*Office of the Comptroller of the Currency*
*Federal Deposit Insurance Corporation*
*Board of Governors of the Federal Reserve System*
*Office of Thrift Supervision*

# Interagency Supervisory Guidance on Counterparty Credit Risk Management

**June 29, 2011**

## Table of Contents

**COUNTERPARTY CREDIT RISK MANAGEMENT**

# I. Introduction

This guidance discusses critical aspects of effective management of counterparty credit risk (CCR), and sets forth sound practices and supervisory expectations for an effective CCR management framework. CCR is the risk that the counterparty to a transaction could default or deteriorate in creditworthiness before the final settlement of a transaction's cash flows. Unlike the credit risk for a loan, when only the lending banking organization[1] faces the risk of loss, CCR creates a bilateral risk of loss because the market value of a transaction can be positive or negative to either counterparty. The future market value of the exposure and the counterparty's credit quality are uncertain and may vary over time as underlying market factors change. The guidance is intended for use by banking organizations, especially those with large derivatives portfolios, in setting their risk management practices, as well as by supervisors as they assess and examine such institutions' management of CCR. For other banking organizations without large derivatives portfolios, risk managers and supervisors should apply this guidance as appropriate, given the size, nature, and complexity of the CCR risk profile of the banking organization.

CCR is a multidimensional form of risk, affected by both the exposure to a counterparty and the credit quality of the counterparty, both of which are sensitive to market-induced changes. It is also affected by the interaction of these risks, for example the correlation[2] between an exposure and the credit spread of the counterparty, or the correlation of exposures among the banking organization's counterparties. Constructing an effective CCR management framework requires a combination of risk management techniques from the credit, market, and operational risk disciplines.

CCR management techniques have evolved rapidly over the last decade, along with increased complexity of derivative instruments under management. Banking organizations substantially improved their risk management practices during this time; however, in some cases, implementation of sound practices has been uneven across business lines and counterparty types. Further, the financial crisis of 2007-2009 revealed weaknesses in CCR management at many banking organizations, such as shortcomings in the timeliness and accuracy of exposure aggregation capabilities and inadequate measurement of correlation risks. The crisis also highlighted deficiencies in the ability of banking organizations to monitor and manage counterparty exposure limits and concentration risks, ranging from poor selection of CCR metrics to inadequate system infrastructure.

To address these weaknesses, this guidance reinforces sound governance of CCR management practices, through prudent board and senior management oversight, management reporting, and risk management functions. The guidance discusses relevant topics in risk measurement, including metrics, exposure aggregation and concentration management, stress testing, and associated characteristics of adequate systems infrastructure. It also covers risk control functions, such as counterparty limits, margin practices, validating and backtesting models and systems, managing close-outs,[3] managing

[1] Unless otherwise indicated, "banking organizations" refers to national banks in the case of the Office of the Comptroller of the Currency (OCC); federal and state savings associations and savings and loan holding companies in the case of the Office of Thrift Supervision (OTS); state member banks and bank holding companies in the case of the Federal Reserve Board (Board); and state nonmember banks in the case of the Federal Deposit Insurance Corporation (FDIC). The U.S. branches and agencies of foreign banks supervised by the OCC, the Board and the FDIC also are considered to be banking organizations for purposes of this guidance.

[2] In this guidance, "correlation" refers to any form of linear or non-linear inter-relationship or dependence between factors.

[3] A close-out is the process undertaken by a banking organization following default of a counterparty to fully collect on all items due from that counterparty.

central counterparty exposures, and controlling legal and operational risks arising from derivatives activities.

CCR management guidelines and supervisory expectations are delineated in various individual and interagency policy statements and guidance,[4] which remain relevant and applicable. This guidance offers further explanation and clarification, particularly in light of developments in CCR management. However, this guidance is not all-inclusive and banking organizations should reference sound practices for CCR management, such as those advanced by industry, policymaking and supervisory forums.[5]

## II. Governance

### 1. Board and Senior Management Responsibilities

The board of directors or a designated board-level committee (board) should clearly articulate the banking organization's risk tolerance for CCR, by approving relevant policies, including a framework for establishing limits on individual counterparty exposures and concentrations of exposures. Senior management should establish and implement a comprehensive risk measurement and management framework consistent with this risk tolerance that provides for the ongoing monitoring, reporting, and control of CCR exposures.

Senior management should adhere to the board's established risk tolerance and establish policies and risk management guidelines appropriately.[6] At a minimum, policies should outline CCR management standards that are in conformance with this guidance. More specifically, they should address the subjects discussed in this document, such as risk measurement and reporting, risk management tools, and processes to manage legal and operational risk. Policies should be detailed and contain a clear escalation process for review and approval of policy exceptions, especially those pertaining to transaction terms and limits.

### 2. Management Reporting

Banking organizations should report counterparty exposures to the board and senior management at a frequency commensurate with the materiality of exposures and the complexity of transactions. Reporting should include concentration analysis and CCR stress testing results, to allow for an understanding of exposures and potential losses under severe market conditions. Reports should also include an explanation of any measurement weaknesses or limitations that may influence the accuracy and reliability of the CCR risk measures.

---

[4]See, for example, Supervisory Policy Statement on Investment Securities and End-User Derivatives Activities, 63 FR 20191, April 23, 1998. Examination guidance on CCR is contained in various agency publications including: FDIC, *Capital Markets Examination Handbook*; Federal Reserve, SR 99-03 and *Trading and Capital Market Activities Manual* (to be amended as appropriate to reflect this guidance); OTS, *Examiner Handbook*, Section 660, "Derivative Instruments and Hedging"; the OCC's Banking Circular 277, and "Risk Management of Financial Derivatives" (*Comptroller's Handbook, January*, 1997).

[5]Industry, policymaking, and supervisory groups include, but are not limited to, the Counterparty Risk Management Policy Group (CRMPG), Committee on Payment and Settlement Systems (CPSS), International Swaps and Derivatives Association (ISDA), Institute of International Finance (IIF), Group of Thirty (G30), Group of Twenty Finance Ministers and Central Bank Governors (G-20), International Organization of Securities Commissions (IOSCO), Senior Supervisors Group (SSG), and Basel Committee on Banking Supervision (BCBS). Documents produced by all of these groups were drawn upon in developing this guidance.

[6] Relevant supervisory guidance discusses establishment of CCR policies and procedures.

Senior management should have access to timely, accurate, and comprehensive CCR reporting metrics, including an assessment of significant issues related to the risk management aspects discussed in this guidance. They should review CCR reports at least monthly, with data that are no more than three weeks old. It is general practice for institutions to report:

- Total counterparty credit risk aggregated on a firm-wide basis and at significant legal entities.
- Counterparties with the largest exposures, along with detail on their exposure amounts.
- Exposures to central counterparties (CCPs).
- Significant concentrations, as outlined in this guidance.
- Exposures to weak or problem counterparties.
- Growth in exposures over time. As a sound practice, metrics should capture quarterly or monthly changes, supplemented (where relevant) by year-over-year trend data.
- Exposures from over-the-counter (OTC) derivatives. When they are material, additional product class break-outs (for example, traditional lending, securities lending) should be included.
- A sufficiently comprehensive range of CCR metrics, as discussed in the CCR metrics section.
- A qualitative discussion of key risk drivers of exposures or conditions or factors that would fundamentally change the risk profile of CCR. An example would be assessment of changes in credit underwriting terms and whether they remain prudent.

### 3. Risk Management Function and Internal Audit

A banking organization's board and senior management should clearly delineate the respective roles of business lines versus risk management, both in terms of initiating transactions that have CCR, and of ongoing CCR management. The board and senior management should ensure that the risk management functions have adequate resources, are fully independent from CCR related trading operations (in both activity and reporting), and have sufficient authority to enforce policies and to escalate issues to senior management and the board (independent of the business line).

The board should direct internal audit to regularly assess the adequacy of the CCR management framework as part of the regular audit plan. Such assessments should include credit line approval processes, credit ratings, and credit monitoring. Such an assessment should opine on the adequacy of the CCR infrastructure and processes, drawing where appropriate from individual business line reviews or other internal and external audit work. Please see the relevant section of this guidance regarding the role of CCR model validation or review. The board should review annual reports from internal audit and model validation or review, assessing the findings and confirming that management has taken appropriate corrective actions.

## III. Risk Measurement

### 1. CCR Metrics

Given the complexity of CCR exposures (particularly regarding OTC derivatives), banking organizations should employ a range of risk measurement metrics to promote a comprehensive

understanding of CCR and how it changes in varying environments. Metrics should be commensurate with the size, complexity, liquidity, and risk profile of the CCR portfolio. Banking organizations typically rely on certain metrics as a primary means of monitoring, with secondary metrics used to create a more robust view of CCR exposures. Banking organizations should apply these metrics to single counterparty exposures, groups of counterparties (for example, by internal rating, industry, geographical region), and the consolidated CCR portfolio. Banking organizations should assess their largest exposures, for instance their top 20 exposures, using each primary metric.

Major dealers and large, sophisticated banking organizations with substantial CCR exposure should measure and assess:

- Current exposure (both gross and net of collateral).
- Forward-looking exposure (that is, potential exposure).
- Stressed exposure (broken out by market risk factors, and/or by scenario).
- Aggregate and stressed credit valuation adjustment (CVA) as well as CVA factor sensitivities.
- Additional relevant risk measures, such as (for credit derivatives) jump-to-default risk on the reference obligor, and economic capital usage.
- The largest exposures by individual business line and product types.
- Correlation risks, such as wrong-way risk, as well as the credit quality of collateral.

Refer to Appendix A for definitions of basic metrics and descriptions of their purposes.

## 2. Aggregation of Exposures

Banking organizations should have the capacity to measure their exposure at various levels of aggregation (for example, by business line, legal entity, or consolidated by industry). Systems should be sufficiently flexible to allow for timely aggregation of all CCR exposures (that is, OTC derivatives, securities financing transactions (SFTs), and other pre-settlement exposures), as well as aggregation of other forms of credit risk to the same counterparty (for example, loans, bonds, and other credit risks). The following are sound CCR aggregation principles:

- Counterparty-level current exposure and potential exposure should be calculated daily, based on the previous day's position data and any exchange of collateral.
- For each organizational level of aggregation, all trades should be included.
- There should be sufficient flexibility to aggregate exposure at varying levels of granularity, including industries, regions, families of products (for example, OTC derivatives, SFTs), or other groupings to identify concentrations.
- While banking organizations are not required to express all forms of risk in a common metric or basis, management should be able to view the various forms of exposures to a given counterparty in a single report and/or system. Specifically, this could include current outstanding exposure across different categories (e.g., current exposure for OTC derivatives and drawn-down lines of commitment for loans). Exposure reports should also include the size of settlement and clearing lines.

- Banking organizations should be consistent in their choice of currency and exchange rate, and take into account the validity and legal enforceability of any netting agreements they may have with a counterparty.
- Management should understand the specific approach used to aggregate exposures for any given risk measure, in order to properly assess the results. For instance, some measures of risk (such as current exposure) may be readily added together, while others (such as potential exposure) are less meaningful when they are added to form an aggregate view of risk.
- Internal capital adequacy models should incorporate CCR.

## 3. Concentrations

Concentrated exposures are a significant concern, as CCR can contribute to sudden increases in credit exposure, which in turn can result in unexpectedly large losses in the event of counterparty default. Accordingly, banking organizations should have enterprise-wide processes to effectively identify, measure, monitor, and control concentrated exposures on both a legal entity and enterprise-wide basis.

Concentrations should be identified using both quantitative and qualitative means. An exposure or group of related exposures (for example, firms in the same industry), should be considered a concentration in the following circumstances: exposures (individually or collectively) exceed risk tolerance levels established to ensure appropriate diversification; deterioration of the exposure could result in material loss; or deterioration could result in circumstances that are detrimental to the banking organization's reputation. All credit exposures should be considered as part of concentration management, including loans, OTC derivatives, names in bespoke and index CDO credit tranches, securities settlements, and money market transactions such as fed funds sold. Total credit exposures should include the size of settlement and clearing lines, or other committed lines.

CCR concentration management should identify, quantify, and monitor:

- Individual counterparties with large potential exposures, when those exposures are driven by a single market factor or transaction type. In these circumstances, banking organizations should supplement statistical measures of potential exposure with other measures, such as stress tests, that identify such concentrations and provide an alternative view of risks associated with close-outs.
- Concentrations of exposures to individual legal entities, as well as concentrations across affiliated legal entities at the parent entity level, or in the aggregate for all related entities.
- Concentrations of exposures to industries or other obligor groupings.
- Concentrations of exposures to geographic regions or country-specific groupings sensitive to similar macroeconomic shocks.
- Concentrations across counterparties when potential exposure is driven by the same or similar risk factors. For both derivatives and SFTs, banking organizations should understand the risks associated with crowded trades,[7] where close-out risk may be heightened under stressed market conditions.

[7] For purposes of this guidance, a "crowded trade" is a large balance of open trading positions in a given asset or group of assets relative to its daily trading volume, when other market participants have similar positions that would need to be liquidated should any adverse price change occur. Coincident sale of these assets by a large number of market participants could lead to significant price declines and dramatic increases in uncollateralized exposures.

- Collateral concentrations, including both risk concentrations with a single counterparty, and risks associated with portfolios of counterparties. Banking organizations should consider concentrations of non-cash collateral for all product lines covered by collateral agreements;[8] including collateral that covers a single counterparty exposure and portfolios of counterparties.[9]
- Collateral concentrations involving special purpose entities (SPEs). Collateral concentration risk is particularly important for SPEs, because the collateral typically represents an SPE's paying capacity.
- Banking organizations should consider the full range of credit risks in combination with CCR to manage concentration risk, including; risks from on- and -off-balance-sheet activities, contractual and non-contractual risks, contingent and non-contingent risks, as well as underwriting and pipeline risks.

## 4. Stress Testing

Banking organizations with significant CCR exposures should maintain a comprehensive stress testing framework, which is integrated into the banking organization's CCR management. The framework should inform the banking organization's day-to-day exposure and concentration management, and it should identify extreme market conditions that could excessively strain the financial resources of the banking organization. Regularly, but no less than quarterly, senior management should evaluate stress test results for evidence of potentially excessive risk, and take risk reduction strategies as appropriate.

The severity of factor shocks should be consistent with the purpose of the stress test. When evaluating solvency under stress, factor shocks should be severe enough to capture historical extreme market environments and/or extreme but plausible stressed market conditions. The impact of such shocks on capital resources and earnings should be evaluated. For day-to-day portfolio monitoring, hedging, and management of concentrations, banking organizations should also consider scenarios of lesser severity and higher probability. When conducting stress testing, risk managers should challenge the strength of assumptions made about the legal enforceability of netting and the ability to collect and liquidate collateral.

A sound stress-testing framework should include:

- Measurement of the largest counterparty-level impacts across portfolios, material concentrations within segments of a portfolio (such as industries or regions), and relevant portfolio- and counterparty-specific trends.
- Complete trade capture and exposure aggregation across all forms of trading (not just OTC derivatives) at the counterparty-specific level, including transactions that fall outside of the main credit system. The time frame selected for trade capture should be commensurate with the frequency with which stress tests are conducted.
- Stress tests, at least quarterly, of principal market risk factors on an individual basis (for example, interest rates, foreign exchange, equities, credit spreads, and commodity prices) for all material counterparties. Banking organizations should be aware that some counterparties may be material on a consolidated basis, even though they may not be material on an individual legal entity basis.

[8] Banking organizations should also track concentrations in volatile currencies.

[9] This analysis is particularly important with repo-style transactions and other forms of SFTs for which the ability of market participants to liquidate large collateral positions may be difficult during periods of market turbulence.

- Assessment of non-directional risks (for example, yield curve exposures and basis risks) from multi-factor stress testing scenarios. Multi-factor stress tests should, at a minimum, aim to address separate scenarios: severe economic or market events; significant decrease in broad market liquidity; and the liquidation of a large financial intermediary of the banking organization, factoring in direct and indirect consequences.
- Consideration, at least quarterly, of stressed exposures resulting from the joint movement of exposures and related counterparty creditworthiness. This should be done at the counterparty-specific and counterparty-group (for example, industry and region) level, and in aggregate for the banking organization. When CVA methodologies are used, banking organizations should ensure that stress testing sufficiently captures additional losses from potential defaults. [10]
- Basic stress testing of CVA to assess performance under adverse scenarios, incorporating any hedging mismatches.
- Concurrent stress testing of exposure and non-cash collateral for assessing wrong-way risk.
- Identification and assessment of exposure levels for certain counterparties (for example, sovereigns and municipalities), above which the banking organization may be concerned about willingness to pay.
- Integration of CCR stress tests into firm-wide stress tests.[11]

## 5. Credit Valuation Adjustments (CVA)

CVA refers to adjustments to transaction valuation to reflect the counterparty's credit quality. CVA is the fair value adjustment to reflect CCR in valuation of derivatives. As such, CVA is the market value of CCR and provides a market-based framework for understanding and valuing the counterparty credit risk embedded in derivative contracts. CVA may include only the adjustment to reflect the counterparty's credit quality (a one-sided CVA or just CVA), or it may include an adjustment to reflect the banking organization's own credit quality. The latter is a two-sided CVA, or CVA plus a debt valuation adjustment (DVA). For the evaluation of the credit risk due to probability of default of counterparties, a one sided CVA is typically used. For the evaluation of the value of derivatives transactions with a counterparty or the market risk of derivatives transactions, a two-sided CVA should be used.

Although CVA is not a new concept, its importance has grown over the last few years, partly because of a change in accounting rules that requires banking organizations to recognize the earnings impact of changes in CVA.[12] During the 2007-2009 financial crisis, a large portion of CCR losses were because of CVA losses rather than actual counterparty defaults.[13] As such, CVA has become more important in risk management, as a mechanism to value, manage, and make appropriate hedging

[10] Exposure testing should include single-factor, multi-factor and material non-directional risks.
[11] CCR stress testing should be consistent with overall banking organization-wide stress testing and follow the principles set forth in the "Principles for Sound Stress Testing Practices and Supervision" issued by the Risk Management and Modeling Group of the Basel Committee in May 2009.
[12] Accounting literature pertinent to CVA includes FAS Statement 157, and Accounting Standards Codification (ASC) Topic 820. In addition, other transaction fair value adjustments should be conducted. For example, those involving a banking organization's own credit risk, or differences in funding costs based on whether transactions are collateralized or not.
[13] Basel Committee on Banking Supervision, "Strengthening the resilience of the banking sector – consultative document," December 2009. http://bis.org/publ/bcbs164.htm

decisions, to mitigate banking organizations' exposure to the mark-to-market (MTM) impact of CCR.[14] The following are general standards for CVA measurement and use of CVA for risk management purposes:

- CVA calculations should include all products and counterparties, including margined counterparties.
- The method for incorporating counterparty credit quality into CVA should be reasonable and subject to ongoing evaluation. CVA should reflect the fair value of the counterparty credit risk for OTC derivatives, and inputs should be based on current market prices when possible.
    - Credit spreads should be reflected in the calculation where available, and banking organizations should not overly rely on non-market-based probability of default estimates when calculating CVA.
    - Banking organizations should attempt to map credit quality to name-specific spreads rather than spreads associated with broad credit categories.
    - Any proxy spreads should reasonably capture the idiosyncratic nature of the counterparty and the liquidity profile.
    - The term structure of credit spreads should be reflected in the CVA calculation
- The CVA calculation should incorporate counterparty-specific master netting agreements and margin terms; for example, the CVA calculation should reflect margin thresholds or minimum transfer amounts stated in legal documents.
- Banking organizations should identify the correlation between a counterparty's credit-worthiness and its exposure to the counterparty, and seek to incorporate the correlation into their respective CVA calculation.

Management of CVA

CVA management should be consistent with sound risk management practices for other material mark-to-market risks. These practices should include the following:

- Business units engaged in trades related to CVA management should have independent risk management functions overseeing their activities.
- Systems that produce CVA risk metrics should be subject to the same controls as used for other MTM risks, including independent validation or review of all risk models, including alternative methodologies.[15]
- Upon transaction execution, CVA costs should be allocated to the business unit that originates the transaction.
    - As a sound practice, the risk of CVA should be incorporated into the risk-adjusted return calculation of a given business.

[14] An accurate measure of CVA is critical to prudent risk-taking, as part of effectively understanding the risk-reward tradeoff in a given derivatives transaction. The more comprehensively CVA is measured, the more transparent the economics of a given transaction.

[15] Liquidity in credit markets has varied significantly over time. As liquidity conditions change, banking organizations should calculate CVA using methodologies appropriate to the market pricing information available for each counterparty and transaction type.

- CVA cost allocation provides incentive for certain parties to make prudent risk-taking decisions, and motivates risk-takers to support risk mitigation, such as requiring strong collateral terms.

- Banking organizations should measure sensitivities to changes in credit and market risk factors to determine the material drivers of MTM changes. On a regular basis, but no less frequently than quarterly, banking organizations should ensure that CVA MTM changes are sufficiently explained by these risk factors (for example, through profit and loss attribution for sensitivities, and backtesting for value at risk (VaR)).
- Banking organizations hedging CVA MTM should gauge the effectiveness of hedges through measurements of basis risk or other types of mismatches. In this regard, it is particularly important to capture non-linearities, such as the correlation between market and credit risk, and other residual risks that may not be fully offset by hedging.

CVA VaR

Banking organizations with material CVA should measure the risk of associated loss on an ongoing basis. In addition to stress tests of the CVA, banking organizations may develop VaR models that include CVA to measure potential losses. While these models are currently in the early stages of development, they may prove to be effective tools for risk management purposes. An advantage of CVA VaR over more traditional CCR risk measures is that it captures the variability of the CCR exposure, the variability of the counterparty's credit spread, and the dependency between them.

Developing VaR models for CVA is significantly more complicated than developing VaR models for a banking organization's market risk positions. In developing a CVA VaR model, a banking organization should match the percentile and time horizon for the VaR model to those appropriate for the management of this risk, and include all significant risks associated with changes in the CVA. For example, banking organizations may use the same percentile for CVA VaR as they use for market risk VaR (for example, the $95^{th}$ or $99^{th}$ percentile). However, the time horizon for CVA VaR may need to be longer than for market risk (for example, one quarter or one year) because of the potentially illiquid nature of CVA. The following are important considerations in developing a CVA VaR model:

- All material counterparties covered by CVA valuation should be included in the VaR model.
- A CVA VaR calculation that keeps the exposure or the counterparty probability of default static is not adequate. It will not only omit the dependence between the two variables, but also the risk arising from the uncertainty of the fixed variable.
- CVA VaR should incorporate all forms of CVA hedging. Banking organizations and examiners should assess the ability of the VaR measure to accurately capture the types of hedging used by the banking organization.

## 6. Wrong-Way Risk

Wrong-way risk occurs when the exposure to a particular counterparty is positively correlated with the probability of default of the counterparty itself. Specific wrong-way risk arises when the exposure to a particular counterparty is positively correlated with the probability of default of the counterparty itself because of the nature of the transactions with the counterparty. General wrong-way risk arises when the probability of default of counterparties is positively correlated with general market risk factors. Wrong-way risk is an important aspect of CCR that has caused major losses at banking organizations.

Accordingly, a banking organization should have a process to systematically identify, quantify, and control both specific and general wrong-way risk across its OTC derivative and SFT portfolios.[16] To prudently manage wrong-way risk, banking organizations should:

- Maintain policies that formally articulate tolerance limits for both specific and general wrong-way risk, an ongoing wrong-way risk identification process, and the requirements for escalation of wrong-way risk analysis to senior management.
- Maintain policies for identifying, approving, and otherwise managing situations when there is a legal connection between the counterparty and the underlying exposure or the associated collateral.[17] Banking organizations should generally avoid such transactions because of their increased risk.
- Perform wrong-way risk analysis for OTC derivatives, at least at the industry and regional levels.
- Conduct wrong-way risk analysis for SFTs on broad asset classes of securities (for example, government bonds, and corporate bonds).

## IV. Systems Infrastructure Considerations

Banking organizations should ensure that systems infrastructure keeps up with changes in the size and complexity of their CCR exposures, and the OTC derivatives market in general. Systems should capture and measure the risk of transactions that may be subject to CCR as a fundamental part of the CCR management framework.

Banking organizations should have strong operational processes across all derivatives markets, consistent with supervisory and industry recommendations.[18] Management should strive for a single comprehensive CCR exposure measurement platform.[19] If not currently possible, banking organizations should minimize the number of system platforms and methodologies, as well as manual adjustments to exposure calculations. When using multiple exposure measurement systems, management should ensure that transactions whose future values are measured by different systems are aggregated conservatively.

To maintain a systems infrastructure that supports adequate CCR management, banking organizations should:

Data Integrity and Reconciliation

- Deploy adequate operational resources to support reconciliations and related analytical and remediation processes.

[16] A standard way of quantifying general wrong-way risk is to design and apply stress scenarios that detect wrong-way risk in the portfolio, record counterparty exposures most affected by the scenarios, and assess whether the creditworthiness of such counterparties is also negatively affected by the scenario.

[17] Examples of this situation are single-name credit derivatives when there is a legal relationship between the counterparty and the reference entity underlying the transaction, and financing transactions when the counterparty pledges an affiliate's security as collateral.

[18] Examples are recommendations made by the Senior Supervisors Group (SSG) and the Counterparty Risk Management Policy Group (CRMPG).

[19] A single platform may in practice contain a number of separate systems and models. These would be considered a cohesive framework if they are operationally stable and accurate in risk estimation, particularly with regard to proper reflection of collateral and netting. A common programming language for these systems facilitates an effective measurement framework.

- Reconcile positions and valuations with counterparties.
  - Large counterparties should perform frequent reconciliations of positions and valuations (daily if appropriate).[20]
  - For smaller portfolios with non-dealer counterparties where there are infrequent trades, large dealers should ensure the data integrity of trade and collateral information on a regular (but not necessarily daily) basis, reconciling their portfolios according to prevailing industry standards.
- Reconcile exposure data in CCR systems with the official books and records of the financial institution.
- Maintain controls around obligor names at the point of trade entry, as well as reviews of warehoused credit data, to ensure that all exposures to an obligor are captured under the proper name and can be aggregated accordingly.
- Maintain quality control over transfer of transaction information between trade capture systems and exposure measurement systems.
- Harmonize netting and collateral data across systems to ensure accurate collateral calls and reflection of collateral in all internal systems. Banking organizations should maintain a robust reconciliation process, to ensure that internal systems have terms that are consistent with those formally documented in agreements and credit files.
- Remediate promptly any systems weaknesses that raise questions about the appropriateness of the limits structure. If there are a significant number of limit excesses, this may be a symptom of system weaknesses, which should be identified and promptly remediated.
- Eliminate or minimize backlogs of unconfirmed trades.

Automation and Tracking

- Automate legal and operational information, such as netting and collateral terms. Banking organizations should be able to adjust exposure measurements, taking into account the enforceability of legal agreements.
- Automate processes to track and manage legal documentation, especially when there is a large volume of legal agreements.
- Increase automation of margin processes[21] and continue efforts to expand automation of OTC derivatives post-trade processing. This should include automation of trade confirmations, to reduce the lag between trade execution and legal execution.
- Maintain systems that track and monitor changes in credit terms and have triggers for relevant factors, such as net asset value, credit rating, and cross-default.
- Maintain default monitoring processes and systems.

[20] Large dealer counterparties should perform portfolio reconciliation on a daily basis, as set forth in relevant industry standards, such as the ISDA "Collateralised Portfolio Reconciliation Best Operational Practices" (January, 2010).
[21] Banking organizations should consider the recommendations in the "Standards of Electronic Exchange of OTC Derivative Margin Calls," issued by ISDA Collateral Committee on November 12, 2009.

Add-Ons

For large derivatives market participants, certain trades may be difficult to capture in exposure measurement systems, and are therefore modeled outside of the main measurement system(s). The resulting exposures, commonly referred to as add-ons, are then added to the portfolio potential exposure measure. In limited cases, the use of conservative add-on methodologies may be suitable, if the central system cannot reflect the risk of complex financial products. However, overreliance on add-on methodologies may distort exposure measures. To mitigate measurement distortions, banking organizations should:

- Review the use of add-on methodologies at least annually. Current or planned significant trading activity should trigger efforts to develop appropriate modeling and systems, prior to or concurrent with these growth plans.
- Establish growth limits for products with material activities that continue to rely on add-ons. Once systems are improved to meet a generally accepted industry standard of trade capture, these limits can be removed.

## V. Risk Management

### 1. Counterparty Limits

Meaningful limits on exposures are an integral part of a CCR management framework, and these limits should be formalized in CCR policies and procedures. For limits to be effective, a banking organization should incorporate these limits into an exposure monitoring system independent of relevant business lines. It should perform ongoing monitoring of exposures against such limits, to ascertain conformance with these limits, and have adequate risk controls that require action to mitigate limit exceptions. Review of exceptions should include escalation to a managerial level that is commensurate with the size of the excess or nature of mitigation required. A sound limit system should include:

- Establishment and regular review of counterparty limits by a designated committee. Further, a banking organization should have a process to escalate limit approvals to higher levels of authority, depending on the size of counterparty exposures, credit quality, and tenor.
- Establishment of potential future exposure limits, as well as limits based on other metrics. It is a sound practice to limit the market risk arising through CVA, with a limit on CVA or CVA VaR. However, such limits do not eliminate the need to limit counterparty credit exposure with a measure of potential future exposure.
- Individual CCR limits should be based on peak exposures rather than expected exposures.
    - Peak exposures are appropriate for individual counterparty limit monitoring purposes because they represent the risk tolerance for exposure to a single counterparty.
    - Expected exposure is an appropriate measure for aggregating exposures across counterparties in a portfolio credit model, or for use within CVA.
- Consideration of risk factors such as the credit quality of the counterparty, tenor of the transactions, and the liquidity of the positions or hedges.
- Sufficiently automated monitoring processes to provide updated exposure measures at least daily.

- Monitoring of intra-day trading activity for conformance with exposure limits and exception policies. Such controls and procedures can include intra-day limit monitoring, trade procedures and systems that assess a trade's impact on limit utilization prior to execution, limit warning triggers at specific utilization levels, and restrictions by credit risk management on allocation of full limits to the business lines.

## 2. Margin Policies and Practices

Collateral is a fundamental CCR mitigant. Indeed, significant stress events have highlighted the importance of sound margining practices. With this in mind, banking organizations should ensure that they have adequate margin and collateral "haircut"[22] guidelines for all products with CCR.[23] Accordingly, banking organizations should:

- Maintain CCR policies that address margin practices and collateral terms, including, but not limited to:
  - Processes to establish and periodically review minimum haircuts.
  - Processes to evaluate the volatility and liquidity of the underlying collateral. Banks should strive to ensure that haircuts on collateral do not decline during periods of low volatility.
  - Controls to mitigate the potential for a weakening of credit standards from competitive pressure.
- Set guidelines for cross-product margining. Banking organizations offer cross-product margining arrangements to clients to reduce required margin amounts. Guidelines to control risks associated with cross-product margining would include limiting the set of eligible transactions to liquid exposures, and having procedures to resolve margin disputes.
- Maintain collateral management policies and procedures to control, monitor and report:
  - The extent to which collateral agreements expose a banking organization to collateral risks, such as the volatility and liquidity of the securities held as collateral.
  - Concentrations of less liquid or less marketable collateral asset classes.
  - The risks of re-hypothecation or other reinvestment of collateral (both cash and noncash) received from counterparties, including the potential liquidity shortfalls resulting from the re-use of such collateral.
  - The CCR associated with the decision whether to require posted margin to be segregated. Organizations should perform a legal analysis concerning the risks of agreeing to allow cash to be commingled with a counterparty's own cash and of allowing a counterparty to re-hypothecate securities pledged as margin.
- Maintain policies and processes for monitoring margin agreements involving third-party custodians. As with bilateral counterparties, banking organizations should:
  - Identify the location of the account to which collateral is posted, or from which it is received.

[22] A haircut is the difference between the market value of an asset being used as collateral for a loan and the amount of money that a lender will advance against the asset.

[23] See guidelines issued by ISDA, SIFMA and MFA, including the "Market Review of OTC Derivative Bilateral Collateralization Practices (Release 2.0)," March 2010, and "Best Practices for Collateral Management," June 30, 2010.

- Obtain periodic account statements or other assurances that confirm the custodian is holding the collateral in conformance with the agreement.
- Understand the characteristics of the account where the collateral is held (for example, whether it is in a segregated account), and the legal rights of the counterparty or any third-party custodian regarding this collateral.

**3. Validation of Models and Systems:**

A banking organization should validate its CCR models initially and on an ongoing basis. Validation of models should include: an evaluation of the conceptual soundness and developmental evidence supporting a given model; an ongoing monitoring process that includes verification of processes and benchmarking; and an outcomes-analysis process that includes backtesting. Validation should identify key assumptions and potential limitations, and it should assess their possible impact on risk metrics. All components of models should be subject to validation along with their combination in the CCR system.

Evaluating the conceptual soundness involves assessing the quality of the design and construction of the CCR models and systems, including documentation and empirical evidence that supports the theory, data, and methods used.

Ongoing monitoring confirms that CCR systems continue to perform as intended. This generally involves process verification, an assessment of model data integrity and systems operation, and benchmarking to assess the quality of a given model. Benchmarking is a valuable diagnostic tool in identifying potential weaknesses. Specifically, it is the comparison of a banking organization's CCR model estimates with those derived using alternative data, methods, or techniques. Benchmarking can also be applied to particular CCR model components, such as parameter estimation methods or pricing models. Management should investigate the source of any differences in output, and determine whether benchmarking gaps indicate weakness in the banking organization's models.

Outcomes analysis compares model outputs to actual results during a sample period not used in model development. This is generally accomplished using backtesting. It should be applied to components of CCR models (for example the risk factor distribution and pricing model), the risk measures, and projected exposures. While there are limitations to backtesting, especially for testing the longer time horizon predictions of a given CCR model, it is an essential component of model validation. Banking organizations should have a process for the resolution of observed model deficiencies detected by backtesting. This should include further investigation to determine the problem, and appropriate course of action, including changing a given CCR model.

If the validation of CCR models and infrastructure systems is not performed by staff that is independent from the developers of the models, then an independent review should be conducted by technically competent personnel to ensure the adequacy and effectiveness of the validation. The scope of the independent review should include: validation procedures for all components, the role of relevant parties, and documentation of the model and validation processes. This review should document its results, what action was taken to resolve findings, and its relative timeliness.

Senior management should be notified of validation and review results and should take appropriate and timely corrective actions to address deficiencies. The board should be apprised of summary results, especially unresolved deficiencies. In support of validation activities, internal audit should review and test models and systems validation, and overall systems infrastructure as part of their regular audit cycle.

For more details on validation, please see Appendix B.

### 4. Close-Out Policies and Practices

Banking organizations should have the ability to effectively manage counterparties in distress, including execution of a close-out. Policies and procedures outlining sound practices for managing a close-out should include:

- Requirements for hypothetical close-out simulations at least once every two years for one of the banking organization's most complex counterparties.
- Standards for the speed and accuracy with which the banking organization can compile comprehensive counterparty exposure data and net cash outflows. Operational capacity to aggregate exposures within four hours is a reasonable standard.
- The sequence of critical tasks, and decision-making responsibilities, needed to execute a close-out.
- Requirements for periodic review of documentation related to counterparty terminations, and confirmation that appropriate and current agreements that specify the definition of events of default and the termination methodology that will be used are in place.
    - Banking organizations should take corrective action if documents are not current, active and enforceable.
    - Management should document their decision to trade with counterparties that are either unwilling or unable to maintain appropriate and current documentation.
- Established closeout methodologies that are practical to implement, particularly with large and potentially illiquid portfolios. Dealers should consider using the "close-out amount" approach for early termination upon default in inter-dealer relationships.[24]
- A requirement that the banking organization transmit immediate instructions to its appropriate transfer agent(s) to deactivate collateral transfers, contractual payments, or other automated transfers contained in "standard settlement instructions" for counterparties or prime brokers that have defaulted on the contract or for counterparties or prime brokers that have declared bankruptcy.

## VI. Managing Central Counterparty Exposures

A central credit counterparty (CCP) facilitates trades between counterparties in one or more financial markets by either guaranteeing trades or novating contracts, and typically requires all participants to be fully collateralized on a daily basis. The CCP thus effectively bears most of the counterparty credit risk in transactions, becoming the buyer for every seller and the seller to every buyer. Well-regulated and soundly-managed CCPs can be an important means of reducing bilateral counterparty exposure in the OTC derivatives market. However, CCPs also concentrate risk within a single entity. Therefore, it is important that banking organizations centrally clear through regulated CCPs with sound risk management processes, and strong financial resources sufficient to meet their obligations under extreme stress conditions.

[24] The close-out amount approach is defined in CRMPG III, Containing Systemic Risk: Road to Reform (August 6, 2008), pp. 122-125. Also, ISDA has published a closeout amount protocol to aid in the adoption of the close-out amount approach.

To manage CCP exposures, banking organizations should regularly, but no less frequently than annually, review the individual CCPs to which they have exposures. This review should include performing and documenting due diligence on each CCP, applying current supervisory or industry standards[25] (and any subsequent standards) as a baseline to assess the CCP's risk management practices.

- For each CCP, an evaluation of its risk management framework should at a minimum include membership requirements, guarantee fund contributions, margining practices, default-sharing protocols, and limits of liability.
- Banking organizations should also consider the soundness of the CCP's policies and procedures, including procedures for handling the default of a clearing member, obligations at post-default auctions, and post-default assignment of positions.
- Banking organizations should also maintain compliance with applicable regulatory requirements, such as ensuring contingent loss exposure remains within a banking organization's legal lending limit.

## VII. Legal and Operational Risk Management

Banking organizations should ensure proper control of, and access to, legal documentation and agreements. In addition, it is important that systems used to measure CCR incorporate accurate legal terms and provisions. The accessibility and accuracy of legal terms is particularly critical in close-outs, when there is limited time to review the collateral and netting agreements. Accordingly, banking organizations should:

- Have a formal process for negotiating legal agreements. As a best practice, the process would include approval steps and responsibilities of applicable departments.
- At least annually, conduct a review of the legal enforceability of collateral and netting agreements for all relevant jurisdictions.
- Maintain policies on when it is acceptable to trade without a master agreement,[26] using metrics such as trading volume or the counterparty's risk profile.
    - Trading without a master agreement may be acceptable in cases of minimal volume or when trading in jurisdictions where master agreements are unenforceable. As applicable, policies should outline required actions, to undertake and monitor transactions without an executed master agreement.
- Use commonly recognized dispute resolution procedures.[27]

[25] For instance, "Recommendations for Central Counterparties," a consultative report issued by the Committee on Payment and Settlement Systems and the Technical Committee of the International Organization of Securities Commissions under the auspices of the Bank for International Settlements (March 2004).

[26] The capital rules in the United States refer to master agreements. These include: The Federal Reserve's "Risk-Based Capital Standards: Advanced Capital Adequacy Framework — Basel II", 12 CFR 208; Appendix F, and 12 CFR 225; Appendix G." For the FDIC, it is 12 CFR 325, Appendix D. For the OCC, it is 12 CFR Part 3, Appendix C. For the OTS, it is 12 CFR Parts 559, 560, 563, and 567.

[27] An example of such procedures would be the ISDA "2009 Dispute Resolution Protocol" (September 2009).

- Banking organizations should seek to resolve collateral disputes within recommended timeframes.
- Senior management should receive reports listing material and aged disputes, as these pose significant risk.

- Include netting of positions in risk management systems, only if there is a written legal review (either internally or externally) that expresses a high level of confidence that netting agreements are legally enforceable.
- Maintain ongoing participation in both bilateral and multilateral portfolio compression efforts. Where feasible, banking organizations are encouraged to elect compression tolerances (such as post-termination factor sensitivity changes and cash payments) that allow the widest possible portfolio of trades to be terminated.
- Adopt and implement appropriate novation protocols.[28]

### 1. Legal Risk Arising from Counterparty Appropriateness[29]

While a counterparty's ability to pay should be evaluated when assessing credit risk, credit losses can also occur when a counterparty is unwilling to pay, which most commonly occurs when a counterparty questions the appropriateness of a contract. These types of disputes pose not only risk of a direct credit loss, but also risk of litigation costs and/or reputational damage. Banking organizations should maintain policies and procedures to assess client and deal appropriateness. In addition, banking organizations should:

- Conduct initial and ongoing due diligence, evaluating whether a client is able to understand and utilize transactions with CCR as part of assessing the client's sophistication, investment objectives, and financial condition.
  - For example, although some clients may be sophisticated enough to enter into a standardized swap, they may lack the sophistication to fully analyze the risks of a complex OTC deal.
  - Banking organizations should be particularly careful to assess appropriateness of complex, long-dated, off-market, illiquid, or other transactions with higher reputational risk.
- Include appropriateness assessments in the new product approval process. Such assessments should determine the types of counterparties acceptable for a new product, and what level of counterparty sophistication is required for any given product.
- Maintain disclosure policies for OTC derivative and other complex transactions, to ensure that risks are accurately and completely communicated to counterparties.
- Maintain guidelines for determination of acceptable counterparties for complex derivatives transactions.

[28] An example would be the ISDA novation protocol.

[29] For guidance on counterparty appropriateness, see the Federal Reserve's "Trading and Capital Markets Activity Manual," section 2070, pp. 6-7, and the "Interagency Statement on Sound Practices Concerning Elevated Risk Complex Structured Finance Activities" (January 11, 2007).

## VIII. Conclusion

For relevant banking organizations, CCR management should be an integral component of the risk management framework. When considering the applicability of specific guidelines and best practices set forth in this guidance, a banking organization's senior management and supervisors should consider the size and complexity of its securities and trading activities. Banking organizations should comprehensively evaluate existing practices against the standards in this guidance and implement remedial action as appropriate. A banking organization's CCR exposure levels and the effectiveness of its CCR management are important factors for a supervisor to consider when evaluating a banking organization's overall management, risk management and credit and market risk profile.

# Appendix A

## GLOSSARY

This glossary describes commonly used CCR metrics. As discussed above, banking organizations should employ a suite of metrics commensurate with the size, complexity, liquidity, and risk profile of the organization's CCR portfolio. Major broker - dealer banking organizations should employ the full range of risk measurement metrics to enable a comprehensive understanding of CCR and how it changes in varying environments. Banking organizations of lesser size and complexity should carefully consider which of these metrics they need to track as part of their exposure risk management processes. At a minimum, all banking organizations should calculate current exposure and stress test their CCR exposures. Definitions marked with an asterisk are from the Bank for International Settlements.

**Exposure Metrics:**

Current Exposure

*Definition*: Current exposure is the larger of zero, or the market value of a transaction or a portfolio of transactions within a netting set with a counterparty that would be lost upon the default of the counterparty, assuming no recovery on the value of those transactions in bankruptcy. Current exposure is often also called replacement cost. Current exposure may be reported gross or net of collateral.

*Purpose:* Allows banking organizations to assess their CCR exposure at any given time, that is, the amount currently at risk.

Jump-to-Default (JTD) Exposure

*Definition:* JTD exposure is the change in the value of counterparty transactions upon the default of a reference name in CDS positions.

*Purpose:* Allows banking organizations to assess the risk of a sudden, unanticipated default before the market can adjust.

Expected Exposure

*Definition:* Expected exposure is calculated as average exposure to a counterparty at a date in the future.

*Purpose:* This is often an intermediate calculation for expected positive exposure or CVA. It can also be used as a measure of exposure at a common time in the future.

Expected Positive Exposure (EPE)

*Definition:* EPE is the weighted average over time of expected exposures when the weights are the proportion that an individual expected exposure represents of the entire time interval.*

*Purpose:* Expected positive exposure is an appropriate measure of CCR exposure when measured in a portfolio credit risk model.

Peak Exposure

*Definition*: Peak exposure is a high percentile (typically 95 percent or 99 percent) of the distribution of exposures at any particular future date before the maturity date of the longest transaction in the netting set. A peak exposure value is typically generated for many future dates up until the longest maturity date of transactions in the netting set.*

*Purpose:* Allows banking organizations to estimate their maximum potential exposure at a specified future date, or over a given time horizon, with a high level of confidence. For collateralized counterparties, this metric should be based on a realistic close-out period, considering both the size and liquidity of the portfolio. Banking organizations should consider peak potential exposure when setting counterparty credit limits.

Expected Shortfall Exposure

*Definition:* Expected shortfall exposure is similar to peak exposure, but is the expected exposure conditional on the exposure being greater than some specified peak percentile.

*Purpose:* For transactions with very low probability of high exposure, the expected shortfall accounts for large losses that may be associated with transactions with high tail risk.

Sensitivity to Market Risk Factors

*Definition:* Sensitivity to market risk factors, is the change in exposure because of a given market risk factor change (for example, DV01).

*Purpose:* Provides information on the key drivers of exposure to specific counterparties and on hedging.

Stressed Exposure

*Definition:* Stressed exposure is a forward-looking measure of exposure based on pre-defined market factor movements (non-statistically generated). These can include single-factor market shocks, historical scenarios, and hypothetical scenarios.

*Purpose:* Allows banking organizations to consider their counterparty exposure under a severe or stressed scenario. This serves as a supplemental view of potential exposure, and provides banking organizations with additional information on risk drivers. It is best practice to compare stressed exposure to counterparty credit limits.

**CVA Related Metrics:**

Credit Valuation Adjustment (CVA)

*Definition:* The credit valuation adjustment is an adjustment to the mid-market valuation (average of the bid and asked price) of the portfolio of trades with a counterparty. This adjustment reflects the market value of the credit risk resulting from any failure to perform on contractual agreements with a counterparty. This adjustment may reflect the market value of the credit risk of the counterparty or the market value of the credit risk of both the banking organization and the counterparty.*

*Purpose:* CVA is a measure of the market value of CCR, incorporating both counterparty creditworthiness and the variability of exposure.

CVA VaR

*Definition:* CVA VaR is a measure of the variability of the CVA mark-to-market value and is based on the projected distributions of both exposures and counterparty creditworthiness.

*Purpose:* Provides banking organizations with an estimate of the potential CVA mark-to-market loss, at a certain confidence interval and over a given time horizon.

CVA Factor Sensitivities

*Definition:* CVA factor sensitivities is the mark-to-market change in CVA resulting from a given market risk factor change (for example, CR01).

*Purpose:* Allows banking organizations to assess and hedge the market value of the credit or market risks to single names and portfolios and permits banking organizations to monitor excessive buildups in counterparty concentrations.

Stressed CVA

*Definition:* Stressed CVA is a forward-looking measure of CVA mark-to-market value based on pre-defined credit or market factor movements (non-statistically generated). These can include single market factor shocks, historical scenarios, and hypothetical scenarios.

*Purpose:* Serves as an informational tool, and allows banking organizations to assess the sensitivity of their CVA to a potential mark-to-market loss under defined scenarios.

# Appendix B:
## DETAIL ON MODEL VALIDATION AND SYSTEMS EVALUATION

A banking organization should validate its CCR models, initially and on an ongoing basis. Validation should include three components: an evaluation of the conceptual soundness of relevant models (including developmental evidence); an ongoing monitoring process that includes verification of processes and benchmarking; and an outcomes-analysis process that includes backtesting. The validation should either be independent, or subject to independent review.

Validation is the set of activities designed to give the greatest possible assurances of CCR models' accuracy and systems' integrity. Validation should also identify key assumptions and potential limitations, and assess their possible impact on risk metrics. CCR models have several components:

- Statistical models to estimate parameters, including the volatility of risk factors and their correlations;
- Simulation models to convert those parameters into future distributions of risk factors;
- Pricing models that estimate value in simulated scenarios; and
- Calculations that summarize the simulation results into various risk metrics.

All components of each model should be subject to validation, along with analysis of their interaction in the CCR system. Validation should be performed initially as a model first goes into production. Ongoing validation is a means of addressing situations where models have known weaknesses and ensuring that changes in markets, products, or counterparties do not create new weaknesses. Senior management should be notified of the validation results and should take corrective actions in a timely manner when appropriate.

A banking organization's validation process should be independent of the CCR model and systems development, implementation, and operation. Alternately, the validation should be subject to independent review, whereby the individuals who perform the review are not biased in their assessment because of involvement in the development, implementation, or operation of the processes or products. Individuals performing the reviews should possess the requisite technical skills and expertise to provide critical analysis, effective challenge, and appropriate recommendations. The extent of such reviews should be fully documented, sufficiently thorough to cover all significant model elements, and include additional testing of models or systems as appropriate. In addition, reviewers should have the authority to effectively challenge developers and model users, elevate concerns or findings as necessary, and either have issues addressed in a prompt and substantial manner or reject a model for use by the banking organization.

### Conceptual Soundness and Developmental Evidence

The first component of validation is evaluating conceptual soundness, which involves assessing the quality of the design and construction of CCR models. The evaluation of conceptual soundness includes documentation and empirical evidence supporting the theory, data, and methods used. The documentation should also identify key assumptions and potential limitations and assess their possible impact. A comparison to industry practice should be done to identify areas where substantial and warranted improvements can be made. All model components are subject to evaluation, including simplifying assumptions, parameter calibrations, risk-factor diffusion processes, pricing models, and risk metrics. Developmental evidence should be reviewed whenever the banking organization makes material changes in CCR models. Evaluating conceptual soundness includes independent evaluation of

whether a model is appropriate for its purpose, and whether all underlying assumptions, limitations, and shortcomings have been identified and their potential impact assessed.

**Ongoing Monitoring, Process Verification and Benchmarking**

The second component of model validation is ongoing monitoring to confirm that the models were implemented appropriately and continue to perform as intended. This involves process verification, an assessment of models, and benchmarking to assess the quality of the model. Deficiencies uncovered through these activities should be remediated promptly.

Process verification includes evaluating data integrity and operational performance of the systems supporting CCR measurement and reporting. This should be performed on an ongoing basis and includes:

- The completeness and accuracy of the transaction and counterparty data flowing through the counterparty exposure systems.
- Reliance on up-to-date reviews of the legal enforceability of contracts and master netting agreements that govern the use of netting and collateral in systems measuring net exposures, and the accuracy of their representations in the banking organization's systems.
- The integrity of the market data used within the banking organization's models, both as current values for risk factors and as sources for parameter calibrations.
- The operational performance of the banking organization's counterparty exposure calculation systems, including the timeliness of the batch-run calculations, the consistent integration of data coming from different internal or external sources, and the synchronization of exposure, collateral management and finance systems.

"Benchmarking" means comparing a banking organization's CCR measures with those derived using alternative data, methods, or techniques. It can also be applied to particular model components, such as parameter estimation methods or pricing models. It is an important complement to backtesting and is a valuable diagnostic tool in identifying potential weaknesses. Differences between the model and the benchmark do not necessarily indicate that the model is in error because the benchmark itself is an alternative prediction. It is important that a banking organization use appropriate benchmarks, or the exercise will be compromised. As part of the benchmarking exercise, the banking organization should investigate the source of the differences and whether the extent of the differences is appropriate.

**Outcomes Analysis Including Backtesting**

The third component of validation is outcomes analysis, which is the comparison of model outputs to actual results during a sample period not used in model development. Backtesting is one form of out-of-sample testing. Backtesting should be applied to components of a CCR model, for example the risk factor distribution and pricing model, as well as the risk measures and projected exposures. Outcomes analysis includes an independent evaluation of the design and results of backtesting to determine whether all material risk factors are captured and to assess the accuracy of the diffusion of risk factors and the projection of exposures. While there are limitations to backtesting, especially for testing the longer horizon predictions of a CCR model, banking organizations should incorporate it as an essential component of model validation.

Typical examples of CCR models that require backtesting are expected exposure, peak exposure, and CVA VaR models. Backtesting of models used for measurement of CCR is substantially different than backtesting VaR models for market risk. Notably, CCR models are applied to each counterparty facing the banking organization, rather than an aggregate portfolio. Furthermore, CCR models should project the distribution over multiple dates and over long time horizons for each counterparty. These complications make the interpretation of CCR backtesting results more difficult than that for market risk. Because backtesting is critical to providing feedback on the accuracy of CCR models, it is particularly important that banking organizations exert considerable effort to ensure that backtesting provides effective feedback on the accuracy of these models.

Key elements of backtesting include the following activities:

- Back-testing programs should be designed to evaluate the effectiveness of the models for typical counterparties, key risk factors, key correlations and pricing models. Backtesting results should be evaluated for reasonableness as well as for statistical significance. This may serve as a useful check for programming errors, or cases in which models have been incorrectly calibrated.
- Backtesting should be performed over different time horizons. For instance, the inclusion of mean reversion parameters or similar time varying features of a model can cause a model to perform adequately over one time horizon, but perform very differently over a different time horizon. A typical large dealer should, at a minimum, perform backtesting over one day, one week, two weeks, one month and every quarter out to a year. Shorter time periods may be appropriate for transactions under a collateral agreement when variation margin is exchanged frequently, even daily, or for portfolios that contain transactions that expire or mature in a short timeframe.
- Backtesting should be conducted on both real counterparty portfolios and hypothetical portfolios. Backtesting on fixed hypothetical portfolios provides the opportunity to tailor backtesting portfolios to identify whether particular risk factors or correlations are modeled correctly. In addition, the use of hypothetical portfolios is an effective way to meaningfully test the predictive abilities of the counterparty exposure models over long time horizons. Banking organizations should have criteria for their hypothetical portfolios. The use of real counterparty portfolios evaluates whether the models perform on actual counterparty exposures, taking into account portfolio changes over time.

It may be appropriate to use back-testing methods that compare forecast distributions of exposures with actual distributions. Some CCR measures depend on the whole distribution of future exposures rather than a single exposure percentile (for example, EE and EPE). For this reason, sole reliance on backtesting methods that count the number of times an exposure exceeds a unique percentile threshold may not be appropriate.

Exception counting remains useful, especially for evaluating peak or percentile measures of CCR, but these measures will not provide sufficient insight for expected exposure measures. Hence, banking organizations should test the entire distribution of future exposure estimates and not just a single percentile prediction.

Banking organizations should have policies and procedures in place that describe when back-testing results will generate an investigation into the source of observed backtesting deficiencies, and when model changes should be initiated as a result of backtesting.

**Documentation**

Adequate validation and review are contingent on complete documentation of all material aspects of CCR models and systems. This should include all model components and parameter estimation or calibration processes. Documentation should also include the rationale for all material assumptions underpinning its chosen analytical frameworks, including the choice of inputs; distributional assumptions; and weighting of quantitative and qualitative elements. Any subsequent changes to these assumptions should also be documented and justified.

The validation or independent review should be fully documented. Specifically, this would include results, the scope of work, conclusions and recommendations, and responses to those recommendations. This includes documentation of each of the three components of model validation, discussed above. Complete documentation should be done initially and updated over time to reflect ongoing changes and model performance. Ability of the validation (or review) to provide effective challenge should also be documented.

**Internal Audit**

A banking organization should have an internal audit function, independent of business-line management, which assesses the effectiveness of the model validation process. This assessment should ensure the following: proper validation procedures were followed for all components of the CCR model and infrastructure systems; required independence was maintained by validators or reviewers; documentation was adequate for the model and validation processes; and results of validation procedures are elevated, with timely responses to findings. Internal audit should also evaluate systems and operations that support CCR. While internal audit may not have the same level of expertise as quantitative experts involved in the development and validation of the model, they are particularly well suited to evaluate process verification procedures. If any validation or review work is out-sourced, internal audit should evaluate whether that work meets the standards discussed in this section.