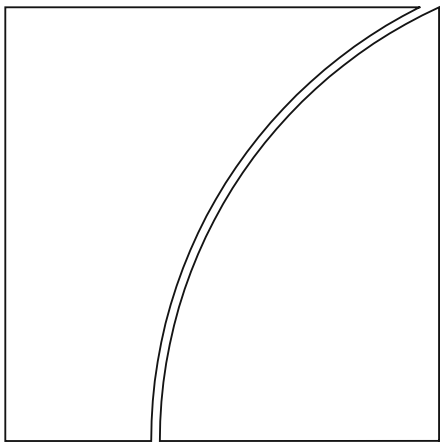
Basel Committee
on Banking Supervision

Consultative Document



Guidelines for counterparty credit risk management

Issued for comment by 28 August 2024

30 April 2024

BIS

This publication is available on the BIS website (www.bis.org).

ISBN 978-92-9259-757-3 (online)

Contents

Guidelines for counterparty credit risk management

Executive summary

In 1999, the Basel Committee on Banking Supervision published *Sound practices for banks' interactions with highly leveraged institutions*.[1] Publication of that report was principally motivated by the collapse of the hedge fund Long-Term Capital Management and associated risk management failures. In recent years there have been additional cases of significant mismanagement of counterparty credit risk (CCR), including events linked to the failure of Archegos Capital Management in March 2021 which caused over $10 billion in losses across numerous financial institutions. Other cases include commodities market volatility after Russia's invasion of Ukraine in 2022 (eg the London Metal Exchange nickel market episode) and gilt market disruption in late 2022 and early 2023. These incidents have made it clear that certain fundamental CCR practices remain inadequate relative to supervisory expectations. Weaknesses pertain to due diligence, both at initial onboarding and on an ongoing basis; credit risk mitigation practices such as margining; risk measurement practices related to potential future exposure and stress testing; and the governance and senior management oversight of CCR.

In response to recent CCR management failings, this consultative document lays out proposed guidelines for CCR management. It builds on *Sound practices for banks' interactions with highly leveraged institutions*, while drawing on other relevant disciplines, such as fundamental credit risk management and market risk management. Although the guidelines discussed in this consultation are intended to be comprehensive, the paper places particular emphasis on key practices critical to resolving long-standing industry weaknesses in CCR management. These include the need to:

- Conduct comprehensive due diligence at both initial onboarding, as well as on an ongoing basis, to ensure banks have a full understanding of the risks they are taking before they make key credit risk decisions, and also that they are able to act swiftly and with sufficient information on the changing risk profiles of counterparties during times of stress.
- Develop a comprehensive credit risk mitigation strategy to effectively manage the inherent risk of their counterparty exposures using robust contractual terms and tools such as risk-sensitive margining.
- Measure, control and limit CCR using a wide variety of complementary metrics while ensuring CCR metrics comprehensively cover the bank's range of material risks, portfolios and counterparties.
- Build a strong CCR governance framework that leverages skilled individuals from across the organisation who have a clear sense of the bank's risk culture; is guided by clear risk management processes, including limits and escalations; and is supported by informative and reliable reporting that is integrated into decision-making processes.

The greatest potential benefit in terms of improvements in CCR management are expected to be in cases where banks have high-risk exposures to non-bank financial intermediary counterparties. The guidelines are, however, designed to be broadly applicable and should, therefore, be used to manage banks' CCR exposures to all types of counterparties. Banks and supervisors are encouraged to take a risk-based and proportional approach in the application of the guidelines, taking into account the degree of CCR generated by banks' lines of business, and their trading and financing activities, as well as the complexity of such CCR exposures.

[1] Basel Committee on Banking Supervision, *Sound practices for banks' interactions with highly leveraged institutions*, January 1999.

The Committee welcomes comments on all aspects of the proposed guidelines from stakeholders. Comments should be submitted by 28 August 2024 using the following link: www.bis.org/bcbs/commentupload.htm. All comments will be published on the website of the Bank for International Settlements unless a respondent specifically requests confidential treatment.

1. Introduction

These proposed guidelines[2] set out critical aspects of effective management of banks' counterparty credit risk (CCR) and sound practices regarding what constitutes a robust CCR management framework. CCR is the risk that the counterparty to a transaction could default before the final settlement of a transaction's cash flows. CCR is a multidimensional form of risk, affected by both the exposure to a counterparty as well as the credit quality of the counterparty, both of which can be sensitive to highly dynamic and fast-moving changes in financial markets. CCR is also affected by the interaction of these risks, for example the correlation between an exposure and the probability of default of the counterparty, or the correlation of exposures among the bank's counterparties. Constructing an effective CCR management framework requires a combination of risk management techniques across credit, market, operational and liquidity risk disciplines.

Recent events, such as the default of Archegos Capital Management, highlighted broad-based weaknesses in areas related to due diligence, risk measurement, risk management and governance. These issues are particularly acute for high-risk counterparties, such as institutions with material concentrations, opaque business activities, limited transparency or high leverage. The risks posed by these weak practices may be exacerbated when competitive pressures in the industry drive a race to the bottom in activities that mitigate risk, such as margining. The sound practices set out in these guidelines aim to address recent CCR management failings. The guidelines build on the Basel Committee on Banking Supervision's *Sound practices for banks' interactions with highly leveraged institutions,*[3] published in 1999, while drawing on other relevant disciplines, such as fundamental credit risk management and market risk management.[4]

CCR management techniques have evolved rapidly over the past decade along with the complexity of derivatives and securities financing transaction (SFT) products, concurrent with the growth in, and banks' interlinkages with, non-bank financial intermediaries (NBFIs), including highly levered institutions. The guidelines aim to take account of market developments in CCR management over the past decade, address recent CCR management failings, and lay out sound practices for CCR management and robust supervisory expectations.

Banks and supervisors are encouraged to use the guidelines to identify potential areas for improvement in CCR management practices. The greatest potential benefit in terms of improvements in CCR management are expected to be in cases where banks have high-risk exposures to NBFI counterparties.[5] The guidelines are, however, designed to be broadly applicable and should, therefore, be

[2] Under the list of Basel Committee on Banking Supervision publication types at www.bis.org/bcbs/help/publ_types.htm, publications classified as "guidelines" supplement standards in many areas, including risk management, corporate governance, anti-money laundering and supervisory cooperation. Committee members are encouraged to adopt guidelines, particularly with respect to internationally active banks.

[3] Basel Committee on Banking Supervision, *Sound practices for banks' interactions with highly leveraged institutions*, January 1999.

[4] For example, see Financial Stability Board, *The financial stability implications of leverage in non-bank financial intermediation*, September 2023.

[5] The Basel Committee on Banking Supervision noted that supervisors consider exposures to highly leveraged counterparties via derivatives and securities financing transactions to be the riskiest. See Basel Committee on Banking Supervision, *Newsletter on bank exposures to non-bank financial intermediaries*, November 2022.

used to manage banks' CCR exposures to all types of counterparties. Banks and supervisors are encouraged to take a risk-based and proportional approach in the application of the guidelines, taking into account the degree of CCR generated by banks' lines of business, and their trading and financing activities, as well as the complexity of such CCR exposure.

2. Due diligence and monitoring

Thorough counterparty credit due diligence is the starting point of a bank's CCR relationship with its clients and it is therefore critical to risk management. Due diligence encompasses a wide range of processes conducted by a bank as it collects information on its counterparty, assesses the level of risk that the counterparty and its activities pose to the bank, and analyses information to make credit decisions. Although aspects of due diligence will differ depending on whether the counterparty is being onboarded for the first time or a review is taking place for the continuation of an existing relationship, a few key sound practices are broadly applicable.

1. Sound management of CCR requires both a strong initial assessment as well as an ongoing understanding of the counterparty's risk profile in both business as usual (BAU) as well as stress conditions. The credit approval process should begin with comprehensive collection and review of financial and non-financial information – including legal, regulatory, reputational and operational risks, as well as other relevant risks – providing a clear picture of a counterparty's risk profile and risk management standards. Additionally, banks should understand the rationale and economics of underlying exposures, and of the key drivers of the counterparties' performance and growth. Banks should be particularly wary of any mechanisms for conducting due diligence and managing material counterparties purely on a portfolio basis without due consideration of the individual counterparties and the risks they pose to the bank. Ongoing monitoring of counterparties requires updated information about material developments such as changes in trading activities and leverage taken, profit and loss developments, as well as significant changes to how the counterparty measures and manages their risks.

2. Credit standards should clearly dictate initial and ongoing due diligence expectations for different types of counterparties and conform to the bank's stated risk appetite. Standards should be appropriately informative, having regard to the product and industry, and be commensurate with the bank's risk profile and business model in that space. Due diligence standards should discuss the frequency and intensity of credit reviews, and be updated as business strategy changes. In some cases, rating scorecards may, with appropriate guidance, serve as a means of stratifying due diligence expectations by counterparty risk.

Onboarding

3. In the onboarding process, banks should ensure that they have a holistic view of a counterparty's potential activities and risks throughout the banking organisation. This process should ensure that onboarding and managing a counterparty's risks across different trading and lending products, and through multiple entities and jurisdictions, is transparent with clear lines of accountability. Economically equivalent risks should be onboarded similarly regardless of onboarding platform, business or legal entity. For example, central versus remote booking should follow the same due diligence process with clear oversight and accountability.

4. Before onboarding a counterparty, banks with sound practices inquire about its past and present reputation and creditworthiness, for example, by accessing credit registers, evaluating legal status, considering regulatory reviews and becoming knowledgeable about the individuals

responsible for managing the institution, including considering any previous supervisory sanctions against the counterparty or the managers. Banks should also assess qualitative factors such as strategy, quality of risk management practices, and staff composition and turnover. However, a bank should not grant credit solely because the counterparty, or key members of its management, are familiar to the bank or are perceived to be highly reputable. Similarly, banks should not unduly rely on profitability considerations when deciding on the onboarding of a new client.

5. Banks with sound onboarding practices recognise that although their initial onboarding decision may be binary, their full credit risk decision-making process can be a spectrum of how much credit and exposure the bank is willing to extend to the counterparty, including the terms of margining used to control the amount of leverage in the trading relationship and transactions with the counterparty. As a result, banks with sound practices demonstrate thoughtful and clear linkages between information analysed during onboarding due diligence and their CCR decisions, including but not limited to risk ratings, limits, contractual terms and risk mitigants (eg collateral and guarantees).

6. Banks should ensure, at the point of onboarding, that their processes consider and assess non-financial risks as part of the credit risk decision-making process. Banks should also establish an escalation process and clear communication channels for the review of non-financial risks. For instance, banks should appropriately characterise the intersection between CCR and geopolitical or country risk. This is a process that may benefit from consultation with the legal department at the point of onboarding. In some cases, risks such as reputational risk may not directly impact the counterparty's capacity to repay – ie probability of default – or immediate financial performance but may introduce other non-quantifiable risks that could materially impact the overall riskiness of the counterparty. These non-quantifiable risks can transform into CCR over the longer term even in cases where no direct impact on the probability of default can be seen.

7. Banks may leverage upstream processes such as those that may already exist in compliance and operational risk management frameworks (eg know-your-customer) to inform and drive assessments performed in the credit risk decision-making process, rather than replicate capabilities across functions. Banks should ensure that established processes are effective in directing or channelling relevant and material considerations – including those of non-financial risks – to credit risk analysis and to the decision-making process. They should also ensure that credit risk management processes adequately evidence analysis and outcomes in decisions.

8. Banks should collect sufficient information during onboarding to understand the client's overall risk profile. In some cases, the collection of financial statements alone is insufficient to assess the riskiness of a counterparty. For example, risky and complex counterparties should provide additional disclosures and risk metrics – such as value-at-risk or stress test results – so that banks have visibility into the counterparty's own assessment of their underlying leverage and risk profile. When counterparties share internal risk reports produced on a regular basis, the bank should use these reports to gauge the quality of the counterparty's risk management capabilities and practices.

9. The credit process should identify the purpose and structure of the transactions for which approval is requested and provide a forward-looking analysis of the repayment capacity based on various scenarios, including stress testing and analysis of idiosyncratic circumstances that could present material risks to the client. Banks should have a good understanding of key assumptions made about a counterparty's risk profile when establishing a relationship with them – such as their level and sources of liquidity and how the orderly liquidation of underlying positions might occur – to facilitate a deeper understanding of the inherent riskiness of the underlying trades with the counterparty, including market directional risk, excessive concentration risk, idiosyncratic risks and wrong-way risk (WWR) arising from the dependency

between client default and its underlying exposure. More generally, banks with sound practices have a framework to directly incorporate the quality of counterparties' disclosures into the conditions of doing business, including but not limited to the level of margin requested, limit setting and/or the internal risk rating process. Policies should clearly articulate the information required in disclosures. After the information from the client has been received, banks should also ensure that adequate proof, assurances or verification are applied as part of their due diligence processes. This type of practice helps ensure that credit risk decisions are not made based on unverified or verbal information. In some cases, banks may benefit from engaging third-party information verification services. This framework should include minimum standards on counterparty disclosure, including an exception process, in addition to requirements for limit setting, margining or other mitigants. A client's failure to provide information should lead to a more conservative approach to limit setting, margining and other forms of credit risk mitigation, or even the rejection or offboarding of the client. As noted previously in this section, the credit risk decision-making process can include a spectrum of the exposure, limits and mitigants a bank is willing to extend to the counterparty.

10. Banks are expected to review proposed trading positions or sample portfolios to assess the underlying risks inherent in the activity that the bank will be financing. Banks with sound practices apply this review whenever onboarding new clients, new funds or approving new types of trading activities for existing clients. This analysis should span at least the main internal metrics used for risk monitoring – including BAU and stressed exposures. In the case of new trading positions of existing clients, the incremental impact of the new positions should be assessed against the existing risk limits for the counterparty. Better due diligence practices incorporate specialised evaluation and technical knowledge on industries such as commodities, where terms vary significantly depending on the type of product being traded and collateral obtained.

Ongoing credit assessment

11. Banks with sound due diligence processes understand that due diligence obligations do not end following the initial onboarding of a counterparty. Instead, they recognise the need to continually receive and assess information that sheds light on a counterparty's risk profile. For example, banks should obtain information about material counterparty developments such as changes in the direction of their trading activities and performance (eg net asset value (NAV)), profit and loss developments, significant changes to leverage, alterations to their risk management procedures or their risk measurement processes, and changes in key personnel. Banks with sound practices rigorously explore whether high returns shown in a counterparty's portfolio are associated with higher risks that have not been properly considered, or represent unknowns and cannot be substantiated without overreliance on the clients' representations.

12. Following the characterisation of the counterparty's risk profile at onboarding (such as through proposed trading positions or sample portfolios noted earlier in this section), deviations from the risk profile should be tracked and lead to adjustments in the ongoing monitoring process as appropriate. Banks should also establish a frequency for ongoing monitoring and predefined triggers for metrics such as performance, volatility, liquidity, management quality and concentration, which should be commensurate with the risk presented by the client under normal and stressed market conditions. The frequency of ongoing monitoring should also take into account the assessment of a counterparty's non-financial risks.

13. Banks with sound practices monitor the timeliness and quality of financial statements and risk information provided by the client on an ongoing basis and track exceptions to established policies at the counterparty level as well as at aggregated portfolio levels. Further, banks should ensure that all information relevant to a counterparty credit relationship, including risk analysis

performed by the counterparty, is made available to the bank on a sufficiently timely and ongoing basis, including on an on-demand basis when warranted. Banks should also consider an exit policy from the contract if the client fails to deliver key due diligence information.

14. An internal risk rating system used to assess and monitor the quality of individual counterparties and across the portfolio should be suitable for and commensurate with the nature, size and complexity of a bank's activities. For counterparties with CCR exposures, due consideration should be given to the dynamic nature of these relationships, as mark-to-market (MTM) exposures can change materially over short time frames that may require updated credit risk assessment and decisions. The frequency of internal risk rating reviews for these counterparties should account for the dynamic nature of their positions and the risk rating process should ensure that any material change in the counterparty's leverage or risk profile should trigger a revised assessment. These revisions should include, but are not limited to, the risk rating score, products allowed for the relationship, margining terms, and exposures and concentration limits.

15. As part of ongoing monitoring, banks should track non-standard contractual terms that are outside the bank's credit policy standards and assess the potential need for adjustments to terms, where necessary, to further enhance their credit risk mitigation. Notwithstanding these practices, banks should not rely solely on strong contractual terms and the ability to closeout transactions with a client to negate the need to conduct proper risk management. Similarly, covenants should facilitate the timely monitoring of a counterparty's risk profile so that banks are aware of adverse financial events and take actions to adjust or mitigate the exposure before the need arises to close out the client relationship.

3. Credit risk mitigation

Credit risk mitigants are tools that are necessary for banks to effectively manage their CCR. Margin is the primary component of risk mitigation for CCR exposures and, in some cases, banks may also choose to rely on other risk mitigants to support credit risk decision-making. These mitigants can range from contractual terms to cross-collateralisation and written guarantees, all of which can provide additional risk mitigation. In many cases margin is necessary but may not be entirely sufficient to mitigate risk without due consideration of other factors such as the creditworthiness of the counterparty, the frequency and reliability of the disclosures, the level of transparency in the overall counterparty's risk profile and the riskiness of the counterparty's positions relative to market depth and conditions.

Regardless of the credit risk mitigants, bank policies and procedures should determine the necessary and allowable contractual provisions that govern counterparty relationships and help mitigate CCR, including the circumstances under which these clauses may be reviewed. These legally binding and enforceable contractual arrangements – coupled with the bank's limit frameworks – determine the size of credit exposure assumed by the bank. It is therefore paramount that, in calibrating these contractual terms, there is close consideration of the nature and creditworthiness of the counterparty, the riskiness of its underlying exposure to the bank, and the overall transparency of the counterparty with respect to its positions and trading strategy. For example, banks should request higher margin when faced with a lack of disclosure and should frequently monitor margin shortfall vis-à-vis the underlying risks.

The next section discusses sound practices regarding margining and risk mitigation of CCR exposure.

Margining

16. Banks with sound practices develop and implement a transparent and robust margining framework that is consistent across all trading products and onboarding platforms. Such practices are reflective of underlying risks and the bank's risk appetite. As a minimum, the margin framework should adequately capture both the market and liquidity risks associated with the portfolio (including valuation risks), the quality of collateral received, as well as the credit risk associated with the counterparties.

17. Margin levels should account for the market risk of the portfolio and be sensitive to changes to the counterparty risk profile and underlying risks. For example, the margin for hedge fund exposure should be sensitive to the implementation of new trading strategies, as well as changes in portfolio directionality, concentration or leverage. Other factors to consider include market conditions impacting the underlying trading activity, such as increased volatility, crowdedness, liquidation and liquidity. The sophistication of margining frameworks should be commensurate with the complexity of banks' portfolios. Computed margins for a particular counterparty should be reflective of its specific portfolio vulnerabilities and exposures, and capture material risks at the single name and risk factor level. Banks should also require margin levels that reflect risks arising from other contractual terms such as early termination, margin lock-up and frequency of margin resets, among others.

18. The margining framework should be informed and reflective of the overall risk profile of the counterparty and not merely based on the narrow risk profile of the bank's trading relationship with the counterparty. For example, banks should review and rely on a counterparty's financials and internal risk assessment, including its jurisdiction risk and stress testing, to infer risk taken outside its portfolio. NAV volatility and growth should inform the riskiness of a counterparty's underlying assets. For gathering this information, banks and their counterparts can agree to rely on professional third parties to calculate and share risk measures and stress results on an adequate, mutually agreed aggregation level. This approach is especially encouraged when counterparties do not have a sophisticated risk calculation framework and/or financial disclosure obligations, as an alternative to infrequent information-sharing or lack of disclosure on meaningful financial indicators.

19. Banks should avoid opaque margining frameworks that lack effective oversight and fail to ensure that risk-sensitive margins are charged on trades or portfolios at the inception of the relationship and on an ongoing basis. Additionally, banks should not engage in margin customisation or deviate from approved margin policies to accommodate commercial or competitive pressures without appropriate governance and the support provided by margin sufficiency benchmarking.

20. Banks with sound practices have systems, policies and procedures to monitor the effectiveness of their margining frameworks and methodologies, which should be periodically reported to banks' senior management. Margin frameworks should be subject to ongoing monitoring and governance related to margin sufficiency, underlying assumptions, contractual terms and limit setting and risk appetite. The monitoring should be undertaken on both the counterparty level and on an adequate portfolio aggregation level. House margin frameworks should undergo a level of governance and scrutiny that is proportionate to their materiality. As part of this, margin frameworks should be back-tested using realised historical exposures as well as stress scenarios. For details on risk reporting, refer to the section titled "Management reporting" in Chapter 5 of this consultative document.

21. Banks should regularly reassess and test the assumptions underlying their margining models. Banks with sound practices test both the appropriateness of the margin over time and reassess the assumptions underlying their margining models. Such models should be subject to proper review and challenge, including initial and ongoing independent reviews.

22. Banks should establish a formal risk appetite for deviations from their margin terms and monitor exposures against it.[6] A clear governance framework should also establish escalation procedures in cases in which the appetite for risk is exceeded.

23. Initial margin (IM) requirements are a particularly important part of a margining framework. They represent the amount of collateral necessary for absorbing potential losses in relation to a particular trade or portfolio of trades that may arise in the time between the last exchange of margin, and the liquidation or hedging of the positions. Such margin is either static, or re-evaluated and adjusted over time (ie dynamic) to reflect changes in a portfolio's risk. When adopted, static margin should be set conservatively to cover unexpected changes in underlying exposure to market value and riskiness.

24. Variation margin (VM) is another important component of the margining framework, generally defined as the amount of collateral necessary to cover the current portfolio exposure, accounting for changes in the MTM valuation of the positions on a contractually agreed frequency. Banks with sound practices have rigorous and robust margin (IM and VM) dispute resolution procedures in place with their counterparty, and, to the extent possible, apply daily variation margin to all material counterparties with zero thresholds and small minimum transfer amounts.

25. Banks should ensure that contractual terms stipulating two-way variation margin do not exacerbate risk by increasing the counterparty's leverage and its credit exposure. In granting two-way margining and rehypothecation rights, banks should give due consideration to the credit quality of the counterparty and the riskiness of the underlying exposure, including collateral. If banks agree to two-way collateral provisions, they should make sure that the resulting additional exposure – of the posted collateral – is monitored and fully integrated in the overall risk management and measurement processes.

26. Banks should assess the need for margin based on the risks and vulnerabilities of the traded positions. For example, banks should assess the margin sufficiency – estimated margin based on underlying risks versus required margin – of all traded products regardless of product type and if the exposure is cleared versus non-cleared and consider the risk of potential delay in margin delivery as well as substitution of collateral, if contractually permissible

27. In managing the risk of counterparties at low risk of default, banks should not have a double benefit from collateral in the measurement of both default and exposure risks. Further, in dealing with highly rated counterparties, banks should assess margin needs based on the riskiness of the underlying exposure, including collateral being posted. Similarly, default risk should not be assessed based solely on the lower risk of the underlying exposure to counterparties due to perceived diversification or market neutrality in long/short types of exposure.

28. Banks should establish policies and methodological frameworks that define eligible collateral and quantify the haircuts to be applied to SFT exposures. Banks should also ensure that haircuts and variation margin for SFTs reflect the underlying risks of the counterparty and riskiness of the exposure, and that initial margin is applied consistently across similar products. Banks with sound practices make SFT haircuts dependent on both the riskiness of the security and on the riskiness of the counterparty.

29. When acting as agents for derivatives transactions, banks should make their own assessment of adequate margin levels for their counterparties. Banks with sound practices do not simply pass on the clearing house or regulatory margins to their counterparties, but rather determine margin

[6] For example of related guidance, see Prudential Regulation Authority and Financial Conduct Authority, *Supervisory review of global equity finance businesses*, December 2021.

sufficiency based on their internal risk assessment. Banks with sound practices have processes to determine if and when they may need to consider applying margin multipliers.

30. Banks should pay particular attention to situations in which margin and collateral established to cover counterparty credit exposures may be significantly reduced if the probability of the counterparty's default is negatively correlated with the value of the collateral or positively correlated with the market value of the contracts.

Guarantees and other risk mitigants

31. Bank policies and procedures should determine the range of allowable credit risk mitigants. These policies should ensure that the usage of mitigants is controlled and monitored appropriately across the bank's portfolio. Furthermore, they should closely relate the allowable mitigants to the credit worthiness of the counterparty and the riskiness of the underlying exposures.

32. Contractual provisions that govern counterparty relationships are a particularly important consideration. Banks with sound practices clearly define the types of allowable and necessary contractual terms which impact CCR – including, for example, early termination rights, margin lock-up agreements and default notification periods – and ensure contractual terms are clearly considered when setting limits and risk appetite for trading with a counterparty.

33. Additionally, the contractual terms of specific trades have significant impact on their risk profile, as certain trades can either generate additional risk or mitigate risk based on the features of the trade. For example, banks should be aware of uses of derivatives such as a bullet swap, which if left thinly margined or unmargined, can present elevated risks when compared with a similar resetting swap.

34. Banks should assess the legal enforceability of all credit risk mitigants and incorporate potential delays in accessing collateral when measuring exposure and margin. This review should consider not just differences in relevant jurisdictions, but also differences across products and collateral types.[7] For example, this practice should determine the criteria under which the protections provided by the legal framework are enforceable to the benefit of the creditor.

35. In situations in which a bank has CCR exposure to a counterparty who – as a standalone legal entity – is not a creditworthy entity, the bank may seek a guarantee. Banks with sound practices assess the credit quality of the guarantor to ensure they can rely primarily on written guarantees that contractually obligate a guarantor to support the obligations of the bank's counterparty.

36. In other situations, there could be a support provider without an explicit written guarantee. In such cases, banks should establish a robust framework to assess the likelihood, willingness and capacity of a support provider to step in and provide support. In all cases, banks should ensure that consideration of implied support is not considered equivalent to written guarantees, and appropriately discount the strength of implied support when making decisions about other risk mitigants that should be obtained. This is especially important when a bank has significant trading activity with subsidiaries which rely on parental support to substantiate credit risk decisions.

37. Banks may obtain written guarantees that are capped, limiting the amount of exposure guaranteed by the guarantor. In the context of CCR exposures, which can increase rapidly as the market environment changes, banks should ensure they have processes to assess the use of

[7] See Committee on Payment and Settlement Systems and the Euro-currency Standing Committee, *OTC derivatives: settlement procedures and counterparty risk management*, September 1998. The report discusses legal risk associated with collateral.

capped guarantees, including guidelines for sizing and monitoring current or potential exceeding of the cap.

4. Exposure measurement

CCR default losses are often driven by tail events, such as large and sudden asset moves or the unforeseen occurrence of unusual market scenarios, the impact of which, on the solvency and portfolio performance of certain counterparties, can be dramatic. Moreover, CCR is by nature multi-dimensional, involving up to several thousand counterparties and a much higher number of underlying assets, combined in portfolios of trades spanning all sorts of risk configurations: linear and non-linear, concentrated and diversified, hedged and directional.

Dealing with this plethora of different risk profiles, and specifically with their tail behaviour, requires that banks, in managing CCR, should rely holistically on a variety of non-equivalent risk metrics that assess all the material dimensions of CCR. Such metrics should provide a complementary and comprehensive view of risk, covering for both BAU and stressed market conditions, as well as for any material vulnerability to specific idiosyncratic risks. The signal of these metrics should be calibrated with a sufficient level of conservatism, aimed at compensating for the inherently large model risk of the quantitative methods used.

Exposure metrics

38. CCR exposure metrics for a given counterparty should be computed with appropriate consideration for the level of aggregation embedded in the calculation. Exposure metrics should be produced frequently and in a timely manner and include all trades giving rise to CCR, across product types (eg bilateral, centrally cleared and exchange traded derivatives and SFTs), as well as across business lines and legal entities. In addition, the CCR risk monitoring process should be fully informed of any additional credit exposure with the counterparty, such as loans outstanding or unused credit commitments.

39. CCR exposure metrics should be comprehensive in covering banks' material risks at portfolio, counterparty and a more granular risk factor level. For every counterparty, exposure metrics should account for the contractual terms – and for their inherent risks, eg related to netting and collateral enforceability – and be consolidated across product types, desks and books. Overall, this suite of metrics should provide a holistic view of the characteristics of the entire distribution of CCR exposures, including average, high quantiles and residual tail risks. Residual tail risks can be very significant for counterparties such as highly leveraged institutions in which solvency, liquidity or both closely depend on portfolio performance.

40. Exposure metrics should be actionable and embedded in the different stages of the CCR management process, including: (i) pricing and setting of the contractual margins (eg x-value adjustment (XVA) and initial margin methodologies); (ii) risk monitoring (eg potential future exposure (PFE) and stress testing); and (iii) capital assessment (standardised approach for counterparty credit risk (SA-CCR), internal models method (IMM) when applicable, and stress testing). Such metrics should supply the bank with an ongoing, timely and accurate view of the counterparty's exposures. When relevant changes occur either in the portfolio or with the risk profile of a specific counterparty, such changes should be promptly reflected in the exposure metrics.

41. The metrics in use to quantify risk at any stage of the CCR management should undergo the appropriate level of internal governance and independent review applicable to the models used, irrespective of any perceived analytical simplicity. This should include the initial and ongoing

review by an independent validation unit. As part of the challenge process for the metrics, end users as well as senior management could be actively involved by means of reviewing parallel runs, impact studies and concrete examples based on existing and/or historical portfolios. Stakeholders should maintain a sound understanding of (i) the risks captured by each of these risk metrics and (ii) the inherent limitations of these risk metrics.

42. Related to the previous paragraph, end users and key stakeholders should be provided with a clear and actionable taxonomy of the supported CCR metrics – including their range of applicability and known limitations – across counterparty groups, product types and contractual arrangements. Such taxonomy, given its central role within the CCR management process, should be reviewed by an independent validation function and agreed by all the relevant risk committees.

43. The exposure metrics, collectively, should provide complementary risk capture and allow banks to have visibility of material drivers of exposure under BAU and stress conditions. Such drivers should account for potential structural risks and vulnerabilities of the positions – considering factors such as leverage, concentration, liquidity and WWR – even when they cannot be fully characterised because of partial information regarding the true risk profile of the counterparty. In a similar fashion, exposure metrics should account for the possibility that perceived risk mitigants or diversification benefits may not work as intended. For example, PFE, as well as IMM and CVA EE profiles, generally produce hardly any actionable signal for over-collateralised counterparties (such as hedge funds or other highly leveraged institutions), since they are often computed ignoring (at least general) WWR and the possibility of margin-driven defaults.[8] Therefore, such metrics should be complemented by additional metrics that better capture the residual risks.

44. In measuring exposure, banks should properly identify, evaluate and capture idiosyncratic risks such as excessive concentration to a single name or single risk factor, material dispersion or basis risk between long and short positions, lack of liquidity due to limited trading volume, the presence of complex or bespoke positions in the portfolio, or simply the sheer position size. Banks with sound practices directly consider how such idiosyncratic risks may affect portfolio correlations and the accuracy of valuations used to determine margins. They should also consider how such risks may exacerbate WWR and ultimately magnify closeout losses. In this context, the overall risk profile of the counterparty should be modelled conservatively, giving due consideration to scenarios such as horizontal hoarding or crowding that can materially skew the exposures distribution.

45. Beside PFE and stress-based exposures (see the next two sections), banks should monitor their aggregated CCR position and the risk profiles of their counterparties using simple and intuitive risk metrics that are model-free, ie solely based on the structural features of the portfolios. These metrics should provide indicative CCR losses in extreme market scenarios, such as a sudden breakdown in asset correlations, a major liquidity dry up or other idiosyncratic events in specific underlying or country/regional turmoil directly affecting the solvency of local counterparties.

46. Examples of sound practices of metrics described in the previous paragraph – either at the counterparty or bank's portfolio level – include: (i) gross notional amount or gross market value (a tool to identify a vulnerability to the breakdown of specific long/short hedges within a counterparty's portfolio); (ii) gross trades' delta exposure (a tool to identify, either at the counterparty or bank's portfolio level, a potential exposure concentration in specific risk factors);

[8] In the case of Archegos Capital Management, the default event was triggered by a massive VM margin call that was not met. It was originated by large gap moves in a few correlated technology stocks. Whereas PFE and IMM/CVA EE profiles are generally computed according to a smooth default paradigm, with closeout losses solely driven by stochastic fluctuations of trades and collateral values over the MPOR horizon.

(iii) received and posted collateral composition (a tool to identify, at the bank's portfolio level, a potential concentration in specific collateral assets); and (iv) country or regional gross exposure (a tool to identify, at the bank's portfolio level, potential exposure concentration with regard to countries or regions with significant geopolitical risk).

47. Institutions should have a dedicated WWR framework in place that is integrated into the general risk assessment framework and gives due consideration to both general wrong-way risk (GWWR) and specific wrong-way risk (SWWR). The WWR framework should be commensurate with the risk appetite and be designed to effectively allow the identification, measurement, monitoring, regular reporting, limit setting and explicit treatment of exposures giving rise to WWR. Such a framework should explicitly account for relevant risk factors, going beyond mere compliance with regulatory requirements. This is specifically relevant for counterparties whose business strategy is particularly vulnerable to certain market risk scenarios, including those with high leverage and other specific structural features of their portfolio.

48. To identify and monitor GWWR, banks should have clear definitions in place in terms of the risk categories applicable to their portfolios, including industry, region, business areas, products and any additional relevant dimension. The regular GWWR identification process should be supported by well defined stress testing based on scenarios of credible severity that are reported with appropriate frequency to senior management.

49. Banks' processes and methodologies for SWWR assessment and monitoring should be well defined and documented. They should enable the identification of correlations between a counterparty's creditworthiness and the CCR exposure to the counterparty. The SWWR classification should be based on a clear definition of legal connection that considers legal frameworks on ownership, including control or consolidation requirements. In addition, banks should also consider applying the SWWR classification to cases with no strict legal connection but where the counterparty is significantly economically dependent on its underlying exposure. The results of the regular SWWR identification process should be reported with adequate frequency and escalated to senior management where necessary.

Potential future exposure

50. Banks should quantify CCR exposure daily, using PFE to measure the future exposure against a given counterparty conditional upon its default. PFE is a risk metric calibrated on BAU market conditions that quantifies, over a defined future horizon and at a specified confidence level, how sizeable the CCR exposure of a given counterparty's portfolio may become given the applicable contractual terms and credit risk mitigants. PFE is predominantly computed based on scenarios generated with Monte Carlo simulations,[9] considering multiple forecasting horizons (typically up to the life of the contract) and a high percentile (eg 95% or 99%) of the simulated portfolio exposures distribution (alternatively, expected shortfall measures linked to such confidence levels are used). For risk monitoring, when calibrating PFE, banks should have due regard to model specifications such as the parameterisation of the stochastic risk factor dynamics (including jump processes or similar ways to model gap moves of the underlying assets), as well as the applicable margin period of risk (MPOR)[10] and collateral haircuts.

[9] For products in scope of IMM, the PFE is based on the same scenarios and valuation framework used to compute the Pillar 1 expected exposure (EE) profiles and effective expected positive exposures (EEPEs).

[10] For the Basel Framework definition of MPOR, refer to the calculation of risk weighted assets (RWAs) for credit risk (CRE) 50.19. In the case of collateralised counterparties, the PFE should consistently account for both the trades' MTM and the collateral, and the forecasted loss materialises over the MPOR after the default event. Specifically, for a default horizon h, the PFE is generally computed as the closeout loss (trades' MTM minus collateral) accrued between h and h + MPOR.

51. While using PFE to monitor BAU risk limits at counterparty and product levels, banks should ensure that the counterparties' PFEs are: (i) reflective of the contractual terms, including trade attributes, netting and collateral requirements; (ii) computed and monitored across all the applicable risk horizons; (iii) based on risk scenarios that conservatively account for the stochastic behaviour of the portfolio's material risk factors and the collateral dynamics over the MPOR; (iv) computed with a sound modelling of correlations among risk factors and of any risk basis (eg long/short positions with residual dispersion) that may materialise in ordinary or distressed markets. In general, banks should be conservative in their treatment and modelling of excess collateral received from counterparties.

52. Banks should adjust the MPOR to account for excessive risks driven from concentrated and/or illiquid portfolios or collateral and give due consideration to related idiosyncratic risks that can materialise upon the default of the counterparty, such as crowding during liquidation and a consequent large drop in the value of the assets. Such risks should primarily be addressed by: (i) a suitable framework able to quantify the closeout MPOR for every counterparty based on its risk profile and portfolio; and (ii) for potentially illiquid counterparties, by simulating the portfolio dynamics with stochastic models calibrated to a level of distress commensurate with the market risk of liquidating highly concentrated positions. It is noteworthy that in the case of Archegos Capital Management (whose closeout period was not unusually long), forecasted PFE was less than a tenth of the realised closeout losses. Further, the ex post MPOR that would have been required to truly account for the impact of concentration and of a disorderly liquidation was a very large multiple of the baseline MPOR values applicable to SFT and bilateral over the counter (OTC) portfolios.[11]

53. PFE as a measure of exposure at default should account for WWR (directly or via suitable adjustments or overlays). This is especially relevant for NBFIs, particularly institutions with high leverage and/or concentrated exposures, whose solvency, because of the leverage and concentration, becomes materially correlated with the portfolio performance. In such cases, banks should calibrate the PFE to historical and idiosyncratic scenarios commensurate, for instance, with those observed during the Archegos Capital Management and Long-Term Capital Management defaults, when WWR drove large gap moves for the underlying portfolio assets and ultimately magnified the closeout losses.

54. Banks should be mindful that plainly offsetting the scenarios trades exposures with the forecasted level of IM (in addition to any applicable VM) may result in zero or negligible PFEs for collateralised counterparties.[12] This perspective does not account for the material risk of margin-driven defaults, where the available IM may not compensate for the large VM collateral shortfall originated by a sudden gap move of the underlying portfolio assets (for instance, driven by the leverage/WWR dynamics previously discussed). This scenario is especially relevant for highly levered institutions, particularly those that take excessive leverage and have significant concentrations.

[11] See Credit Suisse Group Special Committee of the Board of Directors, *Report on Archegos Capital Management*, July 2021. On the basis of publicly available information contained in the above-mentioned report, Archegos Capital Management's PFE with Credit Suisse prior to default was approximately $500 million versus a final closeout loss of approximately $5.5 billion, with a total excess margin held by Credit Suisse of approximately $1 billion. Based on these figures, and assuming that the original PFE was computed with MPOR = 20d (see footnote 94 of the above-mentioned report), a back of the envelope $\sqrt{T}$ scaling calculation indicates that the ex post MPOR required to match the realised losses would have exceeded 1y.

[12] For standard PFE Implementations, this is generally the case by construction for various reasons: i) the VM at scenario level is obtained by matching the current level of the trade exposure at default; ii) the IM is calibrated to compensate for adverse portfolio moves over the MPOR at a high level of confidence; and iii) as a result of i) & ii), the scenarios with material exposure at closeout are very few, and much deeper in the tail compared to the quantiles at which the PFE is typically calibrated.

55. When relying on PFE to manage CCR, stakeholders should maintain a sound understanding of both the risks captured by the metric, as well as its inherent limitations. Such limitations should be documented and reviewed on an ongoing basis and compensated in the CCR management process by assessing exposures using complementary risk metrics based, for example, on factor sensitivities, aggregation on a gross basis and stress testing.

56. As part of the ongoing model governance, PFE should be back-tested using both real and hypothetical portfolios, so as to extensively probe the modelling assumptions versus the realised historical markets. In addition, banks should benchmark their PFE models versus the realised dynamics of well publicised defaults such as Long-Term Capital Management and Archegos Capital Management. They should assess: (i) if their PFE model is able to produce commensurate exposures at realistic quantiles; and/or (ii) if the banks' overall CCR management framework has adequate compensating measures able to flag an excess of CCR for similar portfolios.

CCR stress testing and scenarios analysis

57. As a complementary and necessary metric to PFE, banks with sound practices have developed a dedicated CCR stress testing framework for an assessment of counterparties' exposures in a stressed market environment, where the resulting stressed exposures are fully integrated in the bank's BAU risk management process and monitored against limits. This is especially relevant for exposures to NBFIs for whom stress testing may be the only systemic approach to identify and quantify the main portfolio's vulnerabilities.

58. Banks should have clear, documented governance of their CCR stress testing framework to ensure the appropriate identification of relevant scenarios, their design and revision when necessary. The framework should include a robust number of scenarios, exhaustive of the multi-dimensional nature of the risks to which the bank's portfolio is exposed. In addition, institutions should have the capability to perform in a reasonably short time ad hoc stress tests, reverse stress testing and scenarios analysis. Based on the business model of the counterparty, it should be able to characterise extreme but plausible scenarios that could result in significant adverse outcomes.

59. CCR stress testing should be implemented consistently across all business lines and products in terms of the stress scenarios considered. Banks with sound practices apply market shocks simultaneously both to the trades as well as collateral. The resulting counterparty's exposures should be compared with risk limits at granular counterparty as well as aggregated portfolio risk levels. The CCR stress testing framework should inform the bank's day-to-day exposure and concentration risk management and be able to identify extreme market conditions that could excessively strain the financial resources of the bank.

60. As part of CCR stress testing, a comprehensive set of severe stress tests shall be performed at the counterparty and portfolio levels, applying both different macroeconomic scenarios and dedicated combinations of shocks to risk factors able to identify counterparties' material vulnerabilities. In order to provide a realistic assessment of exposures to counterparties under stress, these scenarios should be granular at the level of material risk factors, informed by vulnerability analyses – severe and varied – and able to capture idiosyncratic risks such as concentration in a single name, sector, geography, tenor, risk rating etc, as well as dispersion, basis risks and liquidity issues.

61. In designing scenarios for CCR stress testing, due regard should be given to (i) historical events; (ii) the current macroeconomic and financial environment; (iii) hypothetical future events,

including new information and idiosyncratic and emerging risks.[13] Regarding the latter, an effective design process should consider specific hypothetical geopolitical or natural disaster scenarios that for some counterparties – eg in the commodities or insurance sectors – are more likely to be the ultimate drivers of the exposure conditional upon default. Overall, a comprehensive CCR stress testing assessment should entail an in-depth review of the counterparty business model and of its portfolio structure. Direct and reverse stress testing, as well as scenario analysis, should be used as active tools to identify and quantify the main portfolio vulnerabilities.

62. When conducting CCR stress testing, banks should test for situations in which risk mitigation measures do not work as intended, especially under stress or counterparty default conditions. This may entail challenging the strength of assumptions made about the legal enforceability of contracts (eg under specific geopolitical risk scenarios in certain jurisdictions), of netting and portfolio diversification, the ability to collect and liquidate collateral, or benefit from any other risk mitigation measures. Stress testing the collateral should provide the institution with an alternative view of their CCR that is not shown when relying solely on PFE. The importance of this is clearly highlighted by the Archegos Capital Management case, in which the realised VM collateral shortfall at default for one of the exposed broker-dealers was more than $1 billion, as compared with no projected shortfall under the PFE metric.

63. The stress testing scenarios should appropriately capture the impacts derived from the costs of winding down portfolios or netting sets comprising less liquid collateral or transactions that are hard to replace after default by the counterparty. In the absence of reliable information on horizontal concentration in portfolios maintained with high-risk counterparties, the stress testing framework should incorporate conservative assumptions with regard to the bank's capability to wind down the defaulted position under stressed market conditions, paying due consideration to measurement of the potential market risk losses derived from unmatched hedging positions upon the default of the counterparty.

64. The CCR stress testing framework should pay particular attention to riskier counterparties as well as to the identification of counterparties for which certain market scenarios could lead to acute stress on their solvency or liquidity positions and are, therefore, particularly vulnerable to exposure tail events. The resulting stressed exposures enable the institution's risk management function to: (i) identify particularly vulnerable counterparties under certain scenarios; (ii) identify the most relevant scenarios for the overall institution's CCR portfolio; and (iii) report the conclusions to senior management to support quick decision making. Senior management should take a leading role in the integration of stress testing into the risk management framework and risk culture of the institution. Senior management should also ensure that stress testing exposures becomes an integral part of the CCR decision-making process.

65. As part of the governance of the CCR stress testing framework, the scenarios, as well as any other key modelling inputs used in computing stressed exposures, should be reviewed periodically by end users and key stakeholders in order to ensure ongoing comprehensiveness, granularity and relevance.[14] This periodic assessment should include some level of benchmarking for the severity of the applied shocks, eg performed by comparing the resulting stressed exposures with historically realised exposures for, at least, the most material and/or vulnerable counterparties.

[13] Scenarios not based on historical events and empirically observed relationships may be warranted for some or all risks if new or heightened vulnerabilities are identified, or if historical data do not contain a severe crisis episode or idiosyncratic risks such as excessive concentration, liquidation, WWR or the geopolitical and natural disaster events mentioned in the main text.

[14] For example, when designing stress scenarios, banks should not rely solely on parallel shocks, ignoring dispersion among tenors, sectors, ratings, currencies, long/shorts etc. Instead, stress test metrics would also need to calculate the MTM of the exposure under instantaneous market shocks.

Limits

66. It is essential that banks develop comprehensive and effective limit frameworks that allow for monitoring and control of the bank's exposures to its counterparties at both the individual counterparty level as well as the aggregate portfolio level. Banks with sound practices leverage their suite of exposure metrics when designing a limit structure, in recognition that any one metric and limit has weaknesses. Broadly speaking, a bank's limit structure should cover a range of both BAU-based exposure metrics and stress-based exposure metrics that can include, for example, current net exposure, PFE, gross notional amount or gross market value, as well as other stress-based measures.

67. Risk limits should be granular enough to monitor key risks – eg concentration, liquidation, dispersion and maturity – in the underlying exposure to a counterparty at the material risk factor level. Risk limits should also capture all the credit exposures to the counterparty across all products and financial relationships within the banking organisation. Banks should ensure that risk aggregation practices, for the purpose of limit setting, are accurate and reliable.

68. Effective limit frameworks should be calibrated with severities – eg 99th percentile – that are consistent with those of the risk metrics being controlled and monitored. Risk limits should not be set so high such that they would lead to excessive buildup of risk and prevent a bank from taking the necessary actions to effectively reduce the level of exposure in a timely manner. Additionally, risk limits should not be set too low such that they do not serve as a credible reflection of the bank's risk tolerance.

69. Banks should ensure that limit calibration processes are rigorous and subject to independent review and challenge. Limit frameworks should be recalibrated with reasonable frequency as well as, at a minimum, upon changes in market conditions, business strategy, business organisation, risk measurement methodologies, riskiness of the counterparty and riskiness of its underlying exposures.

5. Governance

A solid governance for CCR relies on three pillars. The first pillar consists of competent people and the right risk culture in the organisation. The second pillar is the adequate strategy for managing CCR with clear processes and effective limits in place. The third pillar is the management reporting and its integration into the decision-making process. This management reporting should enable swift analyses of key CCR in any market situation.

People and risk culture

70. Banks should foster a culture across the bank that ensures understanding of all risks with accountability for taking risk management actions when necessary. Banks with sound practices have clear lines that link CCR management reporting and metrics to risk-taking or reducing decisions in a way that is consistent across business lines.

71. Banks should foster a culture that values the important role played by data and models in managing CCR. The culture of a bank should encourage an appropriate degree of confidence in data and models underlying CCR management, balanced by an appropriate level of challenge and an awareness of limitations.

72. The dual nature of CCR contains elements of both market risk and credit risk, necessitating that CCR management involves strong collaboration between the market risk and credit risk functions at the bank. Banks with stronger practices have dedicated functions for CCR. At a minimum, the bank's risk culture should foster strong collaboration, including but not limited to knowledge and information transfer between the market and credit risk departments. Therefore, banks should prevent siloed thinking in their risk departments and strongly encourage the exchange of information gathered, in particular on market or credit risk that may be relevant for assessing the credit risk of a counterparty or potentially market distorting events due to the deteriorating credit quality of a counterparty.

73. Banks with sound practices demonstrate that risk management oversight is conducted by risk managers with clearly defined roles and responsibilities and appropriate levels of authority, including exception approval and a clearly defined and actionable escalation framework.

74. Banks' CCR managers need to have experience, expertise and stature sufficient to understand CCR and interact with counterparts in trading businesses and with the bank's most senior managers, including the risk committees of the boards of directors. Banks should appoint managers that have a reasonable level of understanding of CCR from both business and risk perspectives, as well as an understanding of how data and models are used in assessing and managing CCR. Bank boards of directors should know that they are ultimately accountable for the quality of senior management.

75. Banks should foster a culture that enables adequate consideration of CCR arising from changes or dysfunctionalities in the geopolitical landscape. They should be able to assess the impact of potential wars and sanctions on their ongoing businesses. Furthermore, banks with an international presence should be able to swiftly assess the impact of wars and sanctions on intragroup transactions that involve their own legal entities, especially those located in potentially sanctionable jurisdictions.

Risk framework

76. Banks should establish a clear CCR strategy and an effective CCR management process approved by the board of directors and implemented by senior management. The CCR strategy should define the bank's risk appetite, its desired risk-return trade-off and mix of products and markets. Such a strategy should be supplemented by clear, robust and actionable policies and procedures that establish effective monitoring and control of CCR relationships. These policies and procedures should drive the credit-setting process and govern banks' relationships with counterparties and should not be overridden by competitive pressures.

77. Policies and procedures should be clear with regards to ownership, roles and responsibilities – providing clear guidelines for credit approval authority, remediation and escalation processes. Banks with sound practices have a strong balance between ensuring individual ownership of policies, while also ensuring important changes to policy are approved by relevant oversight committees. Additionally, regular policy reviews are conducted on a yearly basis, as a minimum, to ensure their continued relevance. In all cases, authorship and ownership of policies and procedures should be clearly separated.

78. Banks should ensure that CCR oversight – including second and third lines of defence – are effective, with clear mandates, sufficient knowledge and stature, and the ability to operate in an environment in which managers and staff throughout the organisation are incentivised to identify, challenge, escalate and resolve risks.

79. The long-term success of a bank's credit relationships relies heavily on effective and sophisticated risk management. Sound monitoring of the activities of a counterparty requires thorough

knowledge and understanding of the economics of the relevant exposures, including purpose, source of repayment, risks associated with collateral, risk concentrations and controls. Reliance on collateral cannot substitute for day-to-day risk management and monitoring.

80. Banks should establish and empower risk committees as governing bodies with authority over all risk-taking aspects of trading businesses, including risk limits, permitted products, hedging strategies, collateral eligibility, margins, risk measurement methodologies and overall risk appetite. As governing bodies, risk committees should receive appropriate information on a timely basis for the key risk drivers and risk trends of ongoing trading activities, both through risk sensitivities, risk scenarios and stress tests.

81. Banks' governing bodies should have accountability for limit exceptions and approvals in line with the bank's established delegation of authority. Banks with strong practices embed approval authority for policy changes with risk committees that oversee all trading activities for market and CCR and give risk committees review authority for all approved exceptions.

82. Risk committees should include senior managers from trading and risk functions as well as compliance, finance, legal and operations groups. Furthermore, risk committees should report regularly to the bank's board risk committee. Risk committees should be of a size that is adequate to promote the dissemination of decisions taken throughout the organisation, but without reducing the accountability of individual participants. Ideally, the chair of the committee is accountable for the committee's decisions.

83. Complex booking models, for example remote cross-border booking models, are more challenging for banks to allocate adequate responsibility for risk management. Banks with sound practices manage their counterparty exposure by using booking models that are simple and have clear accountability embedded in the booking model framework.

Management reporting

84. Management is directly accountable for the implementation of a sufficiently detailed CCR reporting framework. This reporting should allow management – as well as key risk committees – to easily understand the CCR taken by the bank and to act based on the reported risks. Furthermore, management reporting should empower managers to aggregate the data at an adequate level across key risk dimensions and over time periods. It should also enable managers to easily analyse data and conduct drilldowns on a timely basis.

85. Banks with sound practices have CCR reporting that includes but is not limited to:

    a. the key CCR exposure metrics used at both a single name as well as portfolio level of aggregation;

    b. CCR exposure evolution over time;

    c. top CCRs;

    d. relevant limits, breaches and other flagged risks (such as concerning or potentially distressed counterparties or industries); and

    e. the degree of likelihood of a potential loss.

86. Management reporting should inform senior management about non-standard terms and conditions in CCR contracts. Non-standard terms and conditions in such contracts should be discussed by management on a regular basis.

87. Managers are encouraged to continuously improve the quality of CCR reporting in their institutions. Management reports should be comprehensive, accurate, consistent, actionable,

relevant and timely. Furthermore, a bank should be able to produce and analyse reports in both normal and stressed market conditions.

88. Bank management is responsible for building a management information system (MIS) that does not overwhelm users with data. Managers should use the bank's MIS for management reporting and be able to perform on-request analysis without external help for counterparties with material exposure or those on watch lists/close monitoring lists.

89. Managers should foster a culture that stresses the importance of management reporting in managing CCR. This includes, but is not limited to, valuing the important role played by data and models in managing CCR.

90. Banks with sound practices also promote a holistic view of market and CCR management, enabling the assessment of the impact of a counterparty default on market risk and vice versa, as well as a clear and actionable risk framework around these assessments.

Limit governance and exception management

91. Banks should implement a transparent and actionable limit governance framework with clear and proper oversight and review. The limit framework should include a remediation process for limit breach with distinct and accurate oversight, review and challenge stages commensurate with the severity and materiality of limit breaches.

92. Limits should be set and verified independently from the business function.

93. Limit actions such as exceptions should require approval from an independent risk function. If exceptions are sufficiently large then delegation of authority should require approvals from senior management. Banks with sound practices document such approvals in risk systems with an adequate audit trail.

94. Banks should not disregard limit exceptions that may be considered technical breaches without proper review and escalation. Technical breaches – ie breaches caused by bad data, incorrect mapping or similar issues – should be subject to exception approvals that are sized appropriately to allow for remediation of the root cause of the breach.

95. Passive breaches of counterparty credit limits – ie breaches caused by changes in MTM, not position changes – should require the same review and challenge as active breaches. Independent risk functions should have sole authority to approve limit exceptions, in addition to the authority to allocate risk appetite – such as PFE, RWAs or stress exposure – between businesses and products with the same counterparty.

96. Risk limits should be set based on the risk tolerance level as established by the designated risk committee within the bank. The risk committee should be represented by senior management, including senior risk officers. Members of the risk committees should have the ability to mandate decisive actions to reduce risk even when there are disagreements with the business units.

97. At the counterparty level, risk limits should be set at levels consistent with the bank's assessment of the counterparty's credit quality, the degree of transparency the bank has on the counterparty's overall financial condition and leverage, and the bank's ability to effectively unwind the counterparty's portfolio in a timely manner in the event of counterparty default.

98. Banks monitor actual exposures against established risk limits at least on a daily basis. Furthermore, banks should be able to assess, in a time period that is adequate for trading purposes, whether a new transaction leads to a limit breach or not. In addition, banks are encouraged to establish ad hoc intraday exposure monitoring, which should be adequate for assessing impacts of large intraday market moves on risk limits.

99. Banks should monitor actual exposures against the established risk limits and have in place clear and actionable procedures for escalating limit breaches to the appropriate risk committee and/or senior management. These procedures should apply to limit breaches on the individual counterparty level as well as aggregate exposure. The procedures should also include situations in which a limit is in breach for an extended period or when a counterparty routinely breaches approved limits without sufficient remediation steps. In these circumstances, decision points should include re-underwriting the credit, obtaining additional credit risk mitigants and/or obtaining better information disclosure.

100. Banks should have a clear and actionable strategy for de-risking exposure in case of limit breaches. Furthermore, these procedures should also be actionable during phases of high volatility and illiquidity.

101. Banks may set early warning indicators when limit utilisations increase significantly or at an elevated level but do not yet result in limit breaches. Early warning indicators can promote proactive management of risk and help a bank take early actions when warranted to mitigate risk.

6. Infrastructure, data and risk systems

Timely, accurate, reliable counterparty infrastructure, data and risk systems are necessary for sound management of CCR, as outlined in and reinforced by *Principles for effective risk data aggregation and risk reporting*.[15] All aspects of CCR are impacted by the quality of data, systems and aggregation capabilities used by banks to manage their risks. This includes, for example, information collection that feeds into due diligence, the digitisation of key contractual terms governing the adequacy of credit risk mitigants, the risk metrics used to size counterparty exposure, and the information and reporting needs of not only senior management but also traders and credit officers involved in the day-to-day risk management of CCR.

102. Banks should ensure that risk systems (eg front office, valuation and booking systems, and risk engines) and data management capabilities underpinning CCR management – including risk measurement and limit monitoring – are commensurate with the size and complexity of counterparty exposures. Systems, models and data management capabilities should be sound and sufficiently sophisticated to support CCR measurement under BAU and stress conditions, and they should be enhanced as the bank's risk profile evolves and newer sound practices are established.

103. CCR measurement is a highly involved risk data aggregation process given the complexity of calculations and processes. It is best exemplified by reliance on large internal and external data sets, numerous upstream data systems and platforms, and interdependent models involved in risk measurement. The complexity of these processes requires commensurate capabilities and controls that ensure comprehensive, granular, accurate and timely risk metrics. The inability to produce fit for purpose risk metrics that meet these critical data dimensions can negatively impact a bank's ability to effectively measure, monitor and control CCR given the highly dynamic nature of trading book exposures.

104. Banks should ensure that key risk systems have minimal frictions that would impede comprehensive, accurate and timely risk data aggregation and measurement and, where necessary, they should implement adequate compensating processes and controls, such as data staging platforms to mitigate known shortcomings. Banks should aim to reduce the number of

[15] Basel Committee on Banking Supervision, *Principles for effecti ve risk data aggregation and risk reporting*, January 2013.

systems involved in exposure measurement and management to reduce operational risk. They should allocate adequate resources to implement required upgrades to capabilities where deemed necessary, ie commensurate with the business model and risk profile. Banks with sound practices maintain capabilities to aggregate and measure risk exposures seamlessly across products, businesses, geographies and risk factors to support concentration monitoring at both counterparty and portfolio levels.

105. Banks should ensure that data management protocols, processes and controls underlying counterparty risk data aggregation and measurement are aligned to enterprise/bank-wide data management frameworks and standards to ensure comprehensive, accurate and timely risk monitoring. Banks with sound practices have consistent data taxonomies across businesses that align with enterprise classifications to ensure, for instance, risk metrics estimated by different systems are aggregated accurately and conservatively. Further, stronger practices entail data issue/incident remediation processes for counterparty risk measurement that are directly linked to bank-wide processes to ensure strategic, long-term solutions for system and/or data issues.

106. Banks should ensure that reporting and oversight routines provide key stakeholders with sufficient information about the overall effectiveness of counterparty risk data aggregation and measurement processes. These insights ultimately ensure that end users of risk metrics and reports – eg credit risk officers and front office traders – make informed risk appetite decisions at desk, counterparty and portfolio levels. Such decisions include the approval or restriction of new trades and the implementation of risk mitigation or reduction strategies. The socialisation of known and identified issues with stakeholders and/or end users of reports and metrics is critical to maintaining and strengthening risk aggregation and measurement processes, including receiving sufficient resources, ie "buy in", to remediate issues and implement system/capabilities upgrades. Material issues and weaknesses should also be escalated to relevant bank-wide technology and data management forums for awareness and effective resolution.

107. Strong governance practices are grounded in sound preventative, detective and corrective technology and data quality controls that facilitate the identification, monitoring, escalation and remediation of system, data and model issues. Banks with stronger practices maintain a suite of controls to support counterparty risk data aggregation and measurement, including:

    a. Robust preventative and detective controls to identify data anomalies for all key or material counterparty risk metrics used to constrain risk-taking at the portfolio, desk and counterparty levels – ie not limited to a select few metrics.

    b. Key controls that include data reconciliation and variance analysis processes that efficiently build on each other as opposed to creating control redundancies.

    c. A robust process to monitor data feed transfer from upstream systems to data staging platforms and risk engines, underpinned by well documented service level agreements that are strictly enforced and monitored. Data feed management processes and other relevant technology controls are not executed and managed in a silo by a technology and/or operational team, but are instead integrated into counterparty risk measurement governance and control frameworks.

    d. A robust process to manually adjust missing or incorrect data identified via technology, data reconciliation and variance analysis, or other detective controls. Banks with sound practices have a metrics adjustment process that is well documented and executed through automated capabilities to minimise operational risk. An adjustment process also addresses data issues identified and flagged by upstream data providers.

    e. A key performance indicator (KPI) or risk indicator (KRI) framework designed and monitored against outcomes of technology (eg data feed) and data management controls (eg manual

adjustments). The framework synthesises control outcomes to facilitate reporting to end users of reports – ie a "score card" on the overall effectiveness of the counterparty risk data aggregation and measurement process.

f. Material issues and/or critical KPIs, including KPIs tracking the level of manual intervention (ie data adjustments) or data feed timeliness, which are further escalated to senior governance forums with mandates to oversee CCR. Escalation and reporting to bank-wide management risk committees and the chief risk officer to facilitate awareness of the extent to which CCR exposure is a key contributor to the bank's overall risk profile.

g. Forums established for the sole purpose of overseeing the counterparty risk data aggregation and measurement processes. These governance bodies serve as the first escalation point for system, data or model issues impacting the production of portfolio, desk and counterparty level risk metrics. KPI score cards, issue logs, manual data adjustments etc are all key inputs into ongoing discussions. Participants include system/application owners, model owners, owners of reports/metrics, end users of reports and key upstream data providers.

Counterparty credit risk reporting

108. Banks should embrace the risk reporting practices stated in *Principles for effective risk data aggregation and risk reporting*[16] with respect to their CCR reporting. All principles below should be seen as enhancing these generally formulated risk reporting practices.

109. Banks should regularly assess the relevance, timeliness and quality of CCR reporting. This should include, but not be limited to, an assessment of input data quality, analysis of comments on potential data anomalies, assessment of the frequency of reporting and ensuring adequate socialisation of reports within key business and oversight functions. Banks should discourage fragmented reporting environments for CCR. If the reporting environment is deemed to be too fragmented, banks should re-design the environment without delay.

110. Banks should set up risk reporting through appropriate MIS to ensure an adequate level of CCR analysis. Adequate reporting includes aggregating the data for each decision level, allowing for aggregation across key risk dimensions and over time periods, and enabling easy data analysis and drilldowns on a timely basis.

111. Banks should build up MIS so that relevant CCR data are easily retrievable at risk factor, counterparty and aggregate levels. Banks' MIS should avoid overwhelming users with data, while allowing for detailed on-request analysis by the decision-makers.

112. Banks should build an MIS for CCR reporting that is user-friendly and intuitive. Each decision-maker should have the ability to analyse data individually, ideally without using tools outside the MIS. Furthermore, banks should consider enabling the users to comment on the most relevant CCR measures and store these comments in the MIS. There should be an audit trail of the analysis.

113. Banks should train their personnel in the operation of the MIS. Each user of the MIS should be able to understand and analyse the data to a level that enables consistent and effective risk reporting.

[16] Basel Committee on Banking Supervision, *Principles for effective risk data aggregation and risk reporting*, January 2013.

7. Closeout practices

Sound management of CCR includes banks recognising the need to act quickly based on their contractual ability to close out a counterparty when necessary, with full knowledge of all steps needed to initiate, execute and manage residual impacts, including collateral liquidation and trade replacement.

Watch list practices and default management protocol

114. Banks closing out counterparties should know that the potential costs of such actions can be high. Closeout of counterparties involves business, legal and risk staff carrying out actions properly, as banks serving notice on counterparties should not breach legal provisions in agreements such as the International Swaps and Derivatives Association Master Agreement,[17] the related Credit Support Annex,[18] the International Capital Market Association Global Master Repurchase Agreement[19] or the Global Master Securities Lending Agreement.[20] Liquidation of trades invariably lead to the realisation of MTM losses and the need for new replacement trades. The costs to the bank of carrying out a closeout are material and should be known.

115. Banks should ensure that seasoned professionals familiar with legal processes for carrying out a declaration of counterparty default are able to initiate closeouts as needed. Involvement from the legal department is critical to carrying out all aspects of a counterparty closeout. The process should have input from credit risk and risk management more broadly. As part of the bank's ongoing credit monitoring process, independent credit officers should be engaged in regular oversight of counterparties and they should maintain a watch list of any names that require restricted or risk reducing activity only.

116. Banks with sound practices maintain up-to-date closeout playbooks. They carry out mock closeout exercises to uncover potential issues in advance of an actual closeout. The mock closeout candidate should be a name that involves more than one legal jurisdiction and potentially multiple business lines. The counterparty type should vary from year to year, and the bank should not give advance notice to participants regarding the date of such an exercise. In the event of a closeout, the bank's teams should complete a post-mortem exercise following such incidents to compile lessons learned. Any lessons learned should then be used to enhance existing playbooks for such events in the future. The exercise should include participants from credit, finance, legal, operations, risk and trading teams with the following minimum objectives:

    a. All involved parties are identified and have sufficient resources to execute the closeout in parallel with ongoing BAU.

    b. Demonstrate that relevant reporting is shared with involved functions in due time and is complete and correct.

[17] The Master Agreement is published by the International Swaps and Derivatives Association. It outlines the terms to be applied to a derivatives transaction between two parties.

[18] A Credit Support Annex may accompany the Master Agreement, allowing the two parties involved to mitigate credit risk by stipulating the terms and conditions to post collateral to each other.

[19] International Capital Market Association, *Global Master Repurchase Agreement (GMRA)*, 2011.

[20] For example, the master agreements by the International Securities Lending Association for securities lending transacted under a title transfer arrangement available at www.islaemea.org/gmsla-title-transfer/.

c. Closeout governance allows fast and consistent decision-making by involved management functions and all decisions taken are in line with internal policies and procedures and are consistent with the legal framework for the affected financial contracts.

d. Trading capabilities that enable the orderly unwinding of positions (including experienced traders, access to capital markets and counterparty limits) are available.

117. Banks with strong risk management will understand that contractual terms embedded in legal agreements can limit a bank's ability to reduce or discontinue activity with a counterparty. Closeout provisions should be carefully calibrated based on the banks' assessment of counterparty credit quality, including control and ownership. Any concession to a counterparty regarding such provisions should be made with awareness of the bank's need to maintain flexibility in order to avoid the need to declare a counterparty in default.

118. In an era of rogue actors and geopolitical instability, banks should take special care to ensure that systems have backups and that crucial vendors and third-party relationships have secondary providers in place. They should also take special care to ensure that procedures have been tested in the event that transactions are rerouted and processes remapped. Mission critical payments and securities transfer protocols should be designed with kill switches for manual operation only. The potential for international sanctions to be imposed on an entire legal jurisdiction requires banks to contemplate mock closeout exercises at the level of a full jurisdiction.

8. Glossary

BAU	Business as usual
CCR	Counterparty credit risk
CVA	Credit valuation adjustment
EE	Expected exposure
GWWR	General wrong-way risk
IM	Initial margin
IMM	Internal models method
MIS	Management information system
MPOR	Margin period of risk
NAV	Net asset value
NBFI	Non-bank financial intermediary
PFE	Potential future exposure
RWA	Risk-weighted asset
SA-CCR	Standardised approach for counterparty credit risk
SFT	Securities financing transaction
SWWR	Specific wrong-way risk
VM	Variation margin
WWR	Wrong-way risk
XVA	X-value adjustment