proportionality, given that **such functions will not always justify a full-time job in smaller organisations**. In many CSDs today, the Legal Counsel of the CSD acts as Compliance Officer, for instance. This should continue to be allowed in the future. Similarly, in corporate groups, a single employee often fulfils one of the "dedicated functions" for the entire group, or for different entities within the group. This should continue to be allowed in the future, especially because:

- It allows for a more efficient allocation of tasks and, in the case of corporate groups for instance, provides some benefits (e.g. group-wide perspective on risks);
- Among the 31 CSDs established in the EEA that are members of ECSDA, 21 have less than 100 employees, and among these 12 have less than 50 employees. For such CSDs, it could prove impossible to attract a sufficiently qualified employee for performing the "dedicated

functions" if the function is not combined with other functions.

As a result**, technical standards should make it clear that the "dedicated functions" should be clearly attributed to an individual, but that this individual should be allowed to perform other functions, as long as any potential conflicts of interests are disclosed and managed**, according to the relevant provisions of CSDR.

(b) Potential conflicts of interest:

ECSDA generally agrees with ESMA's approach on conflicts of interest but we think that some clarifications are required as regards the examples listed in §116 of the Discussion Paper. The list provided is indeed quite extensive and could give rise to somewhat excessive interpretations. For example, the mere fact of holding shares in a publicly listed company that is also a client or a partner firm of the CSD does not necessarily entail a conflict of interest. CSDs typically work with many large listed companies, and prohibiting every CSD employee to hold shares in such companies would clearly be excessive. **The focus should be on material holdings in companies having a business relationship with the CSD, which might in some cases give rise to a conflict of interests.** Targeting the 'real' conflicts of interest is all the more important since CSDs will be legally required to *"maintain and operate effective written organisational and administrative arrangements to identify and manage any potential conflicts of interest".*

ECSDA also expects that not all conflicts of interests identified by the CSD will need to be 'managed' (e.g. requiring special adaptations or procedures), and that in many cases disclosure of such potential conflicts of interest will suffice.

(c) Audit methods:

ECSDA generally agrees with §119 of the Discussion Paper which stresses the importance of an independent internal audit function. We insist, however, that the notion of an 'independent and separate" internal audit function should be applied proportionately, taking into account that **it should be allowed for smaller CSDs to combine the internal audit function with other functions, as long as a sufficient degree of independence is guaranteed** (see also our comments on "dedicated functions" under point b) above).

We recommend that independent audits should be planned and performed on a risk-based approach following a cyclical approach so that all processes are audited at least every 3 to 5 years.

As for the use of external auditors to assess and 'audit' the internal audit function on a yearly basis (§120 and 121 of the Discussion Paper), ECSDA would like to express three concerns:

- First, the meaning of Article 26(6) in the Level 1 text of CSDR is not entirely clear. The article only states that CSDs shall be *"subject to regular and independent audits".* Given that the results of such audits might have to be communicated, in certain cases, to the user committee of the CSD, ECSDA had assumed that the Level 1 text was referring to an audit of CSD's financial statements by an external auditor.
- Second, if the intention of the legislator is indeed to require by law that a 'risk audit' be performed by an external auditor, in addition to the annual audit of the accounts, a proportionate approach needs to be adopted, given the important differences among CSDs as regards the size and complexity of their business. Such external audits will represent an additional cost for CSDs, and will come on top of existing supervisory assessments, financial audits and internal audit assessments.
- Third, we note that Question 27 of the Discussion Paper seems to invert the logic of the CSDR Level 1 text by asking for cases where the sharing of audit results with the user committee would not be appropriate. The question seems to assume that, by default, CSDs should share these results with the user committee, whereas the Level 1 text mandates ESMA to specify the *"circumstances in which it would be appropriate (...) to share audit findings with the user committee".* ECSDA believes that 'risk' audits, unlike financial audits, are likely to contain non-

public information on detailed risk management processes and procedures which are not meant to be disclosed outside the CSD and its regulator(s). For example, it is conceivable that such audits could contain information on the risks posed by a specific client of the CSD, or by very specific services, and such information should clearly remain confidential. This is especially true given the competitive environment in which CSDs operate and the fact that CSD participants are also often competitors to the CSD for the provision of certain services.

As a result, subject to the confirmation by the EU legislator that the Level 1 text truly intends to require an external audit of a CSD's internal risk management processes – and not only of the CSD's financial statements, ECSDA recommends the adoption of a proportionate approach to cater for the situation of smaller CSDs, as well as a description, in the technical standards, of the limited number of cases where the audit results could be provided to the user committee, taking into account potential conflicts of interest and confidentiality requirements.

Finally, when specifying CSDR audit requirements, ESMA should take into account that CSDs operating with a banking licence are already subject to extensive audit requirements under CRD IV. Duplications and inconsistencies between both sets of requirements should be avoided.

7. Recordkeeping - Article 29(3), (4)

WHAT THE LEVEL 1 REGULATION SAYS:
Article 29(1): "A CSD shall maintain, for a period of at least ten years, all the records on the services and activity provided, including on the ancillary services referred to in Sections B and C of the Annex, so as to enable the competent authority to monitor the compliance with the requirements under this Regulation."

WHAT THE LEVEL 2 TECHNICAL STANDARDS SHOULD SPECIFY:
Article 29(3): RTS on "the details of the records referred to in paragraph 1 to be retained for the purpose of monitoring the compliance of CSDs with the provisions of this Regulation."
Article 29(4): ITS on "the format of the records referred to in paragraph 1 to be retained for the purpose of monitoring the compliance of CSDs with the provisions of this Regulation."

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

- **"Minimum requirements" approach**

ECSDA does not agree with the "minimum requirements" approach proposed by ESMA for CSD recordkeeping and believes a different approach that ensures truly harmonised standards and a level playing field for CSDs would be more appropriate.

A minimum requirements approach could result in some national regulators 'gold-plating' the ESMA list and adding additional requirements, thereby introducing distortions among CSDs. Instead, we suggest that ESMA should follow whenever possible a "maximum requirements" approach, providing a harmonised list of records while giving some flexibility to competent authorities not to require records that are not relevant for the particular CSD.

That said, we recognise that there will be cases where a need is identified for regulators to have access to certain information that is not part of regular recordkeeping. In such cases, competent authorities should retain the possibility to request CSDs to keep and provide such information, but such requests will typically have a different justification and other purposes than assessing CSDR compliance.

- **Contents of the recordkeeping requirements**

The list of items in Annex III of the Discussion Paper is very extensive and goes far beyond what is required by regulators today. In fact, based on our understanding of ESMA's current proposal, the quantity of data to be stored over (a minimum of) 10 years and related functionalities would result in **potentially huge IT costs**, as it would require many CSDs to build an entirely new IT system, or at least to substantially overhaul their existing systems. Indeed some of the proposed technical requirements, such as an online inquiry possibility, the possibility to re-establish operational processing, a query function through numerous search keys, and direct data feeds, are much more demanding than current CSD recordkeeping practices. Adapting to these requirements would require a combined investment of tens of millions of euros for ECSDA members.

Moreover, for CSDs participating in T2S in particular, having to develop a parallel system outside T2S will create a lot of complexity while negatively impacting the cost efficiencies generated by the use of a single, centralised platform for all T2S markets. We thus believe that the requirements being proposed by ESMA are disproportionate, and go beyond what is necessary to ensure effective supervision.

Most importantly, we believe that the purpose of recordkeeping requirements, as specified in CSDR Article 29, is to allow supervisory authorities to ensure *"compliance [of the CSD] with the requirements under this Regulation."* The objective is not and should not be to:

- Use CSDs as trade repositories, to retrieve market data at individual transaction/instruction level, and obtain details on activities of individual CSD clients;
- Use these records as a way to 'recover' CSD activities in case of financial or operational failures.

Recordkeeping should thus be understood in the light of supervisors' assessment of CSDs' compliance with CSDR, and should be distinct from considerations on trade repository services or recovery and resolution plans. For CSDs, recordkeeping is essentially about data retention and archiving in order to be able to reply to inquiries by competent authorities.

In particular, we are not aware of any specific problems or complaints by regulators as regards the current level of detail of the records stored by CSDs. The rationale behind the far-reaching requirements being proposed by ESMA is thus difficult to understand, and ECSDA sees very limited added value in keeping an unnecessarily heavy amount of data, especially given the **burden it will impose on regulators themselves**, when making use of the data.

As a result, we believe that the list of records contained in Annex III of the Discussion Paper should be significantly shortened. Many of the items in the proposed list generally do not seem relevant for the purpose of ensuring compliance with CSDR. At a minimum, the following items should be removed from the list:

SR3	Persons exercising control on Issuers
SR4	Country of establishment of persons exercising control on issuers
SR13	Persons exercising control on Participants
SR14	Country of establishment of persons exercising control on Participants
FR3	Client of the delivering participant, where applicable
FR9	Client of the receiving participant, where applicable

CSDs typically do not have access to such information and it is unclear how such records would contribute to evidence CSD's compliance with CSDR requirements.

CSDR technical standards should take into account the fact that some of the listed records are linked to the provision of specific services which not all CSDs might offer. CSDs that do not

provide certain services should naturally not be expected to keep the corresponding records. In this context, we welcome the more flexible approach adopted by ESMA on records in relation to ancillary services (§126). However, we would like to recall that the definition of a CSD in Article 2 of CSDR does not require CSDs to provide all three core services, but only two out of the three. Hence, recordkeeping requirements will need to take this into consideration. Actual data available to the CSD will depend on its service offering and the data required for its operational processes. The recordkeeping requirements will thus have to be adapted depending on the individual services provided by a given CSD based on the list of services contained in sections A, B and C of the Annex of the CSD Regulation.

Regarding point iii) under §128 of the Discussion paper stating that *"it is not possible for the records to be manipulated or altered"*, we suggest that ESMA should clarify that the prohibition to alter records applies to transaction data. For other records and static data, it should be possible for the CSD to make changes, albeit with a strict track record of the amendments made.

Estimated costs for implementing the current ESMA proposals on recordkeeping:

Based on data collected from 18 EU CSDs (out of a total of 33), ECSDA has attempted to estimate the direct costs of implementing the requirements suggested by ESMA in its Discussion Paper. These estimates do not take into account the potential costs for regulators (e.g. in handling the required records) and for market participants (e.g. in case the use of LEI would be required). We distinguish between (a) one-off development costs, primarily to build the system required to be able to fulfil ESMA requirements (including the use of a non-proprietary format, LEIs and a direct data feed access for regulators); (b) and annual running costs, to maintain the system.

A. One-off costs

The total estimated system development costs for all 18 CSDs in the sample are considerable, ranging between EUR 41.3 million and EUR 62.4 million (depending on the final specifications of the requirements and other factors)**.** In terms of average costs per CSD, this would mean EUR 2.3 million to EUR 3.5 million.

Understandably, individual costs differ substantially across CSDs, partly due to differences in current system specifications. However, for most CSDs, the highest development costs would result from the mandatory use of a non-proprietary format and of LEIs. For example, based on the cost figures provided, we estimate that it could cost over EUR 500,000 for a small to mid-size CSD to upgrade its system to allow for the use of LEIs. For a larger CSD, the cost would most certainly exceed EUR 1 million. The cost of developing a direct data feed for regulators would generally be lower but could still reach over EUR 500,000 for some CSDs.

Overall, ECSDA estimates that development costs could be considerably reduced if CSDs would be allowed to store the required records in proprietary format (while providing for this format to be 'converted' to an international format upon request) and if LEIs would not be required.

B. Running costs

The total estimated annual running costs for all 18 respondent CSDs are between EUR 11.1 million and EUR 13.7 million. On average, this translate into annual running costs per CSD from EUR 600,000 to EUR 800,000.

C. Overall costs

Given that the aggregated figures above are based on a broadly representative sample of CSDs, we can derive from the average figures the following total estimated costs for the **entire CSD sector in the EEA** (33 EEA CSDs):
Total estimated system development costs for all 33 EEA CSDs: EUR 75.7 Mio – EUR 114.3 Mio
Total estimated annual running costs for all 33 EEA CSDs: EUR 20.3 Mio – EUR 25.0 Mio

D. Timing and human resources

It is also worth noting that, besides the pure monetary costs of building and maintaining a system to support the proposed ESMA requirements on recordkeeping, CSDs would require sufficient time to implement these requirements, and would face a considerable challenge in mobilising the required human resources.

Should ECSDA maintain all the requirements proposed in its Discussion Paper, ECSDA estimates that **CSDs would need on average slightly more than 14 months in order to fully comply with the recordkeeping rules.**

- **Format of the records**

As regards the format of the records to be stored, we think it is not necessary (and indeed sometimes not possible) to require CSDs to maintain records online (immediately available) but that **it should be sufficient to store the data offline as long as this data can be retrieved within a few days.** This is a much more practical approach, considering the high amount of data involved.

ECSDA also cautions against imposing the use of open, non-proprietary standards for recordkeeping purposes. Such a requirement would entail huge costs and would require significant changes to CSDs' system. Instead, **ESMA should allow CSDs to maintain records in a proprietary format wherever this format can be converted without undue delay into an open format that is accessible to regulators.**

- **Timing of implementation**

Depending on the final recordkeeping requirements to be included in the CSDR technical standards, CSDs might have to make considerable investments to build and maintain the relevant IT systems, and such developments are likely to take months to implement. This could mean that **it will be close to impossible for most CSDs to comply with the recordkeeping requirements by the time they apply for authorisation under CSDR.** ESMA should consider such a constraint and determine an appropriate transition period to allow CSDs to develop the required functionalities.

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

- **Direct data feeds for regulators**

ECSDA does not believe that technical standards should require CSDs to build and maintain direct data feeds for their competent authorities, and we wonder whether such a measure might not exceed the mandate granted to ESMA under the Level 1 Regulation. In addition to the cost considerations, it is questionable whether regulators will truly make use such data feeds, and it is far from certain that such type of data exchange would present significant advantages compared to a situation where CSDs provide data promptly to regulators upon request. The use of direct data feeds is currently limited to a few countries and experience suggests that regulators tend to continue to rely on ad hoc requests for information to the CSD, even when they can access the data directly, because the latter is often more convenient.

- **Use of LEI**

ECSDA does not believe that CSDs should be required to use global Legal Entity Identifiers (LEI) in their records. Such identifiers are not currently in use at CSD level, and their implementation has been

limited so far to OTC derivatives markets, where CSDs are typically not involved. Imposing the use of LEIs for the purpose of recordkeeping is unlikely to bring any substantial benefits. As mentioned earlier, CSD recordkeeping requirements should not result in regulators transforming CSDs into trade repositories. Imposing the compulsory use of LEI would require costly changes to current CSD systems and would also increase costs for CSD participants (who would subsequently be required to adapt their systems as well). Such a requirement would also exceed the Level 1 mandate under Article 29 of CSDR.

Moreover, there are specific challenges for direct holding markets that need to be carefully considered. If the requirement to use LEIs were to include all account holders at these CSD, this could encompass several hundred thousand companies. Beyond imposing significant administrative costs on these companies, such a requirement would go against the principle, stated in the CSD Regulation, of neutrality in relation to different account holding models in Europe. The same general reasoning would apply if the requirement were to include issuers, most of which do not use LEI today.

Without denying the benefits linked to the use of LEIs in terms of harmonisation, ECSDA believes that CSDR technical standards on recordkeeping are clearly not the right place to promote their wider use. More analysis is needed, and a gradual implementation of LEIs outside derivatives markets should be coordinated at global level, rather than being imposed on EU CSDs via binding regulation.

8. Refusal of access to participants - Article 33(5), (6)

WHAT THE LEVEL 1 REGULATION SAYS:
Article 33(3): "A CSD may only deny access to a participant meeting the criteria referred to in paragraph 1 where it is duly justified in writing and based on a comprehensive risk analysis.
In case of refusal, the requesting participant has the right to complain to the competent authority of the CSD that has refused access.
The responsible competent authority shall duly examine the complaint by assessing the reasons for refusal and shall provide the requesting participant with a reasoned reply.
The responsible competent authority shall consult the competent authority of the place of establishment of the requesting participant on its assessment of the complaint. Where the authority of the requesting participant disagrees with the assessment provided, any one of the two competent authorities may refer the matter to ESMA, which may act in accordance with the powers conferred on it under Article 19 of Regulation (EU) No 1095/2010.
Where the refusal by the CSD to grant access to the requesting participant is deemed unjustified, the responsible competent authority shall issue an order requiring that CSD to grant access to the requesting participant."

WHAT THE LEVEL 2 TECHNICAL STANDARDS SHOULD SPECIFY:
Article 33(5): RTS on "the risks to be taken into account by CSDs when carrying out a comprehensive risk assessment, and competent authorities assessing the reasons for refusal in accordance with paragraph 3 and the elements of the procedure referred to in paragraph 3."
Article 33(6): ITS on "forms and templates for the procedure referred to in paragraph 3."

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

ECSDA broadly agrees with ESMA's proposal as regards the type of risks that need to be taken into consideration in the risk analysis when justifying the refusal of an applicant participant by a CSD. A distinction of legal, financial and operational risks is reasonable. The examples provided by ESMA for each category are helpful indications, but they should not be considered as an exhaustive list.

As regards legal risks and the third example listed by ESMA under §137(a) of the Discussion Paper, it is important to clarify that CSDs cannot be expected to assess whether *"the requesting party is not compliant with prudential requirements"*, and that they **should be allowed to rely on the existing authorisations obtained by the requesting party.** For example, an institution authorised to operate as a credit institution is deemed to comply with the prudential requirements applicable to banks in its jurisdiction, and the CSD, not being a banking supervisor, is not in a position to make a judgement on the compliance of that credit institution with applicable rules.

Furthermore, it is important to keep in mind that the 'risk analysis' mentioned in Article 33(3) of CSDR is only required in cases of refusal. In principle, this means that CSDR technical standards should not impact the procedure followed by CSDs when approving a new participant. In other words, the criteria for refusal provided by ESMA, which are 'negative' criteria (on what is not acceptable for obtaining the status of CSD participant) should not be interpreted as a substitute for the regular approval process for CSD participants based on 'positive' participation criteria specified by each CSD. Considering the criteria to be specified in CSDR technical standards under Article 33(5) as a basis for the initial assessment of applicant-participants would be misguided, and would result in a more complex and lengthy approval process for CSD participants. Instead, it should be clear that the technical standards are limited to exceptional cases where the CSD has doubts on the eligibility of an applicant-participant.

ECSDA would also like ESMA to ensure that the future CSDR technical standards do not prevent corporates (i.e. non-financial institutions) to be accepted as CSD participants, when applicable (for example corporates making use of CSD services in the repo market).

Finally, we note that in some cases specific participation criteria are determined by national law. In France, for instance, only custodian banks authorised as "*teneurs de comptes-conservateurs*" are legally eligible as participants in the CSD. In other countries, the CSD regulator has to confirm its approval of new CSD participants. As a result, it will be important to avoid contradictions between CSDR technical standards and national rules on CSD participation. We assume that the current national rules will need to be adapted in line with the new technical standards.

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

Yes, ECSDA agrees with the proposed time frames.

9. Integrity of the issue - Article 37

WHAT THE LEVEL 1 REGULATION SAYS:

Article 37(1): "A CSD shall take appropriate reconciliation measures to verify that the number of securities making up a securities issue or part of a securities issue submitted to the CSD is equal to the sum of securities recorded on the securities accounts of the participants of the securities settlement system operated by the CSD and, where relevant, on owner accounts maintained by the CSD. Such reconciliation measures shall be conducted at least daily."

Article 37(2): "Where appropriate and if other entities are involved in the reconciliation process for a certain securities issue, such as the issuer, registrars, issuance agents, transfer agents, common depositories, other CSDs or other entities, the CSD and any such entities shall organise adequate cooperation and information exchange measures with each other so that the integrity of the issue is maintained."

Article 37(3): "Securities overdrafts, debit balances or securities creation shall not be allowed in a securities settlement system operated by a CSD."

WHAT THE LEVEL 2 TECHNICAL STANDARDS SHOULD SPECIFY:
Article 37(4): RTS on "reconciliation measures a CSD shall take under paragraphs 1 to 3."

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

ECSDA is not convinced that an extra reconciliation measure, consisting in comparing the previous end of day balance with all settlements made during the day and the current end-of-day balance, should be included in CSDR technical standards. We understand that ESMA's proposal would be aligned with T2S requirements, but we are not convinced that similar requirements should be imposed outside the scope of T2S.

Given the complexity and technicality of the issue, we believe that further discussions are necessary on this issue, with ESMA but also with the ECB, to find a suitable balance and avoid inconsistencies between the CSDR, T2S and the Eurosystem assessment framework ("User addendum" of January 2014[5]).

As regards §144 of the Discussion Paper, ECSDA does not fully understand the case raised by ESMA. Preventing settlements in case of a reconciliation issue is a measure that entails important risks for market participants and the CSD.

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

No, ECSDA does not see the need for special reconciliation measures in case of corporate actions. In fact, standard reconciliation procedures of CSDs already cover corporate actions, and we are not sure why a specific treatment for corporate actions is being considered by ESMA.

We would also like to point out that, in the case of dividend payments, for example, the issuer or its agent, rather than the CSD, is legally responsible for the reconciliation of individual payments with individual shareholders.

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

Yes, ECSDA agrees that double-entry accounting gives CSDs a sufficiently robust basis to avoid securities overdrafts, debit balances and securities creation.
We do not think that CSDR technical standards should specify other measures.

10. Operational risks - Article 45

WHAT THE LEVEL 1 REGULATION SAYS:
Article 45(1): "A CSD shall identify sources of operational risk, both internal and external, and minimise their impact through the deployment of appropriate IT tools, controls and procedures, including for all

[5] www.ecb.europa.eu/pub/pdf/other/frameworkfortheassessmentofsecuritiessettlementsystems201401en.pdf

the securities settlement systems it operates."
Article 45(3): "For services it provides as well as for each securities settlement system it operates, a CSD shall establish, implement and maintain an adequate business continuity policy and disaster recovery plan to ensure the preservation of its services, the timely recovery of operations and the fulfilment of the CSD's obligations in the case of events that pose a significant risk of disrupting operations."
Article 45(4): "The plan referred to in paragraph 3 shall provide for the recovery of all transactions and participants' positions at the time of disruption to allow the participants of a CSD to continue to operate with certainty and to complete settlement on the scheduled date, including by ensuring that critical IT systems can promptly resume operations from the time of disruption. It shall include the setting up of a second processing site with sufficient resources, capabilities, functionalities and appropriate staffing arrangements."
Article 45(6): "A CSD shall identify, monitor and manage the risks that key participants to the securities settlement systems it operates, as well as service and utility providers, and other CSDs or other market infrastructures might pose to its operations. It shall, upon request, provide competent and relevant authorities with information on any such risk identified.
It shall also inform the competent and relevant authorities without delay of any operational incidents resulting from such risks."

WHAT THE LEVEL 2 TECHNICAL STANDARDS SHOULD SPECIFY:
Article 45(7): RTS on "the operational risks referred to in paragraphs 1 and 6, the methods to test, address or minimise those risks, including the business continuity policies and disaster recovery plans referred to in paragraphs 3 and 4 and the methods of assessment thereof."

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

ECSDA agrees with the definition proposed by ESMA and considers it sufficient. We fully support referring to the definition of operational risk included in the CPSS-IOSCO Principle for financial market infrastructures as we believe this will guarantee consistency with global standards.

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

ECSDA does not think that additional requirements or details are necessary, given the already detailed provisions included in the CPSS-IOSCO Principle for financial market infrastructures and their assessment methodology[6]. We welcome ESMA's approach, which is based on these Principles, but we think clarifications are required on the following issues:

Paragraph in the ESMA Discussion Paper	**Clarifications required**
§154: CSDs should have a *"robust operational risk-management framework with appropriate IT systems, policies, procedures and controls".*	This principle should not be understood as a requirement for CSDs to use special IT tools for operational risk management. There exist some third party IT solutions for managing operational risk but they are not commonly used by CSDs and are not necessarily more appropriate than, or superior to, the established tools and systems for managing operational risk management within CSDs. This is especially true for

[6] Other sources for standards on the management of operational risk include the Eurosystem Business continuity oversight expectations for systemically important payment systems and the High-level principles for business continuity, of the Joint Forum of the Basel Committee on Banking Supervision, among others.

	CSDs not exposed to credit risk.
§157: *"The CSD should have a central function for managing operational risk".*	ECSDA agrees with ESMA's statement but wishes to stress that a 'central function' should be understood as a requirement that responsibilities for the management of operational risks are clearly attributed, not as a requirement for the function to be performed by a CSD employee on an exclusive basis, especially in smaller CSDs (see our answer to question 27 on the responsibilities of key personnel).
§160: The CSD *"should also have comprehensive and well-documented procedures in place to […] resolve all operational incidents"*	ECSDA suggest rephrasing the end of the sentence as follows: *"all **material** operational incidents"* in order to ensure a reasonable and proportional interpretation. The mentioned procedures should not be required for insignificant incidents that do not affect in any way the efficient functioning of a CSD system.
§161: *"The operational risk management processes […] should be subject to regular reviews performed by internal or external auditors".*	ECSDA considers that the review of operational risk management processes will typically be undertaken by the internal auditor, rather than an external auditor (see also our response to question 27 on audit methods).

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

Yes, ECSDA believes that the ESMA proposal is sufficient.

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

ECSDA does not agree with the ESMA proposal, in §167 of the Discussion Paper, to make mandatory an annual yearly review of the IT system(s) and IT security framework of all CSDs. Indeed we believe that the proposed (annual) frequency is excessive, and we think that such reviews should be applied with the 'proportionality' principle in mind, especially given the high amount of resources involved in such annual reviews. A frequency of 3 to 5 years for such reviews appears more appropriate.

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

Requirements imposed on CSDs for a secondary processing site illustrate the importance of a proportional and targeted approach. The meaning of a *"geographically distinct risk profile"* will necessarily depend on local conditions and cannot be defined in an overly prescriptive way, for instance specifying an exact minimum distance. The focus should be on risks, in particular the likelihood of natural disasters. The geographical distance between the first and second processing sites of CSDs today differs considerably. Such decision involves, in particular for smaller CSDs, a trade-off between risk considerations and the quality of the services that can be provided in the secondary site (which partly depends on the possibility to quickly transfer part of the employees from one site to the other). Because such considerations require knowledge of the local geographic and market conditions, ECSDA believes that technical standards should leave some room for local regulators to apply the requirements appropriately.

In line with the single market objective of CSDR, **ECSDA recommends that technical standards**

foresee the possibility for a CSD to set up a second processing site in different Member State (than its home member state). While such a solution will only be appropriate in a limited number of cases, it could have merit for CSDs belonging to multinational corporate groups, especially as integration of European financial markets deepens in the future. We also believe that technical standards should not prevent a CSD from outsourcing the operation of a secondary site to another legal entity, provided solid and adequate contractual arrangements are in place.

Furthermore, ESMA should be aware that CSDR technical standards on operational risk are likely to require some CSDs to amend their policy on the use of their secondary processing site. **In case one or more EU CSDs find themselves in a situation where they have to set up a new secondary processing site in order to comply with CSDR technical standards, it is important that this CSD is given a sufficient time to implement the required changes, i.e. at least 6 months after the entry into force of the technical standards.** This is unavoidable given the important financial and operational resources involved in such projects.

Finally, on §168, we would like to note that T2S currently foresees a maximum recovery time of **4 hours** for critical CSD functions, and not 2 hours as suggested by ESMA in the third bullet point.

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

Yes, ECSDA agrees that the requirements proposed by ESMA form a good basis for identifying, monitoring and managing the risks that key participants, utility providers and other FMIs pose to the operations of the CSDs.

11. Investment policy - Article 46

WHAT THE LEVEL 1 REGULATION SAYS:
Article 46(1): "A CSD shall hold its financial assets at central banks, authorised credit institutions or authorised CSDs."
Article 46(2): "A CSD shall have prompt access to its assets, when required."
Article 46(4): "The amount of capital, including retained earnings and reserves of a CSD which are not invested in accordance with paragraph 3 shall not be taken into account for the purposes of Article 44(1)"

WHAT THE LEVEL 2 TECHNICAL STANDARDS SHOULD SPECIFY:
Article 46(6): RTS on
(a) "the financial instruments that can be considered as highly liquid with minimal market and credit risk as referred to in paragraph 1"
(b) "the appropriate timeframe for access to assets referred to in paragraph 2"
(c) "the concentration limits as referred to in paragraph 5".
"Such draft regulatory technical standards shall where appropriate be aligned to the regulatory technical standards adopted in accordance with Art. 47(8) of Regulation No 648/2012 (EMIR)."

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

ECSDA agrees with the proposed approach. We would like to stress, however, that unlike CCPs, CSDs do not use their capital to guarantee clearing, and that restrictions on their investment policy thus do not necessarily need to be as strict as the EMIR requirements. In practice, CSDs typically have a limited

amount of capital to invest and generally keep that capital in cash deposits.

We agree with ESMA that a distinction between CSD providing banking services and other services can be relevant for the purpose of determining rules on investment policy. For CSDs with a banking licence, the investment of their capital will generally be a function of the management of their liquidity risk and will therefore fall under the scope of CSDR Article 59. It will thus be important that the technical standards proposed by ESMA under CSDR Article 46 do not override those that will be developed by EBA on CSDR Article 59.

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

No. Given the relatively low level of capital of CSDs, resulting from their low risk profile, additional rules do not seem proportionate. For CSDs having a banking licence and a more extensive capital base, the rules in CSDR article 59 should prevail.

On the proposals made by ESMA in relation to the definitions, we would like to stress, as noted previously, that many EMIR requirements are not appropriate for CSDs.

For example, we understand that EMIR requires CCPs to develop their own methodology for credit ratings instead of relying on ratings from external credit agencies for the purpose of determining whether a credit institution has a low credit risk, and is thus eligible to hold CCP assets. ECSDA would like ESMA to clarify that CSDs should be allowed, as an alternative to internal evaluations, to use credit ratings from external agencies for the purpose of managing their investment risk, given that unlike CCPs they are usually not involved in managing credit risks.

Likewise, concentration limits often do not seem appropriate for CSDs with only very limited capital, especially since such capital is typically mostly invested in cash. One solution, for example, could be for ESMA to specify a *de minimis* threshold in relation to the CSD's capital level below which concentration limits are not necessary.

Besides, ECSDA does not fully agree with ESMA's statement, in §182 of the Discussion Paper, that *"CSDs should not be allowed, as principle, to consider their investment in derivatives to hedge their interest rate, currency or other exposures."*
In some cases it should be possible for CSDs to hedge against interest rate or currency risk, for example. This is certainly needed for CSDs with a banking licence. We do not consider the use of the instruments for hedging as "investments".

Finally, we would like to suggest an amendment to §181 of the Discussion Paper. We do not think that point (ii) which states that CSDs should not invest in debt instruments with *"an average duration greater than two years until maturity",* is appropriate. Indeed, the average duration until maturity of debt instruments has in many cases no influence on the liquidity of the instrument. In fact, the liquidity of debt instruments with an average duration of more than 2 years until maturity is not generally lower than for shorter-dated instruments. **We thus recommend removing point (ii) from the list of criteria.**

Regarding eligible debt instruments, we note that existing EMIR technical standards do not specify the concrete category of highly liquid debt instruments, but lists a set of conditions to be considered (Annex II of EC delegated regulation 153/2013). In particular, debt instruments can be considered highly liquid and with minimum market and credit risk where *"the CCP can demonstrate that they have low credit and market risk based upon an internal assessment by the CCP. In performing such assessment the CCP shall employ a defined and objective methodology that shall not fully rely on external opinions and that takes into consideration the risk arising from the establishment of the issuer in a particular country".*
We believe that the same approach should be followed for CSDs provided that they can rely on an

external methodology (in line with our comments above).

12. CSD links - Article 48(10)

WHAT THE LEVEL 1 REGULATION SAYS:
Article 48(3): "A link shall provide adequate protection to the linked CSDs and their participants, in particular as regards possible credits taken by CSDs and the concentration and liquidity risks as a result of the link arrangement.
A link shall be supported by an appropriate contractual arrangement that sets out the respective rights and obligations of the linked CSDs and, where necessary, of the CSDs' participants. A contractual arrangement with cross-jurisdictional implications shall provide for an unambiguous choice of law that govern each aspect of the link's operations."
Article 48(5): "A CSD that uses an indirect link or an intermediary to operate a CSD link with another CSD shall measure, monitor, and manage the additional risks arising from the use of that indirect link or intermediary and take appropriate measures to mitigate them."
Article 48(6): "Linked CSDs shall have robust reconciliation procedures to ensure that their respective records are accurate."
Article 48(7): "Links between CSDs shall permit DVP settlement of transactions between participants in linked CSDs, wherever practical and feasible. Detailed reasons for any CSD link not allowing for DVP settlement shall be notified to the relevant and competent authorities."

WHAT THE LEVEL 2 TECHNICAL STANDARDS SHOULD SPECIFY:
Article 48(10): RTS on
(a) "the conditions as provided in paragraph 3 under which each type of link arrangement provides for adequate protection of the linked CSDs and of their participants, in particular when a CSD intends to participate in the securities settlement system operated by another CSD",
(b) "the monitoring and managing of additional risks referred to in paragraph 5 arising from the use of intermediaries",
(c) "the reconciliation methods referred to in paragraph 6",
(d) "the cases where DVP settlement through CSD links is practical and feasible as provided in paragraph 7 and the methods of assessment thereof."

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

ECSDA fully supports ESMA's approach, which treats standard and customised links equally from a risk perspective. This is in line with the approach taken in the Level 1 Regulation, in particular as regards the authorisation requirements for standard and customised links (Article 19).

We also agree in principle with the conditions for the establishment of standard and customised links. **The term "extensive" in point 3 of §190 is however unnecessary and should be deleted**, at least in relation to CSDs authorised or recognised under the CSDR. Given that the CSDR authorisation procedure is already extensive and covers all the aspects listed in §190, a further 'extensive' reassessment by the CSD itself should not be required. We recognise, however, that a more detailed analysis will usually be required for links with non-ESMA recognised third country CSDs.

Likewise, technical standards should take into account existing CSD link assessments, as performed under the Eurosystem framework, to avoid unnecessary duplication.

Finally, for the sake of consistency, §190 (bullet point 5) should explicitly refer to the *"measures that have been taken to ensure segregation **in line with CSDR article 38** (…)".*

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

Yes, ECSDA agrees that the procedures proposed by ECSDA for 'indirect links' are adequate.

Nonetheless, given that indirect links are not currently subject to such procedures, ECSDA recommends that **ESMA should foresee an additional delay of around 6 months for these requirements to enter into force**. This is because it will be difficult for those CSDs operating many indirect links in and outside Europe to have completed their reassessment all these links based on the new rules by the time they file their application for authorisation.

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

Yes, ECSDA agrees with ESMA's description of reconciliation methods in §196 of the Discussion Paper.

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

Yes, ECSDA agrees with description made by ESMA in §199 of the cases where DvP settlement can be considered practical and feasible.

With regard to §200 of the Discussion Paper, ESMA seems to indicate that both the requesting CSD and the receiving CSD need to offer banking services for DvP settlement to be possible across a link (at least when both CSDs are not in the same currency zone). This would suggest that DVP settlement through links is often only possible in commercial bank money. In practice, it may however be possible to organise DVP settlement in central bank money (mostly when CSDs are in the same currency zone) without the CSD offering cash accounts and services (e.g. like in T2S). In such cases, the considerations in §200 would not be applicable.

13. Refusal of access to issuers - Article 49(5), (6)

WHAT THE LEVEL 1 REGULATION SAYS:

Article 49(3): "A CSD may refuse to provide services to an issuer. Such refusal may only be based on a comprehensive risk analysis or if that CSD does not provide the services referred to in point 1 of Section A of the Annex in relation to securities constituted under the corporate law or other similar law of the relevant Member State."

Article 49(4): "Without prejudice to [insert references to AML directive], where a CSD refuses to provide services to an issuer, it shall provide the requesting issuer with full written reasons for its refusal.

In case of refusal, the requesting issuer shall have a right to complain to the competent authority of the CSD that refuses to provide its services.

The competent authority of that CSD shall duly examine the complaint by assessing the reasons for refusal provided by the CSD and shall provide the issuer with a reasoned reply.

The competent authority of the CSD shall consult the competent authority of the place of establishment of the requesting issuer on its assessment of the complaint. Where the authority of the place of establishment of the requesting issuer disagrees with that assessment, any one of the two competent authorities may refer the matter to ESMA, which may act in accordance with the powers conferred on it under Article 19 of Regulation (EU) No 1095/2010.

Where the refusal by the CSD to provide its services to an issuer is deemed unjustified, the responsible competent authority shall issue an order requiring the CSD to provide its services to the requesting issuer."

WHAT THE LEVEL 2 TECHNICAL STANDARDS SHOULD SPECIFY:
Article 49(5): RTS on "the risks to be taken into account by CSDs when carrying out a comprehensive risk assessment, and competent authorities assessing the reasons for refusal in accordance with paragraphs 3 and 4, the elements of the procedure referred to in paragraph 4."
Article 49(6): ITS on "standard forms and templates for the procedure referred to in paragraph 4."

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

ECSDA agrees with ESMA's proposal as regards the type of risks that need to be taken into consideration in the risk analysis when justifying the refusal of an issuer by a CSD. A distinction of legal, financial and operational risks is reasonable. The examples provided by ESMA for each category are helpful indications, but they should not be considered as an exhaustive list. **It should also be clear that CSDs can, but do not have to, refuse issuers on these grounds.**

It is also important to note that technical standards will not affect the general right for CSDs provided in Article 49(3) of CSDR to refuse issuers in cases where the CSD does not provide notary services in relation to securities constituted under the law of the requesting issuer. This is an important safeguard since it protects CSDs from unnecessary legal risks arising from differences in national law in relation to securities issues.

Moreover, we would like to highlight that CSDR only refers to the refusal of issuers. The case where the CSD's refusal is limited to a particular issuance from one issuer is however also relevant. For example, a CSD may accept to offer notary services to an issuer for its fixed income securities but might not be equipped to offer notary services for its equities, for example because the CSD does not have access to the relevant feed from the CCP or trading venue, or because servicing equities would require it to set up a specific services such as withholding tax procedures. In order to cater for such cases, **ESMA should ensure that the proposed technical standards do not prevent CSDs from refusing news issues from an issuer for which it already provides notary services**.

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

ECSDA agrees with the time frames proposed by ESMA.

14. Refusal of access for CSD links - Article 52(3), (4)

WHAT THE LEVEL 1 REGULATION SAYS:
Article 52(2): "A CSD may only deny access to a requesting CSD where such access would threaten the smooth and orderly functioning of the financial markets or cause systemic risk. Such refusal can be based only on a comprehensive risk analysis."
Where a CSD refuses access, it shall provide the requesting CSD with full reasons for its refusal.
In case of refusal, the requesting CSD has the right to complain to the competent authority of the CSD that has refused access.
The competent authority of the receiving CSD shall duly examine the complaint by assessing the

reasons for refusal and shall provide the requesting CSD with a reasoned reply.
The competent authority of the receiving CSD shall consult the competent authority of the requesting CSD and the relevant authority of the requesting CSD referred to in point (a) of Article 12(1) on its assessment of the complaint. Where any of the authorities of the requesting CSD disagrees with the assessment provided, any one of the authorities may refer the matter to ESMA, which may act in accordance with the powers conferred on it under Article 19 of Regulation (EU) No 1095/2010.
Where the refusal by the CSD to grant access to the requesting CSD is deemed unjustified, the competent authority of the receiving CSD shall issue an order requiring that CSD to grant access to the requesting CSD."

WHAT THE LEVEL 2 TECHNICAL STANDARDS SHOULD SPECIFY:
Article 52(3): RTS on "the risks to be taken into account by CSDs when carrying out a comprehensive risk assessment, and competent authorities assessing the reasons for refusal in accordance with paragraph 2 and the elements of the procedure referred to in paragraph 2."
Article 52(4): ITS on "standard forms and templates for the procedures referred to in paragraphs 1 to 3."

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

In general, ECSDA agrees with the time frames proposed by ESMA. We suggest however the following amendment to the last bullet point of §216:
"*Where the refusal by the CSD to grant access to the requesting CSD is deemed unjustified, the competent authority of the receiving CSD should issue an order requiring the receiving CSD to grant access to the requesting CSD. The CSD should be required to provide access to the requesting CSD through a standard link within 3-8 months of the order.* ***Whenever the setup of the link requires developments (customised link), those costs would be at the expense of the requesting CSD (cf. point 218 b). The requesting and receiving CSDs will have to agree on the scope of the developments, costs and time frame as 8 months may not be sufficient for the developments****."*

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

Yes.

15. Refusal of access to other market infrastructures - Article 53(4), (5)

WHAT THE LEVEL 1 REGULATION SAYS:
Article 53(1): "When a CSD submits a request for access under Articles 50 and 51 to another CSD, the latter shall treat such request promptly and provide a response to the requesting CSD within three months."
Article 53(2): "A CSD may only deny access to a requesting CSD where such access would threaten the smooth and orderly functioning of the financial markets or cause systemic risk. Such refusal can be based only on a comprehensive risk analysis.
Where a CSD refuses access, it shall provide the requesting CSD with full reasons for its refusal.
In case of refusal, the requesting CSD has the right to complain to the competent authority of the CSD that has refused access.
The competent authority of the receiving CSD shall duly examine the complaint by assessing the reasons for refusal and shall provide the requesting CSD with a reasoned reply.
The competent authority of the receiving CSD shall consult the competent authority of the requesting CSD and the relevant authority of the requesting CSD referred to in point (a) of Article 12(1) on its

assessment of the complaint. Where any of the authorities of the requesting CSD disagrees with the assessment provided, any one of the authorities may refer the matter to ESMA, which may act in accordance with the powers conferred on it under Article 19 of Regulation (EU) No 1095/2010.
Where the refusal by the CSD to grant access to the requesting CSD is deemed unjustified, the competent authority of the receiving CSD shall issue an order requiring that CSD to grant access to the requesting CSD."
Article 53(3): "ESMA shall, in close cooperation with the members of the ESCB, develop draft regulatory technical standards to specify the risks to be taken into account by CSDs when carrying out a comprehensive risk assessment, and competent authorities assessing the reasons for refusal in accordance with paragraph 2 and the elements of the procedure referred to in paragraph 2.
ESMA shall submit those draft regulatory technical standards to the Commission by nine months from the date of entry into force of this Regulation.
Power is delegated to the Commission to adopt the regulatory technical standards referred to in the first subparagraph in accordance with the procedure laid down in Articles 10 to 14 of Regulation (EU) No 1095/2010."

WHAT THE LEVEL 2 TECHNICAL STANDARDS SHOULD SPECIFY:
Article 53(4): RTS on "the risks to be taken into account by CSDs when carrying out a comprehensive risk assessment, and competent authorities assessing the reasons for refusal in accordance with paragraph 2 and the elements of the procedure referred to in paragraph 2."
Article 53(5): ITS on "standard forms and templates for the procedures referred to in paragraphs 1 to 3."

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

ECSDA agrees with ESMA's proposal as regards the type of risks that need to be taken into consideration in the risk analysis when justifying the refusal of links with other market infrastructures. A distinction of legal, financial and operational risks is reasonable. The examples provided by ESMA for each category are helpful indications, but they should not be considered as an exhaustive list.

We note however that the CSDR foresees access from other market infrastructures to CSDs as well as access from CSDs to other market infrastructures. Limiting CSDR technical standards to specifying the conditions for the refusal of access of the CSD to other market infrastructures – and not covering the reverse situation – could result in a gap in the regulatory treatment of accesses between CSDs, CCPs and trading venues.

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

ECSDA agrees with the time frames proposed by ESMA.

16. Procedure to provide banking type of ancillary services - Article 55(7), (8)

WHAT THE LEVEL 1 REGULATION SAYS:
Article 16(4): "As from the moment when the application is considered to be complete, the competent authority shall transmit all information included in the application to the following authorities:
(a) The relevant authorities referred to in Article 12(1);
(b) The relevant competent authority referred to in Article 4 (4) of the Directive 2006/48/EC;
(c) the competent authorities in the Member State(s) where the CSD has established interoperable links

with another CSD except where the CSD has established interoperable links referred to in Article 19(5);
(d) the competent authorities in the host Member State where the activities of the CSD are of substantial importance for the functioning of the securities markets and the protection of investors within the meaning of Article 24(4);
(e) the competent authorities responsible for the supervision of the participants of the CSD that are established in the three Member States with the largest settlement values in the CSD's securities settlement system on an aggregate basis over a one-year period;
(f) ESMA and EBA."

WHAT THE LEVEL 2 TECHNICAL STANDARDS SHOULD SPECIFY:
Article 55(7): RTS on "the information that the CSD shall provide to the competent authority for the purpose of obtaining the relevant authorisations to provide the banking services ancillary to settlement."
Article 55(8): ITS on "standard forms, templates and procedures for the consultation of the authorities referred to in paragraph 4 prior to granting authorisation."

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

Yes, ECSDA agrees.

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

We do not believe that *"the investment policy of the credit institution"* (§235) is relevant information for the purpose of this article, as the credit institution will be subject to CSDR articles 54 and 59 and to the limitations included in Section C of the CSDR Annex.

Furthermore, we note that a *"service level agreement"* is only part of the elements to consider in case of outsourcing. The entities should demonstrate compliance with the general outsourcing requirements included in CSDR and the banking legislation.

Additional elements to be considered are:

- The need for prompt access of the credit institution to the securities collateral related to its short term credit provision (i.e. this collateral will be located in the CSD);
- The alignment of recovery and resolution arrangements of the two or more legal entities;
- The need to address possible conflicts of interest in the governance arrangements of the respective entities.

ECSDA thanks ESMA for the opportunity to comment on the Discussion Paper on CSDR technical standards. For any questions on this paper, please contact the ECSDA Secretariat at +32 2 230 99 01 or email soraya.belghazi@ecsda.eu.