**CONFIDENTIALITY STATEMENT: Please treat the cost estimates included in the answer to Question 29 as confidential.**

**KDPW comments to ESMA Discussion Paper “Draft Technical Standards for the Regulation on improving securities settlement in the European Union and on central securities depositories (CSD)”**

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

From our point of view CSDs are not directly in the scope of trade confirmation and allocation between investment firms and their professional clients.

Anyway, to improve and fasten the process on the CSD side it is crucial to use the hold/release and the tolerance level mechanisms.

The hold/release mechanism allows an investment firm to send the instruction to CSD with the status ‘Hold’ while waiting for the confirmation from its client. Then, after the confirmation only, the ‘Release’ is to be done.

The tolerance level allows settlement in the situation when the amount in the instructions differs between counterparties.

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

Automation is crucial for the CSD business, but CSDs must have the possibility to act at their discretion when manual intervention is necessary, especially when the manual intervention might be required to ensure timely settlement.

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

While ISO20022 is mandatory for CSDs for T2S communication, the majority of messaging from participants to CSDs should be ISO15022 based or even proprietary.

Mandatory use of ISO20022 standard for communication between participant and the CSD would imply a significant cost not only for CSDs, but also for all financial institutions in the settlement chain as well. It would be a very challenging task to force all CSDs’ customers to migrate to ISO20022 in the specified timelines.

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

KDPW agrees that matching should be compulsory.

We would suggest adding ‘Settlement Transaction Type’ to the matching fields list.

The tolerance of settlement amount is currently possible but not mandatory in the Polish market. An institution may declare on the settlement instruction level whether or not to use the amount tolerance mechanism.

Currently the client level matching (using account id and institution code) is not mandatory on the Polish market, but it is recommended by the National Market Practice Group Poland.

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

KDPW agrees with the above proposals. For transactions which have not been matched by a trading venue or a CCP, matching on the CSD level should be compulsory in most cases. CSDs should offer real-time matching throughout business day, standardized matching fields, hold/release and bilateral cancellation facilities, tolerance amounts. CSDs should also provide their participants with up-to-date information on the status of their pending instructions.

We support the proposal of penalties for late matching of complete instructions.

In the situation when the information on the instruction status is passed to participants immediately after every change of the status and a participant has an unrestricted possibility to request the information on its instruction status, we do not see any reason for setting a time cap for making the information on the lack of matching available by the CSD to its participants.

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

In our opinion in the case of CSDs which offer real-time gross settlement (RTGS) system allowing for continuous settlement during the day, there is no need to determine the minimal number of settlement batches per day. If a CSD does not have RTGS, it should offer at least 3 settlement batches per day, however the number of settlement batches should be dependent on the market demand. Batches should be as short as possible.

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

In our opinion technical netting, partial settlement and recycling of settlement instructions by the CSD should be the mandatory measures to facilitate settlement on ISD.

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

In our opinion the securities lending and borrowing facilities should not be mandated but should rather be considered as one possible option to prevent settlement fails.

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

KDPW generally agrees with the description of the system monitoring settlement fails.

We also agree with the general content of the proposed report template. We would, however, turn your attention to the fact, that the proposal does not envisage the distinction between domestic and cross-border operations in the report and does not take into account the fact, that for the FoP settlement instructions the value may not be available, which raises a question on whether and how such an instruction should be included in the report.

In our opinion the distinction between domestic and cross-border operations is not quite clear. The term „domestic” might be understood broader than the settlement between participants of the same CSD, therefore we propose to precisely define it as such, or replace the terms „domestic” and „cross-border” with the following terms:

- internal settlement – settlement between two participants of the same CSD  
- external settlement – settlement between a participant of the CSD and a participant of another, linked CSD.

In our opinion the CSDR technical standards should require CSDs to report fails to their competent authority **on a monthly basis**, which would allow to avoid a significant increase in the costs of reporting. In a crisis situation the competent authority would have right to demand daily reporting.

In case of the monthly reporting cycle it is necessary to define precisely, which data should be taken into account for calculation of „% Fail”, e.g. to determine, whether failed instructions should include instructions settled after the intended settlement date or also instructions which were never settled (and finally cancelled in the system)? The detailed definition of data used for calculations will allow to gather comparable data from all the CSDs.

KDPW is currently able to use in its reports both: ISIN and CFI codes for description of financial instruments.

It is not clear for us, what ESMA means by: „…They should at least have open access to their own status on fails and an aggregate status for CSD operating the systems to which they are participants.” (p. 38), so we cannot comment on this point.

KDPW sees the problem with categorizing instructions as FoP and DvP, because after the introduction of settlement netting in KDPW later this year the instructions delivered to the settlement system by the CCP will be defined in a different way, e.g. DwP – delivery with payment or RwP - receive with payment. Thus, we propose to consider the possibility to treat the information regarding the CCP-cleared instructions differently from other instructions.

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

In our opinion a participant should be able to receive from the CSD all information on the failed instructions involving this participant as a side of the settlement.

Taking into account the requirement described in p. 43 “Participants should be able to access the relevant information on their transactions settled/to be settled at a given CSD.” we would like to stress, that if a CSD receives netted instructions (from a CCP), it has no access to information on particular transactions which were included in the netting process, it only has information on instructions settled/to be settled.

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

As regards the publication of data which would be accessible for other CSDs and competent authorities, the implementation of the proposed solution would not pose problems for us. Such a service should be provided via a www solution and it should not be required to build a dedicated solution for each recipient of the information. Competent authorities could have an additional, individual access protected with extra safety measures. The definition of a standard European data format would bring added value. Speaking from experience gained during the EMIR implementation we would advise to define this format, as well as the range of information required, at the beginning of the CSDR implementation. We propose to use the xml and/or csv format. Data should be accessible in a monthly, quarterly or annual period.

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

In our opinion the daily reporting would be onerous for both: a CSD and the competent authority. Additionally, we would like to remark, that if the single format of reported data will not be defined, the reports would have limited value for competent authorities.

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

In general, a buy-in regime is already in place on the CCP level. Different markets have different level of liquidity - a financial instrument illiquid on one market can have a different level of liquidity on another market. Therefore, different levels of liquidity on different markets and also cross-market deliveries have to be taken into consideration (i.e. a harmonized buy-in period should be applied for specific financial instruments across Europe to reduce the market impact).

We support a proper calibration of the buy-in procedure to take into account the constraints in relation to the liquidity of securities. In particular, illiquid securities should be subject to longer timeframes for delivery to the receiving participant.

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

Since currently buy-ins under the EU Short Selling Regulation are executed on S+4 without causing any issues, the period of four business days is feasible for liquid assets and, therefore, no longer extension period is required. In case of OTC transactions KDPW\_CCP uses the period of two days.

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

We believe that the buy-in process is primarily the responsibility of CCPs. As a CSD we cannot define circumstances under which a buy-in would not be possible. We do not see any benefits in envisaging in technical standards a coordination of multiple buy-ins.

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

We believe that the buy-in process is primarily the responsibility of CCPs. As a CSD we cannot define circumstances under which we would deem a buy-in to be ineffective.

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

We agree on the proposed approach.

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

We agree with the ESMA’s approach that value, duration and number of fails should be taken into account, as well as that the level of fails of each participant should be weighed on the basis of its own activity.

Nevertheless, we do not believe that a suspension is a reasonable response in a situation of repeated settlement failures. We are convinced that there are other, more efficient, ways for the CSD to penalise repeated bad behaviour and the suspension of a participant should be considered as an extreme measure. It can only be used as an ultimate solution to a serious problem, and will only be implemented after careful consideration of the circumstances in each case.

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

We agree that the proposed quantitative thresholds established by ESMA (taking into account the value and volume of fails) might help to define the notion of a participant failing “*consistently and systematically*”. The proposal how to calculate the thresholds is, however, too general for us to be able to make detailed proposals. In our opinion, the period upon which the performance of a participant is measured should be sufficiently long, e.g. 12 months. It is essential to precisely define the data for calculation of percentage of the number of settlement instructions submitted by the failing participant over the defined period.

However, we would like to stress that the thresholds should not be too high (in terms of volume or value) and should be calculated over a sufficiently long period.

It is nevertheless very important that the suspension of a participant **should never be triggered automatically** once the thresholds are reached. Some degree of discretion is needed for the CSD to consult with regulators and assess the possible consequences of a suspension for systemic risk.

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

We would like to turn your attention to the fact, that at least in some cases, a CCP itself, as a result of novation of trades, is a counterparty to the settlement of instructions which they send to a CSD. In such case the CCP receives information on settlement fails via standard mechanisms used during the settlement process, such as the information on the status of instructions submitted by the CCP, in which the CCP itself is a counterparty. Thus one can assume that the CCP is immediately informed about settlement fails of its instructions. A CCP is also able, using the linkage between the settlement instruction sent by the CCP to the CSD and the instructions received by the CCP from its clearing members, to determine the clearing member responsible for the transaction which failed to settle. With this information the CCP may execute the buy-in for this clearing member.

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

KDPW does not comment on the requirements for “settlement internalisers”, as this is not an issue for CSDs.

**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.**

We understand ESMA’s approach stated, in paragraph 79, that the application of a CSD *“should include all details needed to demonstrate compliance with all CSDR and relevant technical standards”* but we would like to note that the list of documents contained in Annex 1 of the ESMA Discussion Paper is very extensive, although, according to paragraph 80, it constitutes only minimum information. Taking this into account, **we would like to express an opinion, that the information specified by ESMA under article 17(8) and detailed in Annex 1 of the Discussion Paper should not 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, KDPW 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. Moreover, some items, especially listed under titles E2 and E3, need further clarification and some other – verification, in order to avoid unnecessary duplication.

**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.**

In our opinion the approach presented in the Discussion Paper is appropriate and we agree with the template proposed in Annex II.

Nevertheless, we would like to draw your attention to the fact, that the proposal relating to the medium on which the application for CSD authorization is to be provided to the competent authority may be in conflict with regulations of the local administrative law, which determine the form of proceedings before the administrative authority and the form of providing applications in these proceedings. In Poland, for example, according to the Code of Administrative Procedure, applications provided in proceedings before a public administration (which includes the Financial Supervisory Authority) may take form of a written document, telegram, facsimile or be delivered orally and stated in the minutes, as well as be delivered also by the other means of electronic communication via the electronic inbox. It means, that the Polish law does not envisage the possibility to provide an application in a data storage medium. Thus, in our opinion the RTS should clearly state, that in the case of application for CSD authorisation the local legal requirements related to the form of the application should not apply.

**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?**

KDPW does not agree with all the restrictions suggested by ESMA in relation to CSDs’ participations in other entities. We understand the need for technical standards to ensure that participations in other businesses do not put the 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 contributed 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, and one way of developing such solutions if 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.

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. KDPW agrees with ESMA that this requirement is appropriate.

1. **On limiting control:**

**The proposed prohibition for CSDs to have participation in which they exercise control over subsidiary would be going too far**. ESMA notes that risks resulting from such a participation may materialize depending on local laws. Thus limiting control may be justified only in case where CSD is indeed exposed to risk of sharing liabilities incurred by its subsidiary and should not apply to other CSDs.

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. KDPW 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.

1. **On limiting revenues generated by CSD participations to a certain percentage of total revenues:**

KDPW 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 contribute to maintaining the financial strength and resilience of the CSD. Managing a fixed cap on revenues would be difficult for CSDs and could expose them to legal uncertainty in relation to participations. It is unclear whether the calculation of revenues over 3 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. 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, in contradiction with the objective of CSDR.

**KDPW is thus convinced that** t**echnical standards should not prescribe a fixed cap on revenues from CSD participations.**

1. **On limiting participations to other entities in the securities chain (trading venue, CCP, trade repository):**

KDPW 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 information providers/data vendors**. It should also be possible for CSDs to operate a subsidiary offering registrar services. **KDPW 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 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 or where such control does not expose the CSD to risk of reaching a negative value;
5. **CSDs should not be banned from directly participating in a CCP. The participation of a CSD in a CCP should be a subject to general rules and no particular regulations are needed as regards the participation in such type of entity.**

**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.**

KDPW generally agrees with the proposed approach. That said, we believe that **the notion of “materiality” should be 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 and the scope of information provided to CSDs should be limited to these changes and processes.** 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 the information provided in the context of the ongoing supervisory assessments. Focusing on relevant updates only would considerably facilitate the work for competent authorities and thus contribute to the efficiency of the supervision process. KDPW 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.

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 and only require CSDs 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. It is important to clarify that CSDs shall provide to the competent authorities for the purposes of the review only the relevant and material changes to the arrangements, strategies, processes and policies, which has taken place since the authorisation or the last review.

The above should not prevent CSDs from presenting to the competent authority any other additional information that this CSD reasonably deems relevant.

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

KDPW agrees 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”. 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.

**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?**

1. **Monitoring tools**

It is not clear to what extent a CSD would have to identify, manage, monitor and report risks in relation to participants or other entities (according to paragraph 110). We assume that this process should not go beyond the requirement of managing risks to which a CSD might be exposed. For example, we are not sure whether a CSD should identify, manage, monitor and report risks in relation to participants’ clients. In our view, it is rather the responsibility of the respective participant to assess and manage the risks in relation to its clients.

Thus, we think that some further clarifications are necessary to specify the adequate range of actions that a CSD should undertake to manage risks in relation to other entities.

1. **Responsibilities of key personnel**

KDPW agrees with the list of responsibilities of key personnel suggested by ESMA.

We would like to stress, that technical standards should make it clear that the “dedicated functions” should be clearly attributed to an individual, but this should not require that this individual can only undertake duties pertaining to their function. However, it should be ensured that additional duties, which remain outside of the scope of the dedicated function, do not limit the ability of the person to properly perform the dedicated function.

1. **Potential conflicts of interest:**

KDPW generally agrees with ESMA’s approach on conflicts of interest, however, we expect that not all the ‘conflicts of interest’ identified by the CSD will need to be ‘managed’ (e.g. requiring special adaptations or procedures), and that in some cases the disclosure of such potential conflicts of interest will suffice.

Moreover, KDPW does not agree with the proposal made by ESMA in §114, which would require CSDs to share the audit report or its findings with the user committee. The audit findings could contain confidential information concerning specific clients of the CSD, who simultaneously could be competitors in the environment in which they operate. The ESMA requirement is incomprehensible, difficult to be carried out and definitely goes beyond the International Standards for the Professional Practice of Internal Auditing.

**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?**

In general, we agree with the proposed approach, but some more detailed description would be helpful to better understand the information required for the data categories listed in Annex III. The lack of precision increases a risk of different understanding of these categories among CSDs, which would result in differences between their databases. This relates in particular to the following categories: link, flow (might be difficult to estimate for a CSD), governance and policy.

Currently KDPW keeps most of the information required, but we would like to note, that there are some categories, relating to information on issuers and participants, which would be problematic for CSDs, such as: Persons exercising control on Issuers,  Country of establishment of persons exercising control on issuers, Cash accounts used by Issuers, Persons exercising control on Participants, Country of establishment of persons exercising control on Participants, Participants cash accounts - end of day balances, Issuers’ and Participants’ details, including authorised signatures, Categories of Issuers accepted.

We would like to stress the importance of the identical requirements related to access to data on entities established outside the Union, which would have major influence on costs incurred by CSDs.

KDPW agrees with the proposed approach regarding registering corrections and amendments of records.

**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?**

In our opinion it is necessary to keep the costs of changes as low as possible, at least at the beginning. Taking that into account we propose to limit the usage of LEI as a legal entity identifier to reports for competent authorities only and continue with the existing participants codes in the CSDs databases.

KDPW has estimated the costs of record-keeping according to the requirements described in the Discussion Paper as follows:

|  |  |  |
| --- | --- | --- |
|  | **One-off costs for building the system:** | **Ongoing annual costs for maintaining the system:** |
| A) Costs for maintaining all the required records in an open, non-proprietary format (as opposed to a proprietary format) | 400 000 EUR | 550 000 EUR |
| B) Costs in case the use of LEIs for is made mandatory for CSD records on each settlement instruction | 15 000 000 EUR | 4 500 000 EUR |
| C) Costs of changes in case the LEI code is required only for reports prepared for supervisors (no changes in instruction content etc.). | 200 000 EUR | 60 000 EUR |
| D) Costs in case a direct data feed from the CSD to the competent authority is required: | 500 000 EUR | 200 000 EUR |
| **TOTAL COSTS:** | **15 900 000 EUR**  **(1 100 000 EUR – if LEI used only for reporting to CAs)** | **5 250 000 EUR**  **(810 000 EUR – if LEI used only for reporting to CAs)** |

**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.**

We agree with the above proposals as regards the types of risks that should be taken into consideration in order to justify a refusal. We would underline, however, that the examples given by ESMA for each category are not always appropriate for CSDs.

As regards legal risks, in case of the third example, CSDs cannot be expected to assess whether *“the requesting party is not compliant with prudential requirements”*, and in this situation they should be allowed to rely on the existing authorisations obtained by the applicant participant. For example, a CSD is not in a position to make a judgement on the compliance of the investment firm or credit institution with applicable rules.

We have similar doubts about the fourth and sixth examples in that point.

As regards financial risks, we expect ESMA to provide a precise indication of the basis on which CSDs will make the assessment of the requesting party. In our opinion a CSD may only make a general financial assessment of a participant or evaluate its compliance with the capital requirements imposed by the CSD on the basis of information included in the participant’s financial statement. CSD does not have means and should not be expected to assess, whether the applying participant has the adequate financial resources to fulfil its obligations towards its clients. Such an assessment may only be made by the appropriate competent authority.

Moreover, it should also be clear that the technical standards are limited to cases where a CSD has doubts on the eligibility of an applicant participant and that CSDs can, but do not have to, refuse access to a participant on these grounds.

**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.**

KDPW agrees with the proposed time frames.

**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.**

In our opinion an appropriate reconciliation should include verification by a CSD of the total number of securities credited in accounts in the CSD in comparison to the total number of securities issued into the CSD. Where reconciliation cannot be successfully ended, the CSD should not consider that security for settlement until the reconciliation has been performed. Extra reconciliation should not be included in CSDR technical standards.

**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.**

Statements of a registration account shall be issued without delay when any operation is registered on the account. In addition, a CSD shall send to participants the summary statements for a given accounting date at the end of that day.

It is therefore the responsibility of the participants to reconcile their own internal book-entry systems with the CSD’s records.

At the end of the Record Date participants shall determine the number of securities to receive the distribution entitlements from securities, deposited in the accounts kept by the participants. A CSD shall determine the number of securities whose owners are entitled to dividends, the securities being registered on accounts kept in the CSD for direct participants. A CSD shall notify direct participants of those entitlements. Participants shall clarify and eliminate any discrepancy between the determined values.

**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, we generally agree with the ESMA’s approach, but we do not think that the double-entry accounting gives CSDs a sufficiently robust basis to avoid securities overdrafts, debit balances and securities creation. In our opinion the standards should specify another measure, such as introduction of accounts that allow exclusively debit or credit balances.

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

In our opinion the standard should also address the definition of operational risk included in the Regulation (EU) No 575/2013 of 26 June 2013 on prudential requirements for credit institutions and investment firms (CRR), according to which “*operational risk means the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events, and includes legal risk*”. The CRR definition of operational risk has already influenced risk management systems of financial institutions over the last decade and although CSDR treats legal risk as a separate category, CSDs should be allowed to manage operational and legal risk in one integrated framework (especially in the context of measurement). Certainly legal risk needs specific procedures and controls but the same applies to individual operational risk subcategories (IT systems and information security, employees, external events, etc.).

We may also expect that the regulatory technical standards specifying capital requirements, as those developed for central counterparties (Commission delegated Regulation (EU) No 152/2013 of 19 December 2012), will impose on CSDs the obligation to calculate its capital requirements for operational risk in accordance with Capital Requirements Directive/Regulation, i.e. including legal risk. That would be another argument for the integration of legal risk with operational risk.

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

We have some doubts about the concept of a central function for managing operational risk (*“b. Risk management function and resources”*). In our opinion the process of managing operational risk is always decentralized with the dominant role played by internal business units. The coordination and improvement of that process is necessary and here is the role for the central function to develop general strategies, policies and procedures to identify, measure, monitor and report on operational risk.

However the specific procedures to control operational risk should rather be developed by the internal business units which are the business process owners and we believe that the operational risk management is inseparable from the business process management. Therefore the CSD’s internal business units have to remain responsible for managing operational risks despite the existence of a central function for managing operational risk. The latter should make the operational risk management system complete, e.g. by introducing the effective risk measurement and reporting framework, but it cannot replace the internal business units in their role as the business process owners.

**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?**

The list of the methods of operational risk identification could be expanded with “available risk factor or event type classifications” (such as loss event type classification described in Capital Requirement Regulation for the purpose of Advanced Measurement Approach). That would supplement CSD’s risk scenarios the same way as external loss database would complete internal data.

Moreover the concept behind the key-risk indicators in the context of risk identification may need further specification. In our view the creation of KRIs by CSD is a process of risk measurement and monitoring (after the risk identification). The way we could identify risk via KRIs would be rather through analyzing the formulas of KRIs received from external sources.

As far as mitigation of operational risk is concerned we agree that the risk transfer through insurance does not eliminate the risk. It can only limit the financial consequences of operational risk events. Nevertheless the standard could also address the risk transfer through insurance in positive context as the additional protection of a CSD (and completion of operational risk management system), except using the adequate procedures and controls.

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

We agree with the requirements presented in points 165, 166 and 167, stating that the IT solutions should be secure, efficient, scalable, audited and tested. Nevertheless, taking into account the mandatory annual review of the IT system(s) and IT security framework of all CSDs proposed in §167 of the Discussion Paper, we would like to stress the cost of such a solution for a CSD, reaching several hundreds thousands Euro each year. It is also not clear, which areas of the IT system should be audited this way. In case of a strict, operational review, an audit conducted every two years would be sufficient, but if the review would be focused on the documentation and risk and security policies, 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?**

We have some doubts about the CSD’s ability to ensure the continuity of the critical functions in the event of global emergencies such as pandemic situations mentioned in paragraph 170 or terrorist attacks (especially in the context of a maximum recovery time of 2 hours). For instance, in such circumstances the government or local authorities could issue special regulations or declare a state of emergency and hence a CSD would not be able to take necessary actions because of the conflict with the necessity to conform to those special regulations.

The global emergencies should be addressed in the CSD’s business continuity policy and disaster recovery plan but the standard should take into account that a CSD might have very limited control over such situations.

**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?**

The requirement of providing “full information” about the performance of CSD’s utility providers and critical service providers to the authority needs some further clarification. No such expression was used in the context of participants or links to other FMIs, so it seems like the relevant authorities would expect very detailed information particularly about interdependencies connected with utility providers and critical service providers. We are not sure whether the system for identifying, measuring, monitoring, managing and reporting operational risk should include some special arrangements just for those specific interdependencies.

Moreover we would like to stress that some CSDs may have substantially high criteria for all of their participants, especially regarding minimum operational and business continuity requirements, and that those CSDs perform regular audits of the participants’ activities. We are not sure whether identifying critical participants based on transaction values and applying specific rules for them would be necessary in such circumstances. In our view, the requirement to manage operational risks associated with CSD’s participants could regard “first of all” the critical entities but the standard should also allow CSDs to have the uniform criteria for all participants.

**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?**

We agree for the unified RTS  approach to CDSs  in terms  of  investment policy irrespectively of the services offered or functions performed by the CSDs.

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

We  do not recommend ESMA to consider any other elements which define highly liquid financial instruments. In our opinion  the  average duration to maturity should be extended  up to five years. One may consider combined requirements, for example a five-year average duration provided that the duration of a single financial instrument isn’t longer than 11 years.

The proposed maximum of two-years duration is too restrictive and should be extended, taking into account that CSD’s liquidity needs are not so frequent as those of a CCP.

We think that a five year maximum average duration is reasonable especially because of the remaining requirements, e.g.  a liquid secondary market and not significant (acceptable) price fluctuations. Treasury financial instruments or instruments of the central bank have high and comparable liquidity regardless whether the period to maturity is 2,5 or 10 years.

**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.**

KDPW agrees that one of the ways in which to reduce risks in CSD links is to “…perform an extensive analysis of the receiving CSD’s financial soundness, governance arrangements, processing capacity, operational reliability and reliance on a critical service provider and has taken the necessary measures to monitor and manage the issues that may arise from such analysis” (190 – indent 3). However, these are the very criteria which are to be evaluated by the competent authority in the receiving CSD’s home state (for receiving CSDs subject to the provisions of the CSD Regulation). Since such risk criteria can be assessed more accurately by competent authorities rather than CSDs, such an extensive analysis as proposed by ESMA may be unnecessary repetition at least with respect to authorised (i.e. non-third country) CSDs.

As regards DvP links, KDPW agrees that CSDs which use intermediaries for cash settlement need to monitor them to ensure they perform as expected. It may however be necessary to indicate how credit risk should be assessed and if credit ratings are to be used, what the rating source should be.

For interoperable links (193) KDPW is unsure whether common contingency and default procedures (indent 5) can exist bearing in mind that if the CSD systems are separate (as they most often are in cases of interoperability: e.g. Clearstream-Euroclear link, Baltic CSD links) such procedures will be almost impossible to merge.

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

As regards monitoring of intermediaries in indirect links, it should be noted that for such links within the EU, where custodian banks are used as intermediaries, these will already be regulated for risk by other regulations (e.g. CRD IV).

KDPW believes in addition that recovery and resolution procedures of the intermediary should be examined as well.

It should be mentioned that, KDPW and many other CSDs, in particular ICSDs, operate numerous indirect links as well. It would therefore be prudent for ESMA to extend the deadline for the new requirements relating to indirect links to come into force, since it may be unduly onerous for many CSDs managing such indirect links to comply with these requirements before filing for authorisation. A 6-9 month delay would be deemed sufficient.

**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, KDPW 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.**

KDPW agrees with the description of instances where DvP settlement is practical and feasible.

**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.**

KDPW 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, however, not clear for us how the insolvency rules in a country of the issuer could justify a refusal of access of that issuer to a CSD.

As regards financial risks posed by an issuer, for a CSD it is essential to be able to refuse to provide services to an issuer who does not fulfil its financial obligations towards the CSD, without being obliged to make a comprehensive risk analysis.

We expect that the 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 unnecessarily legal risks arising from differences in national law in relation to securities issues.

**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.**

KDPW agrees with the time frames proposed by ESMA.

**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.**

KDPW agrees with the time frames proposed by ESMA.

**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?**

KDPW does not take part in the T2S project, thus we do not have expertise to comment on that issue.

**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?**

KDPW 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. Some of the examples provided by ESMA for each category are helpful indications, but we have doubts whether the presence of „the necessary internal anti-money laundering, anti-terrorism financing and anti – tax evasion measures” should be checked by a CSD. We do not understand the reason why this should justify a refusal of access for other market infrastructures.

**It should also be clear that CSDs may, but do not have to, refuse other market infrastructures on these grounds.**

**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.**

KDPW agrees with the time frames proposed by ESMA.

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

Yes, KDPW does agree with these views.

**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?**

As a CSD which does not perform banking services, KDPW has no experience required to answer this question.