European Association of CCP Clearing Houses

EACH feedback on the FSB-CPMI-IOSCO Report "Central Counterparty Financial Resources for Recovery and Resolution"

April 2022

European Association of CCP Clearing Houses AISBL (EACH), Avenue des Arts 6, 1210 Brussels

Introduction

The European Association of CCP Clearing Houses (EACH) represents the interests of Central Counterparties (CCPs) in Europe since 1992. CCPs are financial market infrastructures that significantly contribute to safer, more efficient and transparent global financial markets. EACH currently has 18 members from 14 different European countries. EACH is registered in the European Union Transparency Register with number 36897011311-96.

EACH appreciates the opportunity to provide feedback on the FSB-CPMI-IOSCO Report "Central Counterparty Financial Resources for Recovery and Resolution" (hereinafter called "the report").

The **key messages** expressed by EACH in this document are the following:

- CCPs already have in place a **comprehensive number of measures to prevent and mitigate non-default losses** arising from the various types of risk scenarios, e.g. investment and custody risks, general business or operational risks and uncovered liquidity shortfalls.
- Researchers have calculated that the **probability of a non-default event** causing a loss capable of exhausting both the regulatory capital held by the CCP and the annual profits held by the CCP, and therefore **triggering resolution actions, is extremely low**.
- **The results of scenario 2 on cyber theft** (i.e. that only through the use of resolution tools sufficient resources would have been mobilized to address the losses caused by a cyber theft) **should be read with caution**, as they could have been different would sampled CCPs have interpreted the given scenario differently and would have applied operational arrangements or cyber security measures with are also part of CCP risk management practices.
- Certain business and operational failures, such as a cyberattack, are not likely to be addressed with additional resources, but they should rather be **prevented through the application of ex-ante measures**, such as an appropriate cybersecurity policy.

Introduction: Types of non-default loss scenarios

Given the business model of CCPs and the markets in which they serve, in line with the FSB guidance[1] we considered there are **three main types of risk scenarios** that could give rise to a non-default loss (NDL):

- **Investment and custody risks**
- **General business or operational risks**
- **Uncovered liquidity shortfalls**

[1] https://www.bis.org/cpmi/publ/d162.pdf

1. Investment and custody risks

Description

Investment risks refer to the potential risks faced by the CCP as a result of the investment of the resources provided by the CCP, its clearing members and/or clients. Due to the conservative investment rules in place, outlined in Article 47 of the EMIR Legislation[2], it would only be in the most extreme cases that the CCP's investments could materialise in losses that might prevent the CCP from meeting its financial obligations towards its participants. In addition, due to the provisions in EMIR preventing CCPs from depositing more than 5% of their overnight cash balances with commercial banks and the fact that several central banks do not accept overnight deposits from CCPs, CCPs have to invest the majority of cash collected as margins and default fund contributions. EMIR sets prudent investment standards, so only in an extreme scenario, such as government or repo counterparty default, could this lead to investment losses.

Custody risks refer to the potential risks faced by the CCP in case the custodians that keep the resources of the CCP, its clearing members and/or clients are subject to severe stress that prevents them from meeting their obligations as defined in the agreements made with their partners, including CCPs. The CPMI-IOSCO Principles for Financial Market Infrastructures (PFMIs)[3] refer to insolvency, negligence, fraud, poor administration or inadequate record-keeping as potential sources of custody risks.

Mitigating investment and custody risks – Measures and resources

To mitigate investment risks and prevent potential **investment** losses, CCPs have developed **robust and conservative investment strategies and monitoring systems**, building on the demanding and conservative standards already prescribed by EMIR as a best practice.

Regulators and CCPs share the ultimate goal of protecting the funds of clearing members from any potential loss and have worked together to develop prudent standards for investment of margin and default funds' contributions. These requirements, as well as each CCP's approach to meeting them, are publicly available through the CCP's rulebook and disclosures, ensuring total transparency into each CCP's investment approach and risk management.

To further reduce investment risks, EACH Members maintain a **balanced range of options to deposit collateral**, including where possible access to central banks, in order to avoid concentrating the deposits at commercial banks that are also clearing members. Investment risks could be further reduced by:

- Ensuring a **diversified scope of high-quality investment counterparties** (e.g. investing in secured money market funds);

[2] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32012R0648&from=EN
[3] https://www.bis.org/cpmi/publ/d101a.pdf

- Considering **rules to give CCPs a special treatment** in the event of a custodian/CSD recovery and resolution event;
- Extending **access to central bank facilities**.

With regard to the measures to mitigate custody risks and prevent potential **custody** losses, while the dedicated legislation on Central Securities Depositories (CSDR)[4] makes CSDs even more stable, efficient and safer market infrastructures, in the extreme scenario of a CSD or custodian being severely disrupted, regulators may consider exploring **provisions for CCPs to directly access their assets held at CSDs**. It should be noted that a given CSD may not itself be the definitive record of title to a particular security. There may be a chain of **intermediaries** between that CSD and the local CSD which is the definitive record of title to which CCP might be exposed to.

In jurisdictions where a CCP does not have access to a CSD (such as a European CCP accepting US collateral), EMIR permits the use of **custodians**. This introduces the normal sorts of investment risk which are associated with any counterparty.

In line with the PFMIs international standards and Article 16 of the EMIR Legislation, CCPs must hold sufficient resources in the form of **capital**, including retained earnings and reserves, proportionate to the risk stemming from the activities of the CCP to address potential investment and custody losses[5]. This capital *'shall at all times be sufficient to ensure an orderly winding-down or restructuring of the activities over an appropriate time span and an adequate protection of the CCP against credit, counterparty, market, operational, legal and business risks which are not already covered'* by the default lines of defence.

2. General business or operational risks

Description

General business or operational risks refer to the potential risks that could result from events other than the default of a clearing member or those related to investment and custody. Operational risk management is a key piece of the regulatory framework and has been a focus of regulators around the world in recent years. CCPs support robust operational risk frameworks that define risk mitigation strategies and are subject to on-going regulatory review. Potential losses related to general business or operational risks could arise from:

[4] http://ec.europa.eu/finance/financial-markets/central_securities_depositories/index_en.htm

[5] http://bit.ly/1Nr5w4l European Market Infrastructure Regulation (EMIR) - Article 16 Capital requirements: A CCP shall have a permanent and available initial capital of at least EUR 7,5 million to be authorised pursuant to Article 14. CCP's capital, including retained earnings and reserves, shall be proportionate to the risk stemming from the activities of the CCP. It shall at all times be sufficient to ensure an orderly winding-down or restructuring of the activities over an appropriate time span and an adequate protection of the CCP against credit, counterparty, market, operational, legal and business risks which are not already covered by specific financial resources as referred to in Articles 41 to 44.

- **Third-party service providers** – Some CCPs rely on third-parties to ensure certain aspects of the day-to-day functioning of their business. These parties may include referential, market and price data providers or trade sources such as execution platforms and middlewares. A failure of these parties may impact the staff and operational systems of the CCPs and prevent them from functioning properly. CCPs mitigate this risk through defined service level agreements with third-party service providers, on-going due diligence on third-parties and third-party risk assessments.
- **System failures** (e.g. cybercrime or failure of monitoring tools) – This risk refers to the potential failure of the IT systems of the CCP. This could be the result of a general system failure or a concrete failure such as a cyberattack on the CCP. CCPs mitigate potential system failures through the measures such as the development of system redundancies, secondary sites, business continuity tests, continuous monitoring and testing of systems and security or third-party assessment of security. In line with principle 17 of CPMI-IOSCO PFMIs, the risk of system failures should be addressed amongst other through the CCP's business continuity plans.
- **Fraud** – This risk refers to the potential losses that could result from a fraudulent action by an employee of the CCP or a clearing member. CCPs mitigate fraud risk through the maintenance and enforcement of internal anti-fraud compliance policies, on-going monitoring of employee activity, limited access to online transmission or storage tools, and robust compliance requirements under regulations. Specific measures are described in each CCP's CPMI-IOSCO quantitative disclosures.
- **Legal claims/professional responsibility** – This refers to the legal risk to which the CCP may be subject as a result of, among other things, improper documentation among its partners and members. CCPs mitigate legal risk through on-going and regular review to ensure contractual relationships with its clearing members, which are subject to regulatory approval by National Competent Authorities (NCAs) and EMIR colleges, clients and vendors are legally robust and capable of functioning in case of recovery and resolution scenario. Third-party legal reviews in conjunction with reviews at the inception of new relationships (i.e. onboarding a new clearing member or settlement bank), including an evaluation of the entity's jurisdiction.

As with investment and custody risks, in line with the PFMIs international standards and Article 16 of EMIR, CCPs hold sufficient resources in the form of **capital**, including retained earnings and reserves, proportionate to the risk stemming from the activities of the CCP to address potential general business and operational risks.

In our opinion, it is important to stress that in certain cases **a CCP should cover all losses caused by a general business or operational failure**. In this regard, we would like to quote the Chicago Fed Paper "Non-default loss allocation at CCPs"[6], according to which "*CCP's*

[6] https://www.chicagofed.org/-/media/publications/policy-discussion-papers/2017/pdp-2017-02-pdf.pdf?sc_lang=en

owners choose and supervise the managers who run the CCP. The managers make decisions that either lead to or prevent business and operational failures. Therefore, the CCP's owners are ultimately responsible for such failures and should bear the cost." The Chicago Fed Paper explains that at a **demutualized CCP**, the responsibility of efficiently running the CCP avoiding business and operational failures fall on the shareholders and requiring them to pay for losses caused by their improper management would act as an incentive for them to ensure a robust CCP management. Instead, a **mutualized CCP** is – as specified by the Paper – owned by its members, and requiring a CCP to bear a NDL resulting from a business or operational failure would mean **requiring clearing members to bear such loss**. The loss allocation should be proportional to the level of responsibility of each stakeholder involved.

For **cyberattacks**, the **evaluation on who should bear the related NDL would be different**, because the cyberattack could have been "*facilitated by a connection between the CCP and a clearing member. In such a case, **the loss should be shared between the responsible clearing member and the CCP**.*"

Mitigating general business or operational risks – Measures and resources

To mitigate general business or operational risks, CCPs have in place the following **set of measures and resources**:

- Service legal agreements with third-parties and due diligences
- Legally robust contractual relationships.
- Continuous assessments
- Secondary sites, business continuity tests, monitoring and testing
- Anti-fraud compliance policies and employee monitoring
- Third-party legal reviews
- Capital legally required by EMIR

Furthermore, additional equity or recapitalization, asset sales or the subscription of insurance agreements are other measures available for CCPs to mitigate this type of risks.

3. Uncovered liquidity shortfall

By virtue of its central position in transferring assets (collateral) and cash variation margin payments between members, as well as because of having to re-use and invest assets in public markets, CCPs are exposed to the **risk of being unable to transform assets** in a timely way, resulting in a temporary liquidity shortfall. Depending on how the liquidity shortfall is addressed, **it may or may not result in a loss**.

CCPs mitigate the risk of liquidity shortfalls through daily **monitoring** of liquidity resources and frequent **re-evaluation** of liquidity needs. CCPs should also **stress test** their liquidity needs to ensure they would be able to meet their them under extreme but plausible

circumstances. This ensures that even under an extreme NDL scenario, CCPs maintain sufficient funding to meet their liquidity obligations.

CCPs may take additional steps to mitigate potential liquidity risk:

- CCPs may define their own **limits for collateral**, rather than subscribing firm limits on cash balances, in order to ensure they can maintain sufficient levels of the most liquid forms of collateral.
- Considering rules in the CCP's rulebook which give the CCP discretion at any time **to declare specific types of collateral to be ineligible**. This would allow a CCP to deal with any investment risks which were specific to a certain form of collateral by requiring replacement collateral from members.
- Considering rules in the CCP's rulebooks that **cash collateral** is not treated by the CCP as being received and allocated to the member until it is credited to the CCP's central/settlement bank account, therefore preventing the CCP bearing the risk of the default of a clearing member's settlement bank.

EMIR requires CCPs to hold enough **capital** to ensure a wind-down or restructuring period of at least six months in which the CCP's operations can be terminated or restructured in an orderly way.

Mitigating potential non-default losses arising from uncovered liquidity shortfalls – Measures and resources

CCPs should establish and regularly **assess** the adequacy of additional funding resources that could be called upon to fund potential liquidity shortfalls. Providing all qualified CCPs with an **equal opportunity to access central bank facilities** across the EU would help ensure all CCPs have additional support in managing liquidity risk during extreme market conditions.

Additionally, CCPs may be given the **power to convert the currency of an account to another currency** under extreme circumstances. As an example, if a CCP has a liquidity issue in relation to USD, it can convert a clearing member's account currency to EUR or GBP (in respect of which the CCP may have access to sufficient commercial credit lines or central bank money) and pay the member in that currency. This option may be considered in an extreme scenario, rather than as business as usual, if considered adequate to save a CCP from insolvency.

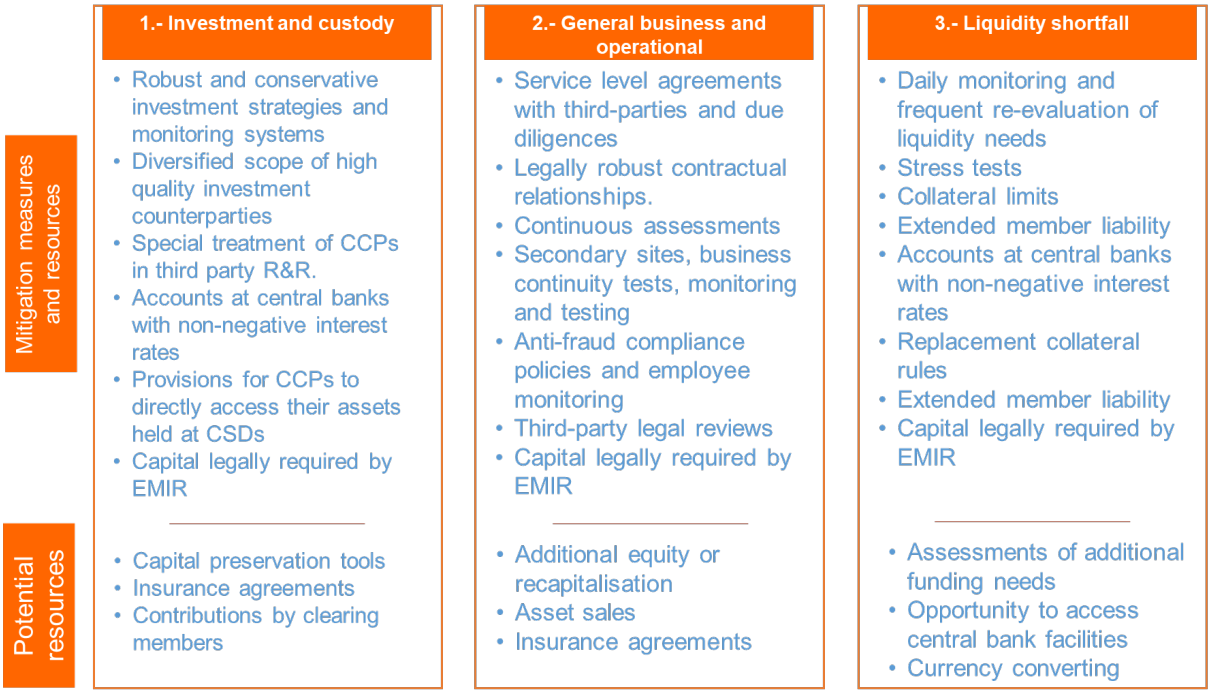
It is also important to underline that the CCP Recovery and Resolution framework[7] also provides tools for CCPs to address NDLs. An example is the additional amount of pre-funded own resources that CCPs – the so-called "second skin in the game"[8] – have to dedicate and which shall be used during the recovery phase before resorting to other recovery measures

[7] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32021R0023&from=EN
[8] https://www.esma.europa.eu/sites/default/files/library/esma91-372-1706_fr_rts_ssitg_art_915.pdf

requiring financial contributions from clearing members. This amount of resources is to be used both in case of a default loss and a non-default loss.

Figure 1 below **summarizes** the mitigation measures and resources to address potential NDLs.

Figure 1 – Mitigation measures and resources to address potential NDLs



EACH feedback on the non-default scenarios considered by the report

The report considers two specific scenarios of NDLs for all CCPs in the sample:

- **Scenario 1**: Liquidity risks from the loss of access to the institution (other than the central bank) holding assets (securities and/or cash) on behalf of the CCP.
- **Scenario 2**: Cyber theft (a quantum of cash stolen from the CCP was assumed to equal the highest daily value of the sum of all cash the CCP transferred to any single investment agent or depository on a single day).

EACH welcomes the FSB-CPMI-IOSCO's finding that "*all of the sampled CCPs would have had sufficient prefunded and recovery resources and tools to cover losses in the applied default loss scenarios*". However, we agree that **there are limitations to the analysis as acknowledged in the report**. In particular, the chosen scenarios were "*significantly more severe than the 'extreme but plausible' standard set out in the PFMI*", hence, it is worth highlighting that the assumptions taken for the stress losses calculation in a default event have indeed been rather rigorous (cover 4 with doubled liquidation horizon vs. the general CCP calibration of a cover-2 in 99.9% confidence level).

Against this background, it is an even more positive outcome that **CCPs show such strong resilience to default losses**, confirming our view that CCPs' default related recovery and resolution tools are sufficient and that CCPs are very well equipped to deal with even extreme scenarios.

The report finds that, concerning **scenario 1**, **all the CCPs were able to address the liquidity needs**. The report also adds that some CCPs have included in their rulebooks "*conditions into determining that a loss of access to or a failure of a custodian / central securities depository (CSD) would not result in a liquidity stress at the CCP but rather at the clearing member level, as the clearing members would be obliged to replace assets not accessible by the CCP*." No CCP, however, had to rely on these arrangements.

Concerning **scenario 2**, the report finds that, with the **exception of 2 CCPs** whose prefunded and recovery resources were sufficient to cover the loss resulting from the cyber theft, all the others saw their **losses exceeding their prefunded and recovery resources** reached between $265m and $11.8b, likely triggering resolution.

EACH would like to stress that the **report acknowledges the limitations of its assumption and analysis**, and we agree with that the most significant limitation of the NDL analysis was that the results greatly depend on the "choice of scenarios". In particular the cyber theft scenario was designed at an abstract level and with, from our point of view, implausible assumptions due to a lack of "actual experience" with such a case. **EACH therefore believes that the results of scenario 2** (i.e., that only through the use of resolution tools sufficient resources would have been mobilized to address the losses) **should be read with caution**, as they could have been different would sampled CCPs have interpreted the given scenario differently and would have applied operational arrangements or cyber security measures with are also part of CCP risk management practices.

In this context, EACH would like to put forward the following comments:

- **The importance of prevention measures** – Non-default events are not just dealt with through additional resources. Some non-default events such as a cyberattack are unlikely to be addressed with additional resources, but they should rather be prevented through the application of ex-ante measures, such as an appropriate cybersecurity policy.
- **CCP Recovery and Resolution regulatory provisions** – As mentioned above, existing European legislations on CCP Recovery and Resolution provide for additional tools to address NDLs, such as the CCP's second skin in the game which has to be deployed in recovery both in case of default and non-default losses, prior to requesting clearing members' financial contribution. Furthermore, recital 20 of the EU CCP Recovery and Resolution (CCP RR) Regulation specifies that "*recovery plans should ensure that the CCP's capital is exposed to losses caused by both default and non-default events, before losses are allocated to clearing members. As an incentive for proper risk management and to further reduce the risks of losses for the taxpayer, the CCP should use a portion of its pre-funded dedicated own resources*". The recital also underlines

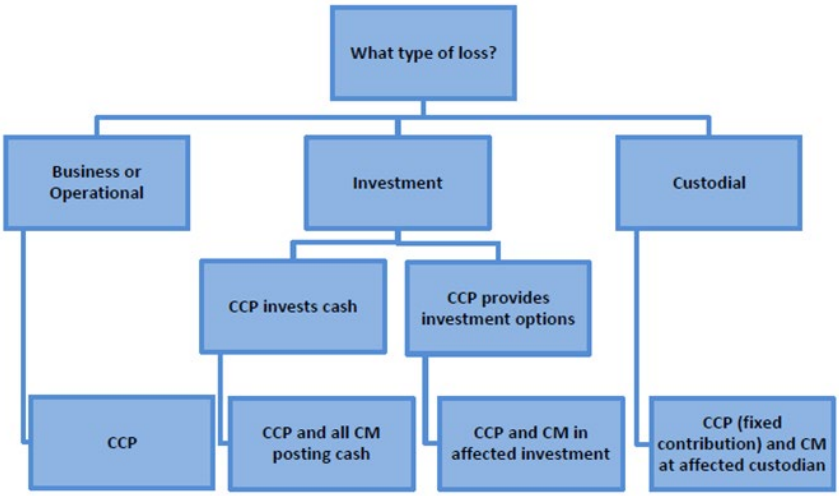
that "*as a general principle, losses in recovery should be distributed between CCPs, clearing members, and, where applicable, their clients as a function of their responsibility for the risk transferred to the CCP and their ability to control and manage such risks"*.

- **The "polluter pays" principle** – In line with what foreseen in recital 20 of CCP Recovery and Resolution, as explained above, EACH is of the opinion that loss allocation for non-default losses should be **proportional to the level of responsibility** of each stakeholder involved (e.g. CCP owner or CCP user) for bringing risk into the CCP or defining the policies to mitigate those risks.
- **Different resources for different losses** - The appropriate tool to allocate a particular NDL will therefore depend on the type of loss in question:
  - Capital of the CCP – In line with the PFMIs and the EMIR Legislation, European CCPs hold capital, including retained earnings and reserves, proportionate to the non-default risks that the CCP is exposed. This capital *"shall at all times be sufficient to ensure an orderly winding-down or restructuring of the activities over an appropriate time span and an adequate protection of the CCP against credit, counterparty, market, operational, legal and business risks which are not already covered"* by the CCP's other lines of defence. Should it be necessary, a CCP might increase its capital resources through the use of capital preservation tools (e.g. reduction in dividend payments, cost reductions, asset sales), payment of its liabilities in instalments or conversion of its debt into equity (subject to an appropriate agreement between the CCP and its counterparty), or general capital raising from investors. CCP capital is appropriate for the allocation of non-default losses for which the CCP is the only entity with the responsibility for creating and managing those risks. European CCPs are well placed to meet such losses and thus ensure continuity of the CCP's critical services and the preservation of market stability.
  - Clearing member contributions – Shareholders should bear losses related to idiosyncratic processes and procedures put in place by CCP management, such as operational risk (e.g. defective processes, human error, internal fraud). However, where the clearing members are responsible for determining the way the risks they bring to the CCP are managed, such as directing the investment strategy for their assets (which dictates counterparty credit quality, collateral acceptability criteria, limits etc.), or selecting the custodian at which their assets are deposited or dealing with liquidity related losses (in the cases where the CCP has agreed upfront a detailed liquidity framework with its members), then the CCP should not be held solely accountable for losses associated with such decisions. The same reasoning applies, as already mentioned, is a **cyberattack has been facilitated by a connection between the CCP and a clearing member**.
    Instead, the CCP should only be responsible for a proportion of such losses. At the other extreme, where a fraud was perpetrated by a clearing member, then that clearing member should be solely liable for any losses.
  - Other potential resources – CCPs may maintain additional resources for the allocation of those non-default losses for which the CCP is the only entity with the

responsibility for creating and managing those risks. These additional resources include insurance agreements which can, in some cases, be a potential additional resource to address losses from activities that the CCP undertakes.

Figure 2 below summarizes which stakeholders should bear a NDL on the basis of their involvement in making the decisions that led to the non-default event.

Figure 2[9] – Who should bear the costs of an NDL?



Furthermore, it is important to mention that part of the ex-ante procedures a CCP takes to prevent a cyber-attack – and a potential related cyber-theft – is that, for instance, once a CCP identifies an issue with a given bank during the day, the CCP would not continue to use such bank for further transfers throughout the whole day. **CCPs have indeed in place risk management practices/controls so that issues can be identified and rectified in a timely manner in case they occur**. The report does not seem to acknowledge this particular practice.

Also, it should be underlined that the probability of a non-default event triggering resolution actions is very low. As the University of Tilburg Paper "Why is a CCP failure very unlikely?"[10] explains, currently regulators require a charge of 15% of annual net revenues calculated as the average of the past 3 years annual figures. This corresponds to a conservative proxy for coverage up to a high quantile (99.9%) of the loss distribution. On this basis, the authors calculate that an NDL event *"which **exhausts both the regulatory capital held by the CCP and the annual profits held by the CCP** has a **very rare chance of occurring** of about 1.5bps. This is considered **AAA risk equivalent according to the Rating Agencies** and is even **under the Basel floor of 3bps**."*.

[9] Figure extracted from the Chicago Fed Paper "Non-Default Loss Allocation at CCPs": https://www.chicagofed.org/-/media/publications/policy-discussion-papers/2017/pdp-2017-02-pdf.pdf?sc_lang=en

[10] https://pure.uvt.nl/ws/portalfiles/portal/46839740/2021_002.pdf

Conclusions

Potential NDLs are primarily a result of CCP business that may be incurred by the CCP operator (i) in the course of managing its internal risks or complying with local regulation or (ii) as a consequence of events happening to the CCP's partners (e.g. CSDs, payment banks acting as intermediaries for funds transfers, etc.). CCPs, by their very nature of *central* counterparties, stand in the middle of various flows and have relationships with market participants and other financial markets infrastructures. The **analysis of NDLs**, which in many cases would result from events exogenous to the CCP, should therefore be considered from the **point of view of the entire market, not just by looking at the CCP in isolation**.

CCPs have carefully designed their risk management procedures, financial resources and recovery and resolution tools to manage market stress and ensure appropriate incentives for market participants to effectively manage their risks. In line with the PFMIs international standards, Article 16 of EMIR and the provisions included in European CCP Recovery and Resolution Regulation complementing the EMIR Legislation, CCPs already hold sufficient resources in the form of **capital**, proportionate to the risk stemming from the activities of the CCP to address NDLs, in addition to a series of measures and resources specifically designed to deal with the individual types of NDLs described in this document. Therefore, as detailed in the previous sections, the **probability of a non-default event** causing such a loss capable of exhausting both the regulatory capital held by the CCP and the annual profits held by the CCP, and therefore **triggering resolution actions, is extremely low**. In this context, it is also important to recognize that CCPs' resources for recovery and resolution cannot be looked at in isolation from other CCP risk management tools. Rather, it is fundamental to acknowledge that certain business and operational failures such as a **cyberattack** are **not likely to be addressed with additional resources**, but they should rather be prevented through the application of ex-ante measures, such as an **appropriate cybersecurity policy**.

We would kindly encourage FSB-CPMI-IOSCO to also take into account the **loss allocation policy** that should be applied in case of a non-default event and that should reflect, in a proportional manner, each stakeholders' involvement in the decision-making process that led to the non-default event. Furthermore, EACH is of the opinion that further political guidance on NDLs or on other parts of the FSB-CPMI-IOSCO analysis would not be necessary.