EUROPEAN CENTRAL BANK

BANKING SUPERVISION

Sound practices in counterparty credit risk governance and management

October 2023

Contents

1 Introduction

Over the past ten to fifteen years, the low interest rate environment fostered search-for-yield strategies and incentivised some banks to increase the volume of capital market services they provided to more risky and less transparent counterparties, often non-bank financial intermediations (NBFIs) and less regulated or unregulated entities such as hedge funds and family offices.

In its planning for 2022-24, the European Central Bank (ECB) identified exposures to counterparty credit risk (CCR) as a supervisory priority for 2022 and initiated a range of supervisory actions. Following the collapse of Archegos Capital Management, the ECB, like other supervisors of major jurisdictions, reviewed the risk management practices of a sample of banks that were particularly active in providing prime brokerage services, a specific capital markets activity with high CCR exposure, and in August 2022 published its supervisory expectations for prime brokerage services (PBS).[1]

In the last quarter of 2022, the ECB concluded a targeted horizontal review of governance and risk management of CCR at 23 institutions that were materially active in derivatives and securities financing transactions (SFTs) with non-banking counterparties. The review was also an occasion to assess how some banks were meeting the expectations on PBS, which are reflected – albeit in more general terms – in the sound practices presented in this document.

In consideration of the volatility of energy and commodity prices brought about by Russia's war in Ukraine, particular attention was paid to non-financial counterparties such as commodity traders and energy utilities.

Some institutions exposed to CCR were not included in the sample of the targeted review but were subject to on-site inspections whose scope and findings were closely aligned to and integrated with the off-site targeted review.

1.1 Background

Since the collapse of Long-Term Capital Management (LTCM), a highly leveraged hedge fund, in 1998, the international community of banking supervisors has been increasingly vigilant about CCR. By January 1999 the Basel Committee on Banking Supervision (BCBS), through its "Sound Practices for Banks' Interactions with Highly Leveraged Institutions"[2], called for thorough customer due diligence and cautioned against overreliance on the collateralisation of mark-to-market exposures.

---

1 See "Supervisory expectations for prime brokerage services", *Supervision Newsletter*, ECB, 17 August 2022.

2 See "Sound Practices for Banks' Interactions with Highly Leveraged Institutions", Basel Committee on Banking Supervision, January 1999.

In September 2000 the BCBS issued its "Principles for the Management of Credit Risk".[3] In this publication, the Committee also highlighted the need for a clear and detailed definition of a bank's strategy and risk tolerance for CCR arising from derivatives and SFTs in the banking and trading books. The BCBS clarified that banks must receive sufficient information for a comprehensive assessment to be made of the true risk profile of a counterparty, including the counterparty's capacity to repay based on historical trends and future projections under various scenarios.

Furthermore, the industry provided valuable contributions for the sound management of CCR. For example, following the June 1999 report of the first Counterparty Risk Management Policy Group (CRMPG), in July 2005 the second CRMPG (CRMPG II) issued recommendations on how to limit the probability and severity of financial shocks.[4] In particular, the Group noted that CCR is one of the main variables in determining whether, and with what speed, financial disturbances become financial shocks, and also that the evaporation of market liquidity is influenced by crowded trades and other circumstances that cannot be anticipated by individual institutions. Three years later in the middle of the global financial crisis and just before the bankruptcy of Lehman Brothers and the bailout of American International Group (AIG), the third CRMPG (CRMPG III) was stressing the need for banks to have daily and comprehensive information in place on the exposure to their counterparties in order to obtain insights into concentrated positions and crowded trades.[5] The Group also suggested regular interaction among global institutions to better identify and manage future sources of contagion risk.

The global financial crisis of 2007-08 prompted banking regulators to undertake a major review of the Basel framework's minimum capital requirements (Basel III) to better tackle CCR, excessive leverage and liquidity risk. For CCR, the internal model method (IMM) was enhanced to better reflect margined trading, and specific and general wrong-way risk (WWR) were included in the framework. Some years later the standardised approach for CCR was revised, with the objective of making it more risk-sensitive but also of discouraging institutions from entering into derivatives transactions without sufficient risk-bearing capacity.

In parallel with the review of the Basel framework, some supervisors expressed expectations on CCR management. Most notably, US supervisors jointly published their "Interagency Supervisory Guidance on Counterparty Credit Risk Management" in June 2011[6]. In their guidance, the US supervisors stress that CCR is a multidimensional form of risk, affected by the exposure to a counterparty as well as its credit quality, both of which are sensitive to market-induced changes. Moreover, CCR is also affected by the interaction of these risks, e.g. the correlation between an exposure and the credit spread of the counterparty. Hence, constructing an effective

---

3 See "Principles for the Management of Credit Risk", Basel Committee on Banking Supervision, September 2000.

4 See "Toward Greater Financial Stability: A Private Sector Perspective", The Report of the Counterparty Risk Management Policy Group II, 27 July 2005.

5 See "Containing Systemic Risk: The Road to Reform", The Report of the CRMPG III, 6 August 2008.

6 See "Interagency Supervisory Guidance on Counterparty Credit Risk Management", Office of the Comptroller of the Currency, Federal Deposit Insurance Corporation, Board of Governors of the Federal Reserve System and Office of Thrift Supervision, 29 June 2011.

CCR management framework requires a combination of risk management techniques from the credit, market and operational risk disciplines.

Lastly, in February 2023 the Financial Stability Board (FSB) published "The Financial Stability Aspects of Commodities Markets"[7], providing another example of how the combination of market events can result in a concerning build-up of CCR. The report outlines the heterogeneity of commodity markets in terms of market structure and practices, and also points to the interconnectedness of a small number of non-financial commodity traders – some highly leveraged – with core financial sector participants. The review performed by the FSB also suggests that some commodity traders are able to meet their liquidity demand by increasing credit facilities or borrowing additional funds. Additionally, it was observed that market participants have adapted to volatility by reducing funding liquidity risk and taking more credit and market risk, most notably in the form of CCR, by migrating from centrally cleared to uncleared derivatives to reduce the risk of margin shocks.

1.2 Objective

This document should be read in conjunction with the prudential requirements set out in the EU's regulatory framework and other applicable regulatory frameworks, as well as standards set on an international level. While a rigorous implementation of the regulatory framework is crucial, institutions are expected to go beyond mere compliance with regulatory minimum requirements when designing their risk management and control approaches to CCR. These approaches should be proportionate to the scale and complexity of the business, products offered and the nature of the counterparties. In doing so, institutions need to be prepared to keep pace with the risks that are relevant for CCR management associated with an increasingly fast-moving and complex market situation.

The document provides a collection of sound practices in CCR governance and management that were observed during the performance of the targeted review. It also contains an assessment of the convergence towards those practices, accounting for the principle of proportionality (particularly for institutions with a less complex CCR business). The ultimate objective is to encourage institutions to improve their risk management capabilities in a way that is commensurate with their CCR profile.

It is acknowledged that in their individual implementation, some practices might need to be adapted to the specific characteristics of institutions and that various configurations of CCR can be addressed by different organisational arrangements. Institutions should always look at the sound practices in the light of their overall approach to CCR and the size and complexity of their CCR portfolio, which might change over time. The growing NBFI sector as well as any other non-banking counterparty whose business strategy is particularly vulnerable to market shocks are two examples. While stress testing is one crucial tool for identifying such clients and

[7] See "The Financial Stability Aspects of Commodities Markets", Financial Stability Board, 20 February 2023.

the potential risks associated with their portfolios that are not covered by regulatory capital requirements, institutions can also use Pillar II models to better capture the many facets of CCR in the exposure calculation. Developments in business practices might affect CCR governance and management practices. Hence, institutions should also expect the nature of these sound practices to evolve over time.

2 Overview of the targeted review

The assessment of the targeted review carried out in 2022 consisted of three phases: (i) sample selection based on CCR materiality and the most relevant key risk indicators, (ii) identification of sound practices across institutions for the different areas of interest, and (iii) benchmarking of the institutions in the sample against those sound practices.

Supervisory tools used in the targeted review included a qualitative questionnaire, supporting documents from institutions, such as process descriptions or relevant committee and management body reports, as well as the results of meetings with key function holders of some institutions. The conclusions of relevant on-site inspections were also included in the assessment.

Bank-specific assessments were subject to a horizontal quality assurance to ensure consistency in the identification of areas requiring improvement, considering the above-mentioned principle of proportionality. In the first quarter of 2023 Joint Supervisory Teams (JSTs) began discussing bank-specific observations with supervised institutions. Observations are followed up, where necessary, as part of the ongoing supervisory work and within the Supervisory Review and Evaluation Process (SREP) assessment. Follow-up activities may include additional dedicated on-site inspections.

2.1 Overview of CCR in the sample of selected institutions

CCR originates from a variety of non-traditional lending activities, where the types of transaction can be broadly differentiated as either derivatives or SFTs.

At the reference date for the exercise (31 March 2022), the banks selected for the targeted review held on aggregate approximately €1,245 billion of CCR exposure value (of which, 59% was derivatives and 41% SFTs) and €278 billion of CCR risk-weighted exposure amount (RWEA) (of which, 82% was derivatives and 18% SFTs), as illustrated in Chart 1. The criteria employed for the sample selection captured not only the institutions contributing most in absolute terms, but also those for which CCR was of particular relative relevance. While, on average, the share of CCR RWEA as a portion of total RWEA was just below 10%, for some institutions the share was well over 35%, reflecting the importance of these market operations within their overall mix of activities.

Most institutions in the sample could be categorised as either universal banks (including global systematically important banks (G-SIBs)) or investment banks. There is a certain variety in the spectrum of transactions and counterparty types giving rise to CCR. For example, repo transactions originated by the treasury function with a central bank may be large in exposure volume but attract little or no risk weight, while longer-term derivatives with corporates or other financial

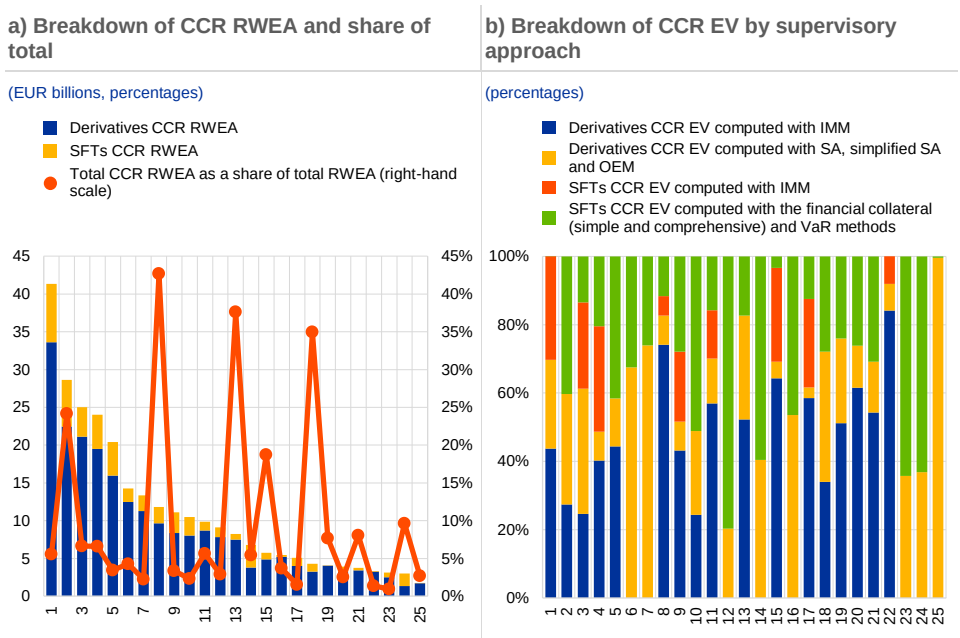
institutions expose a bank to higher CCR RWEA. Further elements of risk mitigation such as collateralisation, margining and netting, or central clearing, play a very important role in the determination of the exposure size and add further complexity. Indeed, a higher share of centrally cleared transactions reduces the associated CCR RWEA also because of the lower regulatory risk weights associated with exposures to central counterparties (CCPs). However, centrally cleared business activities can expose institutions and their clients to other types of risk such as liquidity risk or the risk of margin shocks.

Institutions subject to the targeted review and related on-site inspections also showed a mix of regulatory methodologies for computing CCR exposure values, with 17 banks using the IMM for derivatives and nine banks using this method for SFTs. For the risk weighting of CCR exposures, the sample reflected the Single Supervisory Mechanism's (SSM) landscape of institutions making use of the internal ratings based approach and the standardised approach (SA) for credit risk.

Chart 1 panel a) provides an overview of CCR RWEA for the institutions in the sample, while panel b) shows the share of CCR exposure subject to the IMM or non-IMM methods. The share of total CCR exposure value (EV) that is not centrally cleared is on average about 84%, as per supervisory reporting information.

Chart 1

Key information from Common Reporting (COREP) for banks in the sample



Source: COREP, as of the targeted review reference date (31 March 2022).
Notes: The charts display figures for institutions included in the sample for the targeted review as well as for institutions subject to on-site inspections at the time of the review.

Institutions that were subject to an off-site targeted review provided qualitative information about the broad spectrum of activities across trade types and counterparties. Differences in the level of complexity of instruments and underlying risks broadly reflect differences in business models and in the relevance of trading operations within banking groups.

In terms of derivatives, Table 1 shows that banks in the sample engaged in transactions ranging from low to high complexity,[8] with almost all active in rates and foreign exchange (FX) products, followed by equity and credit, while fewer banks traded more complex underlying risk types as well.

Table 1

Sources of CCR: overview of derivatives transactions by degree of complexity and type of underlying risk for banks in the sample

	Low complexity derivatives	Medium complexity derivatives	High complexity derivatives
Equities			
Interest rates			
Credit			
Currencies			
Commodities (including precious metals)			
Volatilities			
Correlations			
Dividends			
Inflation			
Other (including exotic underlyings)			

Source: Questionnaire submitted by banks in the sample.
Notes: Darker shades indicate more banks considering a certain combination as being relevant for them.

Table 2 shows that underlying securities of SFTs reported by banks were typically investment-grade (IG) bonds, but also other types of debt security (covered bonds, ABS), including a relatively high percentage of sub-investment-grade assets (e.g. high-yield bonds). Single equity stocks were a very common asset type for securities borrowing/lending as well as margin financing activities. Nearly all banks reported engaging, for various purposes, in total return and collateral swaps transactions with different reference assets.

[8] Classification performed by banks based on grouping categories defined under Article 7(a), (b) and (c) of the EBA Final draft Regulatory Technical Standards on the internal model approach assessment methodology (EBA/RTS/2016/07).

Table 2

Sources of CCR: overview of SFTs by transaction type and underlying security type for banks in the sample

	Repurchase transactions (including buy-sell back or sell-buy back transactions)	Securities or commodities lending or borrowing transactions	Margin lending transactions
Government bonds (IG)			
Government bonds (sub-IG)			
Corporate bonds (IG)			
Corporate bonds (sub-IG)			
Covered bonds			
Single equity stocks			
Equity indices			
ABS/MBS and similar			
Funds			
Other			

Source: Questionnaire submitted by banks in the sample.
Notes: Darker shades indicate more banks considering a certain combination as being relevant for them. IG stands for investment grade.

It is worth noting that the contractual possibility of collateral re-use (on both sides of a trade) in the context of SFTs is very high, underscoring the importance of sound collateral management and monitoring frameworks.

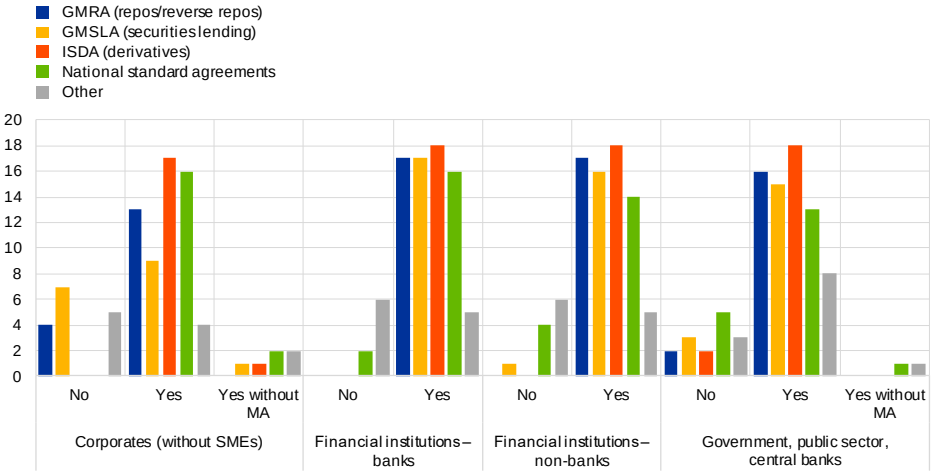
Turning to individual counterparties, based on information disclosed by banks in the questionnaire, concentrations are structurally largest for exposures to CCPs (with a number of direct/indirect clearing memberships, as well as client clearing services) but also to other banks (typically global dealers) and to some recurring corporate names. Insurers, asset managers and pension funds are the typical NBFI counterparties, while in most cases no large exposures to riskier NBFIs such as hedge funds were reported. Although most institutions in the sample stated that they conducted business with hedge funds, hedge funds were a major source of CCR for only a few.

From a contractual agreement perspective, the information provided by the institutions shows that industry or national standard netting agreements are widely used across the different counterparty types, as shown in Chart 2. The chart also shows that in most cases, institutions use netting in conjunction with margin agreements, although, for corporates, margining is often limited to counterparties for which it is required under the European Market Infrastructure Regulation (EMIR) or to cases in which activities carried out with the client are subject to clearing.

Chart 2

Netting agreement types per counterparty type

(number of institutions making use of netting agreements, with and without margining agreement (MA))



Source: Questionnaire submitted by banks in the sample.
Notes: "GMRA" refers to agreements using the Global Master Repurchase Agreement, "GMSLA" refers to agreements using the Global Master Securities Lending Agreement, "ISDA" refers to agreements using the Master Agreement of the International Swaps and Derivatives Association (ISDA), "Other" refers to other master netting agreements.

2.2 Summary of observations

The targeted review confirmed the progress already made by institutions and identified a number of good industry practices. However, it also exposed several material shortcomings compared with sound practices, even accounting for differences in terms of scale, complexity of the business, products offered and nature of the counterparties. More specifically:

- Customer due diligence procedures, both at onboarding and on an ongoing basis, should be improved when dealing with non-banking counterparties and have a substantial impact on credit decisions and contractual conditions. This includes taking a more conservative approach towards setting credit terms for clients failing to provide information transparently. First and second lines of defence (1LoD and 2LoD) should monitor those counterparties to ensure they provide transparent information on whether sufficient shock-absorbing capacity and adequate policies, procedures and controls are in place.

- Institutions with material or complex CCR exposures should explicitly specify their willingness to accept this risk in their risk appetite statement, rather than capturing it implicitly in credit risk, as CCR might present additional complexities compared with general credit risk.

- The stress testing framework should address not only counterparties' creditworthiness, but also their vulnerability to specific exposure tail events, where such vulnerabilities can be magnified by combinations of WWR, high leverage, maturity mismatch and non-linearities resulting from exposure to crowded trades. The framework should aim to identify counterparties whose

solvency or liquidity position might come under pressure in certain market scenarios, and to detect concentrations in exposures to margin shocks, a significant build-up in credit exposures or vulnerabilities to rapid deleveraging, among other potential vulnerabilities. The frequency of stress tests should reflect a rapidly changing risk environment. Stress testing results should have an impact on decision-making, including proactive risk mitigation strategies.

- There is still room for improvement in how, on a firm-wide basis, CCR is mitigated, monitored and managed when a counterparty is in trouble or defaults. In many cases, static margins have not yet been replaced with more risk-sensitive arrangements. Early warning indicators specific to derivatives and SFTs, such as discipline in margin payments, are not always considered when compiling watchlists.

2.3 Overview of sound practices

The targeted review and the on-site inspections showed that some of the institutions in the sample apply leading practices in each of the four areas of the assessment, namely: (i) CCR governance; (ii) risk control, management and measurement; (iii) stress testing and WWR; and (iv) watchlist and default management process (DMP). The number of institutions already applying leading practices varies across the assessed areas.

This document describes 43 observed sound practices, drawn from the assessed institutions, and provides additional insights about the convergence towards those practices. It also shows the areas where there is greater need for improvement across a higher number of institutions.

The fact that several sound practices have been observed in almost all institutions demonstrates the sector's ability to adapt to changing market conditions. However, there are clearly areas in which few institutions deploy sound practices, indicating the need for further efforts to enhance CCR governance and management approaches across the industry.

Table 3

Sound practices described in this report

Chapter	Section	#	Topic
3 CCR governance	3.2 Sound practices for CCR governance	1	Presence of a three lines of defence model for CCR
		2	Dedicated CCR framework with clear responsibilities for 1LoD and 2LoD
		3	Sufficient 1LoD and 2LoD resources for all CCR counterparties
		4	Daily monitoring and management processes for high-risk clients
		5	Dedicated coverage of CCR in relevant committees
		6	Sufficiently detailed CCR-related reporting to senior management
		7	Appropriate collateral management processes and reporting
		8	Inclusion of the risk assessment of CCR exposures in the credit risk assessment
		9	Inclusion of the results of customer due diligence processes in credit decisions and recognition of CCR in customer due diligence processes

Chapter	Section	#	Topic
		10	Assessment of CCR in new product processes
		11	Effective processes for NBFI client identification and monitoring
		12	Explicit assessment of the CCR framework by 3LoD, i.e. internal audit
4 Risk control, management and measurement	4.2 Sound practices for risk control, management and measurement	13	Identification of CCR sources and assessment of materiality
		14	CCR framework commensurate with CCR risk profile
		15	Adequate recognition of CCR in the RAS
		16	Policies addressing risk acceptance for CCR as an integral part of the RAF
		17	Adequate limit framework for CCR
		18	Appropriate choice of CCR metrics
		19	Effective monitoring of counterparty concentrations to margin shocks
		20	Adequate identification and monitoring of illiquid and concentrated positions
		21	Appropriate economic measure for costs of CCR portfolio wind-down
5 Stress testing and WWR	5.2 Sound practices for stress testing and WWR	22	Documented governance for stress testing framework
		23	Explicit consideration of the CCR component in stress testing
		24	Comprehensive set of CCR-relevant stress scenarios
		25	Use of stress testing framework for the identification and monitoring of increasing risks for high-risk clients
		26	Explicit stress testing of CCR exposures in the ICAAP to identify clients vulnerable to tail risk events
		27	Adequate WWR framework included in the RAF
		28	Identification and monitoring of GWWR with well-defined models and data
		29	Identification of GWWR under specific market stress events
		30	Sound SWWR assessment and monitoring
		31	SWWR identification without legal connection
6 Watchlist and default management processes	6.2 Sound practices for watchlist and default management processes	32	Documented watchlist policy
		33	Definition of relevant watchlist indicators including CCR
		34	Defined actions based on watchlist classification
		35	A posteriori review of watchlist performance
		36	Clear ownership of DMP policy
		37	DMP policy implementing governance of default management
		38	Description of a binding process and identification of clear responsibilities
		39	Integration of risk management functions in DMP decision-making
		40	Procedures conducive to effective information flows and default management
		41	Post-default process ensuring minimal losses and legal risks
		42	For market-makers, assessment of (local) close-out capabilities
		43	Regular fire drills for the DMP

3 CCR governance

This section describes sound practices for the first assessment area of the CCR targeted review and looks more closely at the governance framework for CCR, including collateral management.

Since CCR is a special type of credit risk, the requirements and supervisory expectations for credit risk governance and management apply. Given its nature, those requirements and expectations are complemented by more specific provisions for CCR. In this regard, it should be noted that some requirements are directly applicable only to institutions using the IMM for CCR. However, those provisions can serve as a reference point for other institutions with a material or more complex CCR portfolio.

Directive 2013/36/EU (Capital Requirements Directive, or the CRD) and Regulation 2013/575/EU (Capital Requirements Regulation, or the CRR) set out minimum requirements for institutions, including sound internal governance models and effective risk management (see Article 74(1) CRD). This requirement is further specified in the European Banking Authority (EBA) Guidelines on internal governance (EBA/GL/2021/05). Moreover, institutions should also fulfil requirements on credit and CCR in relation to the granting and monitoring of credit facilities throughout their life cycle, as laid down in Article 79 CRD, which is further specified in the EBA Guidelines on loan origination and monitoring (EBA/GL/2020/06).

More specifically, Article 286(1) CRR requires institutions to establish and maintain a CCR management framework consisting of policies, processes and systems to ensure the identification, measurement, management, approval and internal reporting of CCR. An institution's management body and senior management must be actively involved in, and ensure that, sufficient resources are allocated to the management of CCR.

Article 287(2) CRR on the organisation of CCR risk management of IMM institutions requires an independent control unit to be set up (i.e. 2LoD) and sets out specific tasks that this unit must fulfil (design and implementation of the CCR management systems, daily reports).

Article 287 CRR also establishes a set of requirements for the collateral management of IMM institutions. Accordingly, a bank must set up a collateral management unit, responsible for the tasks listed in Article 287(3) CRR. Those tasks notably relate to margin calls and dispute management, reconciliation activities, collateral re-use and concentration, reporting and involvement of senior management. In addition, Article 288 CRR prescribes regular independent reviews of the collateral management unit activities.

According to Chapter 4 of the ECB Guide on assessment methodology (EGAM),[9] supervisors will review the soundness of an institution's internal governance for CCR management and discuss the performance of tasks with relevant staff members of the institution. Supervisors also assess compliance with the above-mentioned CRR requirements by reviewing internal policies and procedures and internal reports from collateral management units, internal audit or risk management functions.

Collateral used to mitigate CCR plays a crucial role in the relationship with the customer. It also has implications for liquidity management and might give rise to operational risk. Therefore, the role of collateral and its proper management have been extensively discussed by the BCBS.[10] In its publications, the BCBS has underlined that in-depth credit analyses as well as appropriate credit standards and processes play a key role, and that overreliance on collateralisation of individual exposures should be avoided. Instead, institutions should enter transactions with a customer based primarily on the strength of the borrower's repayment capacity,[11] because collateral is neither a substitute for the comprehensive assessment of the counterparty's creditworthiness, nor can it compensate for insufficient information.

Furthermore, Principle 3 of the BCBS Principles for the Management of Credit Risk of September 2002[12] stresses that institutions should ensure that the risks of products and activities new to them are subject to adequate risk management procedures and controls before being introduced or undertaken, and they should be approved in advance by the management body or its appropriate committee. Principle 6 reaffirms the need for a clearly established process for approving new credit limits as well as for the amendment, renewal and refinancing of existing credit limits. This supports the earlier communication[13] which states that effective monitoring of the activities of highly leveraged clients requires thorough knowledge and understanding of their trading strategies, exposure levels, risk concentrations and risk controls by an institution. Reliance on collateral cannot replace day-to-day risk management and monitoring, especially for high-risk and other material clients.

3.1 Range of practices for CCR governance

In most cases, CCR roles and responsibilities are set according to the three lines of defence model. More complex institutions have generally more sophisticated setups. Overall, the following was observed:

---

9 See "ECB Guide on assessment methodology (EGAM)", ECB, February 2020.

10 See, for example, "Sound Practices for Banks' Interactions with Highly Leveraged Institutions", Basel Committee on Banking Supervision, January 1999 and "Principles for the Management of Credit Risk", Basel Committee on Banking Supervision, September 2000).

11 In paragraph 34 of the "Principles for the Management of Credit Risk", the BCBS says that banks "can utilise transaction structure, collateral and guarantees to help mitigate risks (both identified and inherent)".

12 See "Principles for the Management of Credit Risk", Basel Committee on Banking Supervision, September 2000.

13 See "Sound Practices for Banks' Interactions with Highly Leveraged Institutions", Basel Committee on Banking Supervision, January 1999.

- 1LoD: Business lines, mainly corporate and investment banking and global financial markets, are the CCR risk owners. Treasury and asset and liability management (ALM) units are also CCR risk owners using appropriate transactions to manage liquidity and hedge the balance sheet. Within banking groups, CCR risk owners can be located at both subsidiary and group level.
- 2LoD: In general, CCR falls under the credit risk 2LoD. Many institutions have a dedicated 2LoD team responsible for CCR, with specific know-how and risk monitoring tools.
- Third line of defence (3LoD): With regard to the role of internal audit, it was noted that IMM institutions and institutions that are more active in derivatives trading perform more detailed internal audits on CCR governance and management on a more frequent basis.

Some of the most sophisticated globally active banks with large CCR exposures and more intensive business relationships with risky counterparties (such as hedge funds) have dedicated risk teams in the 1LoD. However, those teams appeared to be able to ensure an adequate coverage of all relevant counterparties only in a few cases.

Within the 2LoD, the more advanced institutions have teams of specialists with knowledge of both credit and market risk, benefiting from dedicated tools and infrastructure. Less advanced institutions rely on separate credit risk and market risks teams to monitor the contribution of capital market transactions to the overall risk of the institution.

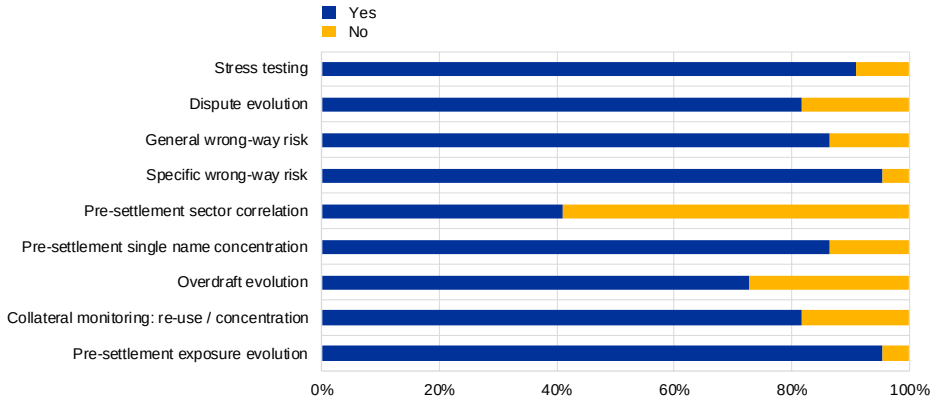
Most banks have conducted several audits on CCR topics in the past three years or plan to do so in 2023. Only a few banks have not conducted any internal audits in the past few years and have no clear plans for the short term. However, audits often tackle CCR from the perspective of the individual business unit using a piecemeal approach. Only a few banks have adopted a holistic audit approach to CCR processes and governance across their organisation.

In nearly all cases, CCR is integrated into the credit risk committees' workflow and very few banks have specific CCR governance committees. By the same token, only a small fraction of banks has dedicated committees/management fora or working level fora to discuss CCR topics. Most banks leverage risk committees (committees to which risk management has been delegated by the management body) or credit committees (the highest management forum of the credit department) to discuss CCR topics. Generally, CCR topics are discussed monthly. In some cases, the frequency is even lower (quarterly).

Only a small fraction of banks prepare dedicated CCR reports for senior management. For many institutions, CCR reporting is part of the wider credit risk reporting process. In their reporting to senior management, institutions provide different elements of CCR (Chart 3), sometimes scattered across a number of reports.

Chart 3

Elements of CCR monitored by/reported to senior management at consolidated level



Source: Questionnaire submitted by banks in the sample.
Notes: Figures populating the chart have been re-worked centrally by the ECB as not all institutions in the sample may have provided an answer or an answer that is consistent with that submitted by other banks.

Most institutions that carry out the strategic monitoring of pre-settlement exposure evolution also include this in reporting to senior management (sometimes as part of counterparty exposure monitoring). In most, but fewer, institutions, senior management monitors collateral and disputes, while in less than half of the institutions it also monitors sector correlations. Different units may be responsible for different monitoring activities. Some institutions specified that it is more common for a (traded) credit risk management/control unit to perform strategic monitoring on aspects related to exposures, while collateral-related matters and disputes may be the responsibility of a dedicated collateral unit or back office.

Most banks have set up a dedicated collateral management unit, sometimes also responsible for EMIR compliance. However, only a few concentrate all the tasks listed in Article 287 CRR in a single collateral management unit. It is commonly observed that other units are responsible for some collateral management tasks, such as monitoring collateral concentration and re-use or reporting. It is also worth noting that the structure and mandate of the collateral management unit depend on the type of accepted collateral (only cash vs cash and non-cash securities). Dispute escalation processes are generally structured according to the size (absolute/relative) and duration of disputes. In about half the institutions, an independent review of collateral management is conducted annually. The other banks follow a two to three-year review cycle.

The particularities of CCR (dynamics of the exposure, interlinks among exposure, probability of default and value of the collateral) are not fully appreciated and addressed by several less sophisticated institutions, although complex transactions and/or higher-risk counterparties have become part of their portfolios. Banks that do not have a strong capital markets presence tend to have a less explicit focus on CCR, with reported metrics centred more on the current credit risk exposure (current exposure, nominal amount).

3.2 Sound practices for CCR governance

1. Presence of a three lines of defence model for CCR

Institutions have dedicated, comprehensive governance and risk management frameworks in place to deal with increased CCR exposures from market activities in derivatives, SFTs or long settlement transactions. These frameworks include a well-defined three lines of defence model with proper allocation of responsibilities and clear reporting lines.

2. Dedicated CCR framework with clear responsibilities for 1LoD and 2LoD

For institutions with material or complex CCR portfolios, a dedicated CCR framework is in place, including specific teams with market risk or CCR expertise in 1LoD and 2LoD to support credit risk-focused teams.

3. Sufficient 1LoD and 2LoD resources for all CCR counterparties

1LoD and 2LoD units are set up to monitor and manage all CCR transactions with individual counterparties. For each large counterparty, an individual or a group of persons is explicitly assigned, both in 1LoD and 2LoD.

For subsidiaries of a banking group, the local risk management function is participating in, and is accountable for, the decision-making process related to CCR transactions of the relevant subsidiary.

4. Daily monitoring and management processes for high-risk clients

Institutions dealing with material counterparties whose risk profile, liquidity or solvency situation can change quickly (e.g. hedge funds or other entities whose solvency and/or liquidity depends on portfolio performance as a result of high leverage, active daily trading, their business activities or other circumstances) set up additional risk control processes to monitor and manage the CCR exposure to those clients on a daily basis. Such processes may be embedded in and supported by teams both in 1LoD or 2LoD.

5. Dedicated coverage of CCR in relevant committees

The structure of committees or fora involved in the risk management process facilitates effective cooperation among the various teams involved in CCR management. In institutions with material or complex CCR exposure, exchanges between 1LoD and 2LoD are duly formalised. As a minimum, the management body or a delegated committee (e.g. risk committee) regularly receives a comprehensive report, highlighting the outcome of CCR monitoring.

In addition, as part of their risk appetite framework or related policies, institutions have clear thresholds that trigger notifications and approvals or decision-making by management with sufficient seniority, appropriate to the materiality of the issue. This includes a clear limit breach procedure outlining the escalation process and reporting breaches of internal risk limits at counterparty level.

6. Sufficiently detailed CCR-related reporting to senior management

Regular CCR reporting to an institution's senior management allows management to understand (i) the current level of exposure (i.e. magnitude of potential losses when counterparties default), (ii) how this exposure may evolve in the future, and (iii) which losses may occur with varying degree of likelihood. Furthermore, the reporting allows senior management to identify market scenarios with most material impact on the risk profile of an institution.

Consequently, this reporting includes at least the following items:

- overview of current and potential future exposures (PFE) based on internal and regulatory metrics (present value, current exposure, PFE, effective expected positive exposure (EEPE) and exposure at default (EAD)), including trend analysis and key risk drivers of the development;
- identification of concentrated and illiquid collateral and hard-to-replace transactions;
- stress test results at the portfolio level and for counterparties with the largest exposures;
- WWR analysis;
- overview of the largest CCR exposures, including CCPs;
- overview of weak counterparties with material exposures, with special regard to those already on the watchlist and under close monitoring.

Institutions either entering material SFT transactions or accepting non-cash collateral regularly report the composition of the collateral accepted and potentially concentrated positions.

7. Appropriate collateral management processes and reporting

Institutions organise the main tasks of CCR collateral management in a dedicated collateral management unit or units which have clear responsibilities.

Regular reporting by the collateral management unit to the senior management of the institution allows the management to oversee the current collateralisation structure, including concentration risk and the status of margin disputes. The reporting reflects the complexity of the exchanged collateral in terms of structure and periodicity. It also includes information about collateral re-use, where applicable. Processes and procedures to handle and escalate margin and margin call disputes are implemented. Senior management is informed about material or persisting disputes in a timely manner through regular and ad hoc reporting.

The collateral management framework is subject to a regular independent review. This review reflects the complexity of the framework in terms of depth and frequency.

8. Inclusion of the risk assessment of CCR exposures in the credit risk assessment

The credit risk assessment of the most material counterparties (e.g. by gross size of the portfolio) considers illiquid or hard-to-replace transactions contained in the portfolio with these counterparties. Furthermore, the overall credit risk assessment contains an analysis of how the capital position of the institution would evolve under stress (via an increase in CCR RWEA and direct impact on Common Equity Tier 1 (CET1) capital) as a result of losses from defaults of such counterparties.

9. Inclusion of the results of customer due diligence processes in credit decisions and recognition of CCR in customer due diligence processes

Far from being a pro forma exercise, customer due diligence – both at onboarding and on an ongoing basis – has a substantial impact on credit decisions. Adequate, comprehensive, well-documented customer due diligence procedures take into account the particularities of CCR and aspects of the client relationship, especially for clients whose business strategy is vulnerable to market stress events. Among other things, customer due diligence includes an assessment of a client's solvency position and financial resources, as well as its operational capability to manage and mobilise those resources in times of market stress. A client's failure to provide information results in a more conservative approach to credit rating, limit setting, margining and other forms of credit risk mitigation, or even the rejection or offboarding of the client.

10. Assessment of CCR in new product processes

The new product approval process includes a clear policy for new transactions carrying CCR, including a clearly documented escalation procedure. Exceptions to the product approval process (e.g. for particular clients) are duly documented, including (i) a description of the conditions under which approval could be granted, (ii) the required management level, and (iii) the minimum risk information needed for an informed decision to be made on such exceptions.

11. Effective processes for NBFI client identification and monitoring

Institutions with significant exposures to NBFI/NBFI-like counterparties implement effective monitoring and reporting systems on these clients from origination, including the proper identification of NFBI/NBFI-like clients, ongoing due diligence to ensure that NBFI/NBFI-like clients have sufficient shock-absorbing capacity and specific risk-based policies, procedures and controls.

12. Explicit assessment of the CCR framework by 3LoD, i.e. internal audit

Independent reviews and internal audits take place regularly to ensure the integrity, accuracy and effectiveness of the overall CCR management system. Such reviews and audits are conducted by internal auditors or independent external parties with adequate knowledge of CCR. While ad hoc investigations on specific aspects might become necessary from time to time, holistic coverage of CCR is ensured on a regular basis. When coverage is achieved through various reviews, the internal audit

function is able to demonstrate that there are no gaps in the independent review of the institution's overall CCR management system.

3.3 Results of the assessment of CCR governance

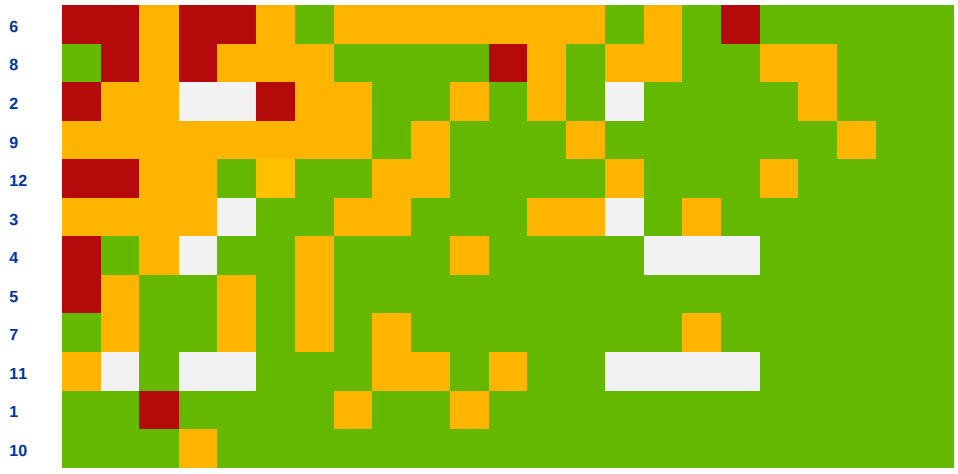
Based on the size and complexity of their derivatives and SFT portfolio, about two-thirds of the banks in the sample are broadly aligned with sound practices.

Chart 4 provides a more detailed picture for the different sound practices in this area. Topics such as the implementation of a three lines of defence model, the dedicated coverage of CCR in relevant committees or the assessment of CCR in new product approval processes do not appear to be problematic. However, improvements are needed in reporting to senior management and in the inclusion of CCR in the credit risk assessment. The identification and monitoring of NBFI/NBFI-like clients also warrants more attention in some cases.

Chart 4

CCR governance: overview of observed deviations from sound practices per bank and practice

(red = significant room for improvement, amber = moderate room for improvement, green = aligned with sound practice)



Source: Assessment as performed by the targeted review central team based on the information provided by the institutions.
Notes: See Table 3 for the numbering of practices.
Ranking follows the two dimensions of practice and bank: sound practices (rows) are sorted in the chart on the basis of the extent to which banks (columns) were observed to deviate from them in the targeted review. The highest degree of deviation is shown in the top left corner.

4 Risk control, management and measurement

The risk appetite framework (RAF) – together with governance, risk culture and risk management and control functions – forms the foundation for the prudent management of credit institutions. The risk appetite statement (RAS), the cornerstone of the RAF, outlines all levels and types of risk that the institution is willing to accept, within its risk capacity, to achieve its strategic objectives and implement its business plans.

CCR is a complex blend of credit and market risks. Consequently, the challenge for institutions lies in the development of tools to capture and combine all facets of the risk in a comprehensive, consistent view that enables effective risk monitoring and risk management, at the aggregated level as well as at the individual counterparty level.

According to Article 286(1) and (2) CRR, institutions should have a CCR management framework consisting of (a) policies, processes and systems to ensure the identification, measurement, management, approval and internal reporting of CCR; and (b) procedures for ensuring that those policies, processes and systems are complied with.

As put forward by the BCBS in 1999,[14] a credit risk strategy should define the bank's risk appetite, its desired risk return trade-off and mix of products and markets. In this context, an effective CCR management process should include appropriate documentation, the use of risk mitigants such as collateral and covenants, methodologies for measuring current and future exposure, effective limit-setting procedures, and ongoing monitoring of both the institution's exposure and the changing risk profile of the counterparty.

4.1 Range of practices for risk control, management and measurement

The ECB observed that only some institutions have explicit CCR management policies or adapt their wider credit risk management policies to the context of CCR. This means that several institutions have no documented policy listing the sources of CCR and setting out their related control processes.

All institutions have credit risk policies specifying general principles for risk acceptance. More sophisticated institutions set up dedicated policies based on product and type of counterparty, for example, with dedicated risk control processes for riskier clients, in particular hedge funds, and for prime brokerage businesses. The

[14] See "Sound Practices for Banks' Interactions with Highly Leveraged Institutions", Basel Committee on Banking Supervision, January 1999.

level of detail of the risk appetite policies varies considerably. Client rating, maturity of transactions and minimum expectations for collateralisation are usually considered. Some institutions also include details on collateralisation terms, covenants and documentation to be provided by the client.

For most institutions, CCR is only implicitly considered under credit risk, although for some the relative materiality of CCR or the complexity of the CCR portfolio would justify a dedicated setting of the institution's risk appetite.

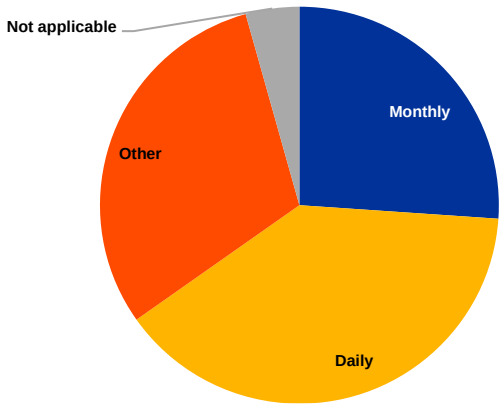
Few institutions explicitly mention CCR in their RAS. In those institutions, there is also a direct link between CCR limits, counterparty quality and terms of business because, according to their policies, counterparty-specific limits are based not only on product type and client rating, but also on terms of business (e.g. collateralisation, covenants, disclosure of information, etc.).

Most institutions leverage credit risk metrics (e.g. credit value-at-risk, RWEA, or exposure per country or segment) to measure CCR at group and/or entity level and below (e.g. business lines). Only a few set global limits with other metrics such as exposure values, exposures subject to general wrong-way risk (GWWR) or specific wrong-way risk (SWWR), etc. It was noted during the review, however, that some institutions were working on introducing more CCR-specific risk-sensitive measures. In all institutions, limits on CCR, either explicit or within overall credit risk, both at portfolio and at counterparty level, are set by the independent risk function (2LoD) following a scheme of delegation. In a few banks, the 1LoD is involved in the process and suggests limits for further validation and approval by the 2LoD.

Generally, counterparty-specific limits (both CCR-specific and wider credit risk limits including CCR) are monitored daily, in most cases by specific teams (usually as part of credit risk management). Higher-level limits, such as breakdowns by different geographies and/or business lines, and/or counterparty types/sector (i.e. at portfolio level) are monitored more frequently, ranging from monthly to weekly/daily. Limits that are part of the RAF at management body level are generally monitored monthly (occasionally quarterly or weekly) as shown in Chart 5.

Chart 5

Frequency of monitoring of limit utilisation for CCR limits



Source: Questionnaire submitted by banks in the sample.

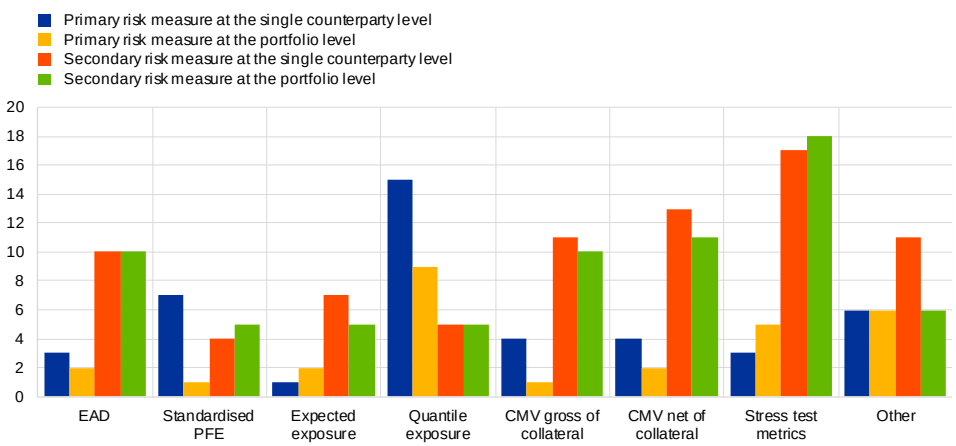
Material limit breaches are usually escalated to management daily and an overview of general limit utilisation and breaches is reported to senior management or committees on a monthly basis. Most institutions monitor portfolio-wide limits monthly while some do so weekly.

Chart 6 provides an overview of the primary and secondary metrics that the institutions in the sample deploy to manage CCR at counterparty or portfolio level. Primary risk measures are normally used to set formal limits for the business lines, whereas secondary measures are of an informative nature. In other words, they represent additional monitoring tools that do not imply mandatory triggers for escalation but are used to support expert judgement. A few institutions were found not to apply any CCR risk metrics as a primary risk measure at portfolio level.

Chart 6

CCR metrics as a primary and secondary risk measure

(number of institutions deploying the respective metric as a primary/secondary risk measure)



Source: Based on summary of information provided by the institutions.
Notes: CMV stands for current market value.

Generally, the risks of concentration and illiquidity of collateral (SFT underlying and margin collateral) are addressed using specific eligibility criteria for accepted collateral, concentration limits and concentration add-ons. Some IMM institutions concluded that the margin period of risk (MPOR) extension required by CRR is sufficient to account for illiquid collateral.

Few institutions address the concentration of transactions in counterparties, although many of them have some monitoring in place. For hard-to-replace transactions, institutions usually apply the MPOR extension – which is prescribed by the CRR for both the IMM and the standardised approach for measuring CCR (SA-CCR) – while some will try to avoid such transactions through restrictive internal policies. It is worth noting that not all of the institutions that apply only SA-CCR identify hard-to-replace transactions and extend MPOR accordingly. Although the portfolios of SA-CCR banks are in most cases less complex than those of IMM banks, implementing this aspect of the CRR might deserve more careful consideration by institutions, or at least documenting processes to identify potential cases requiring MPOR extensions.

Finally, although half the institutions in the sample claimed to have a specific measure in place to calculate the economic costs of winding down a portfolio, a number of these simply apply Pillar 1 MPOR extensions, which is not necessarily an adequate risk-sensitive tool from an economic perspective. The few institutions that calculate the economic costs of a portfolio wind-down generally leverage their xVA models (e.g. additional valuation adjustment (AVA) calculations) or assess bid/ask spreads for each position.

4.2 Sound practices for risk control, management and measurement

With regard to CCR management, control and measurement, the ECB has identified the following sound practices:

13. Identification of CCR sources and assessment of materiality

Institutions identify and assess the materiality of CCR and its sources. This includes a 2LoD review of the aggregated portfolio-wide and counterparty-specific exposure to CCR. Particular attention is paid to high-risk counterparties whose default may be strongly driven by their portfolio's performance.

14. CCR framework commensurate with CCR risk profile

The risk management framework is aligned with the CCR risk profile and ensures that high-risk counterparties and products are adequately considered.

15. Adequate recognition of CCR in the RAS

Institutions with material or complex CCR exposures explicitly specify their willingness to accept this risk in their RAS, rather than capturing it implicitly in credit risk. In setting risk appetite and limits, additional complexities of CCR with respect to general credit risk, such as illiquid collateral and hard-to-replace transactions or exposure volatility triggered by market stress events, are considered.

16. Policies addressing risk acceptance for CCR as an integral part of the RAF

Institutions implement risk policies explicitly reflecting their willingness to accept CCR resulting from derivatives and SFTs or other market activities with a long settlement. These risk policies are an integral part of the RAF and are commensurate with the business model, product offer, types of counterparty and with the materiality of CCR exposure. The 2LoD is the owner of these policies by virtue of delegation of authority by the management body, which is ultimately responsible for them.

As a minimum, these policies provide qualitative guidance on which combinations of counterparty quality, transaction types and terms of business (in particular, collateralisation and covenants) are acceptable. Institutions with material CCR have

grids combining terms of business with counterparty quality for major product categories.

17. Adequate limit framework for CCR

Risk appetite limits set the level and types of risk that the institution is willing to accept, within its risk capacity. Risk measures used as a reference for limit definition set by the 2LoD appropriately reflect the future variability of the counterparty's portfolio value, also with respect to the most complex derivatives.

18. Appropriate choice of CCR metrics

Institutions deploy various metrics reflecting the specificities of CCR commensurate with their internal risk management processes and procedures instead of relying only on a single measure of CCR. These metrics enable management to understand the current exposure, e.g. through the current market value of the netting set, and potential future exposures based on, for example, future netting set values from a quantile metric or stress exposure values.

CCR is assessed both at portfolio and individual counterparty level. Institutions are always able to assess the gross exposure of netting sets, i.e. disregarding the margin collateral, with individual counterparties.

19. Effective monitoring of counterparty concentrations to margin shocks

Institutions have measures in place allowing for an effective monitoring of counterparty concentrations to margin shocks. These measures serve to proactively interact with potentially affected clients and agree with them on additional risk mitigating steps to be taken if a margin shock occurs. Such steps can comprise margin covenants, letters of credit or additional liquidity facilities.

20. Adequate identification and monitoring of illiquid and concentrated positions

Institutions identify and monitor illiquidity and concentration at least at portfolio level, for both transactions and collateral, and reflect the impact of such positions adequately in economic risk measures.

21. Appropriate economic measure for costs of CCR portfolio wind-down

For risk management purposes, institutions go beyond the sole application of the regulatory MPOR and deploy complementary economic measures for the costs of winding down portfolios with high-risk counterparties or netting sets comprising less liquid collateral or hard-to-replace transactions.

When deploying such economic measures, due consideration is paid to the effects of a netting set wind-down on hedging positions with other counterparties, and to potential additional market risk losses from the unmatched hedging positions.

4.3 Results of the assessment of risk control, management and measurement

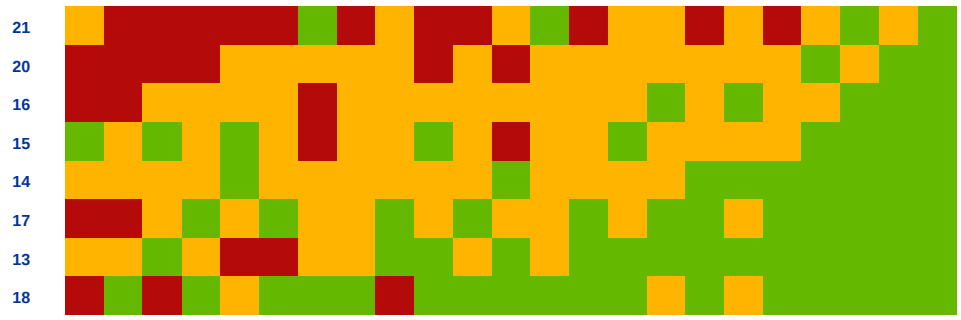
Based on the size and complexity of the institution's CCR portfolios, there is overall less convergence with observed sound practices in the area of risk control, management and measurement and therefore more room for improvement than for CCR governance, as discussed in the previous chapter.

Chart 7 provides a more granular picture of the different sound practices in this area. Alignment with sound practices is generally satisfactory for topics such as the identification of CCR sources, assessment of materiality and choice of CCR metrics. However, some institutions should improve their identification and monitoring of illiquid and concentrated positions and develop appropriate economic measures for the costs of CCR portfolio wind-downs. In addition, policies addressing risk acceptance for CCR as an integral part of RAF would benefit from enhancements in a number of institutions.

Chart 7

Risk control, management and measurement: overview of observed deviations from sound practices per bank and practice

(red = significant room for improvement, amber = moderate room for improvement, green = aligned with sound practice)



Source: Assessment as performed by the targeted review central team.
Notes: See Table 3 for the numbering of practices.
Ranking follows the two dimensions of practice and bank: sound practices (rows) are sorted in the chart on the basis of the extent to which banks (columns) were observed to deviate from them in the targeted review. The highest degree of deviation is shown in the top left corner.

5 Stress testing and WWR

As CCR is a blend of credit and market risks, one of the main challenges for institutions is to establish comprehensive stress testing programmes. The BCBS[15] has emphasised that meaningful tools to manage counterparty credit risk exposures incorporate an assessment of the impact of volatile market conditions through the development and implementation of timely and plausible stress tests for CCR exposures.

According to Article 290 CRR, an institution must have a comprehensive stress testing programme in place to identify possible events or future changes in economic conditions that could have unfavourable effects on its CCR exposures and assess its ability to withstand such changes. The stress measures in the programme must be compared with risk limits. The programme must also include reverse stress tests to identify extreme, but plausible, scenarios that could result in significant adverse outcomes. Senior management must take a leading role in the integration of stress testing into the risk management framework and risk culture of the institution.

Stress testing is also inextricably linked to the WWR frameworks of institutions, as WWR arises when counterparty default and exposure are both subject to the same adverse market developments. While GWWR refers to the correlation between the likelihood of default of counterparties and general market risk factors, SWWR refers to the correlation between exposure to a specific counterparty and the counterparty's probability of default.

Article 291 CRR provides the definition and the requirements for both components, and Chapter 7 of the EGAM provides insights into the ECB's approach to assessing these CRR requirements. While the CRR requirements for GWWR apply directly only to IMM institutions, SWWR requirements apply to all institutions regardless of the method used to compute their CCR exposure (see Article 273(9) CRR).

According to the CRR, institutions must have processes in place to identify, monitor, control and report WWR regularly. Stress testing and scenario analyses are reasonable instruments for identifying GWWR and monitoring this risk by product, region or any other relevant category.

For SWWR, an institution must carry out identification and monitoring for each legal entity, and throughout the life of the transaction. It should be noted that in cases where SWWR is identified and there is a legal connection between the counterparty and the issuer of the underlying of the transaction, Article 291(5) CRR prescribes the specific treatment of these transactions for the calculation of own funds requirements (i.e. the use of a separate netting set and calculation of the jump-to-default exposure).

---

15 See "Sound Practices for Banks' Interactions with Highly Leveraged Institutions", Basel Committee on Banking Supervision, January 1999.

5.1 Range of practices for stress testing and WWR

Not all institutions seem to have clear governance to ensure that their choice and design of stress scenarios are discussed and reviewed regularly.

Nevertheless, most institutions in the sample conduct regular stress testing that implicitly or explicitly captures CCR with a comprehensive set of stress tests at the portfolio and counterparty level. All banks apply at least historical scenarios (such as a financial crisis), and most of them apply scenarios with different severities and narratives. Moreover, ad hoc scenarios are frequently used to cover crises (e.g. COVID-19, Russia's war in Ukraine, etc.). While the use of stress tests based on macroeconomic scenarios is widely observed, only around half the institutions also regularly deploy risk factor-specific stress tests to identify vulnerabilities of their CCR portfolio to shocks on individual market risk factors or common combinations of risk factor shocks that are independent of historical or other macroeconomic scenarios.

Although several institutions have adequate capabilities in their stress testing infrastructure to identify clients that are vulnerable to exposure tail events or margin shocks, few of them assess their stress testing results explicitly for this purpose and none use this information as a mandatory indicator for action. Instead, institutions rely to a large extent on the knowledge of their relationship managers to identify vulnerable clients in acute market stress events. Exposure models can be an additional tool for identifying potential exposure tail events and/or clients vulnerable to such events, provided that a mechanistic calibration is avoided and that hypothetical scenarios are also considered.

To calculate economic capital in the ICAAP, most institutions in the sample use a credit portfolio model in which CCR is represented only partially and implicitly, as part of the overall credit risk. Inconsistencies in implementation are often noted when institutions apply their ICAAP stress tests to the input parameters of the credit portfolio model. While nearly all institutions apply stressed probabilities of default (PDs) and stressed losses given default (LGDs) according to their stress scenarios, only some of them also derive stressed CCR exposure metrics from these scenarios, despite market risk factors being affected. The few institutions with consistent stress testing under the ICAAP also generally assume a correlation between creditworthiness and CCR exposures in the credit portfolio model, while other institutions assume these to be uncorrelated. A consistent application of stress test scenarios to all metrics affected by changes in the relevant market parameters results in a more comprehensive understanding of the impacts of those scenarios on the institution.

The most sophisticated institutions have well-documented and comprehensive policies addressing both GWWR and SWWR. These include the identification, measurement, monitoring and control of those risks, with clear responsibilities across the three lines of defence. For some banks, limit definition and escalation for both GWWR and SWWR are explicit and included in the institution's RAF, with monthly reporting to senior management. In some instances, risk add-ons are applied in the case of GWWR for internal risk management purposes.

GWWR analyses are performed at different levels of granularity – by business area and product, sector/industry and region/country.

SWWR is usually considered in the calculation of the exposure when legal connections exist between the counterparty and the underlying of the transaction. However, it was also observed that some banks might be failing to comply with Article 291(5) CRR when calculating their exposures under the SA-CCR by leaving the respective transactions in their original netting set and/or calculating the exposure following SA-CCR instead of the jump-to-default metric. At the other side of the scale, there are also a few institutions that go beyond CRR requirements and identify and measure SWWR in cases where no legal connection is present, based on strong economic dependencies between the counterparty and the issuer of the underlying.

For less sophisticated institutions, there is a wide range of practices for the formalisation of procedures, the granularity of analyses or factors included in the methodology for identifying WWR exposures, and the (lack of) integration in the limit system and the RAF. Moreover, in some cases the scope of transactions captured by the GWWR/SWWR analyses appears to be too limited.

Finally, only a handful of institutions have additional measures or methods in place to identify and/or treat WWR for clients with a business strategy that is particularly vulnerable to certain market risk scenarios (e.g. hedge funds or clients with comparable business strategies).

In summary, although most institutions have a set of CCR management tools in place, many of them lack a holistic view and do not use stress testing and WWR analysis results for CCR management purposes. Less sophisticated institutions lack essential tools such as counterparty and portfolio-specific exposure stress tests or a concise view of GWWR.

5.2 Sound practices for stress testing and WWR

The ECB has identified the following as sound practices for stress testing and the identification and monitoring of WWR:

22. Documented governance for stress testing framework

Institutions have a clear, documented governance of their stress testing framework in place, including stress testing for CCR, to ensure the appropriate identification of relevant scenarios, their design and revision. In addition, institutions have the capabilities to perform ad hoc stress tests on new or amended scenarios, if needed.

23. Explicit consideration of the CCR component in stress testing

Institutions have stress testing frameworks in place, explicitly considering CCR in a manner commensurate with the materiality and complexity of the portfolio. Such stress testing frameworks pay particular attention to riskier counterparties as well as the identification of counterparties for which certain market scenarios could lead to

acute stress on their solvency or liquidity position and, therefore, are particularly vulnerable to exposure tail events.

24. Comprehensive set of CCR-relevant stress scenarios

A comprehensive set of severe but plausible stress tests is performed at portfolio and counterparty level applying different macroeconomic scenarios and dedicated sets of risk factor stress testing. The results of these stress tests enable the institution's risk management function to (i) identify the most relevant scenarios for the overall institution's CCR portfolio, (ii) identify particularly vulnerable counterparties under certain scenarios, and (iii) report the conclusions to senior management.

25. Use of stress testing framework for the identification and monitoring of increasing risks for high-risk clients

Commensurate with the materiality and complexity of the CCR portfolio, institutions apply their stress testing framework to identify and monitor potential increases in risk for those counterparties whose performance is particularly vulnerable to exposure tail events, for instance because their solvency or liquidity is affected by stress events that impact their portfolio quality.

26. Explicit stress testing of CCR exposures in the ICAAP to identify clients vulnerable to tail risk events

For ICAAP purposes, the calculation of economic capital and stress testing of CCR exposures (together with PDs and LGDs) – for example in a credit portfolio model – is an observed sound practice for material or complex CCR portfolios. Such an approach is also considered to identify clients whose performance might be impacted directly by portfolio tail events rather than by the deterioration of their own creditworthiness, which might take place only as a consequence of the tail event.

27. Adequate WWR framework included in the RAF

Institutions have a dedicated WWR framework in place that is integrated into the RAF, giving due consideration to both GWWR and SWWR. This framework is commensurate with CCR risk appetite and explicitly accounts for relevant risk factors, going beyond mere compliance with regulatory requirements when required by the size and complexity of the business. The WWR framework is designed to effectively allow the identification, measurement, monitoring, regular reporting, limit setting and explicit treatment of exposures giving rise to WWR.

28. Identification and monitoring of GWWR with well-defined models and data

To identify and monitor GWWR, institutions have clear definitions in place in terms of the risk categories relevant to their business. The regular GWWR identification process is supported by well-defined stress testing and scenario analysis of credible severity that are reported to senior management with an appropriate frequency. The application of GWWR limits supports institutions' risk management.

29. Identification of GWWR under specific market stress events

The process and methodologies for the identification of GWWR allow the institutions' risk management function to also identify counterparties where GWWR might occur only under specific market stress events given the nature of the counterparty's business or portfolio profile. This might be the result of the vulnerability of the counterparty's business to particular stress events or to the concentration of the counterparty's portfolio in certain products or markets that tend to be less liquid in stressed conditions. In this context, institutions consider a more prudent approach for less transparent counterparties, linking the GWWR methodology to the customer due diligence process.

The GWWR analyses should include an assessment of potential WWR at industry and regional level, as appropriate.

30. Sound SWWR assessment and monitoring

Institutions' processes and methodologies for SWWR assessment and monitoring are well-defined and documented. They are suitable for identifying the correlation between the counterparty's creditworthiness and the CCR exposure to the counterparty. The SWWR methodology is deployed on a clear definition of legal connection that considers legal frameworks on ownership, including control or consolidation requirements. The results of the regular SWWR identification are reported with adequate frequency and followed up.

31. SWWR identification without legal connection

Institutions consider the identification of SWWR for risk management purposes also for cases with no strict legal connection but where there is a strong economic dependency between the counterparty and the issuer of the derivative's underlying.

5.3 Results of the assessment of stress testing and WWR

With regard to stress testing and WWR, the overall outcome of the assessment suggests there is considerable room for improvement.

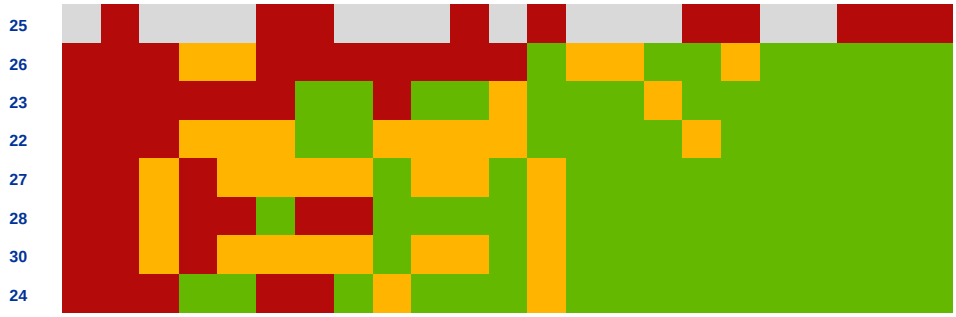
Chart 8 shows that while most institutions have adequately documented governance for their stress testing framework, there is considerable room for improvement in the stress testing of CCR exposures in the ICAAP to identify clients that are vulnerable to tail risk events. The same holds true for the use of the stress testing framework to identify and monitor high-risk clients.

Furthermore, although the review identified significant shortcomings in the WWR framework in only a few institutions, for such institutions weaknesses were observed in most aspects of the framework, which therefore needs a substantial overhaul.

Chart 8

Stress testing and WWR: overview of observed deviations from sound practices per bank and practice

(red = significant room for improvement, amber = moderate room for improvement, green = aligned with sound practice)



Source: Assessment as performed by the targeted review central team.
Notes: See Table 3 for the numbering of practices. For sound practice #25 included in chart above, related information and horizontal assessment were possible only for institutions that had a meeting during the targeted review. JSTs are gathering information from the other institutions as part of the follow-up activities. Sound practices #29 and #31 were excluded as no horizontal assessment was performed for the institutions in the sample.
Ranking follows the two dimensions of practice and bank: sound practices (rows) are sorted in the chart on the basis of the extent to which banks (columns) were observed to deviate from them in the targeted review. The highest degree of deviation is shown in the top left corner.

6 Watchlist and default management processes

This section describes sound practices for the identification, monitoring and management of watchlist and default management.

Although the monitoring and management of counterparties in distressed conditions or in default are not subject to specific supervisory requirements, the general requirements and expectations based on Articles 74(1), 79c and 286 CRR, on risk management related to the creditworthiness of counterparties, apply.

This implies that the risk management framework for CCR, including watchlist processes and reporting, should be consistent with the size and complexity of the institution's operations and risk profile and be comprehensive enough to facilitate informed decision-making. In addition, the existence of a clear and well-defined DMP complemented by the early identification of distressed counterparties (referred to as the "watchlist") are integral parts of the sound and effective risk management of CCR. Therefore, procedures and policies are widely developed and used by the banking industry to anticipate, organise and limit any potential losses from counterparties in difficulties.

A robust governance framework entails the clear definition of roles and responsibilities for the (operational, risk management and legal) units involved and includes effective processes to establish the courses of action and the circulation of appropriate information to allow timely risk-reduction actions to be executed.

The industry[16] has recommended that market participants promptly and periodically review their existing documentation covering counterparty terminations and ensure that they have appropriate, current agreements in place, including the definition of default events and the termination methodology that will be used. With regard to the execution of the DMP, the CRMPG III recommends that market participants periodically conduct hypothetical simulations of close-out situations (also called fire drills) to verify the speed and accuracy with which comprehensive counterparty exposure data and net cash outflows can be compiled. Fire drills also allow for the testing and sequencing of critical tasks and promote decision-making responsibilities associated with events leading up to the execution of a close-out event.

6.1 Range of practices for watchlist and default management processes

With regard to the definition of watchlists for clients experiencing a deteriorating risk profile, most institutions have a well-defined process for including or excluding clients from their watchlist, with clear roles and responsibilities. However, only about half the

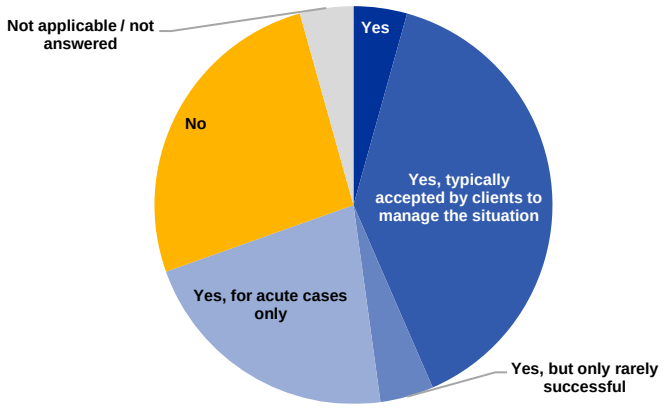
[16] See "CRMPG III, Containing systemic risk: the road to reform", 6 August 2008.

institutions have comprehensive watchlists, with early warning indicators specific to CCR. For the other institutions, the watchlist process applies only to specific client groups or to clients already known to be experiencing difficulties, the watchlist criteria relate to general credit risk only or the watchlist contains too few criteria for appropriate risk differentiation.

Chart 9, however, shows that around half the institutions negotiate additional risk-mitigating measures with clients on their watchlist, which are often accepted by clients to manage the situation. The other institutions affirm that additional risk-mitigating measures are negotiated only in the most serious cases.

Chart 9

Negotiation of additional risk-mitigating measures for the CCR portfolio as part of the regular watchlist process

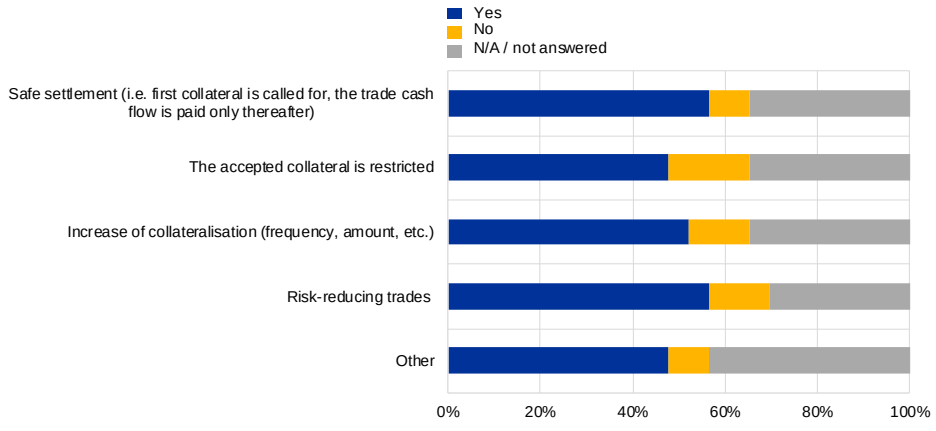


Source: Questionnaire submitted by banks in the sample.

These risk-mitigating measures mostly include safe settlement procedures, followed by risk-reducing trades and increased collateralisation/restriction of acceptable collateral (Chart 10).

Chart 10

Risk-mitigating measures usually negotiated as part of the regular watchlist process for the CCR portfolio



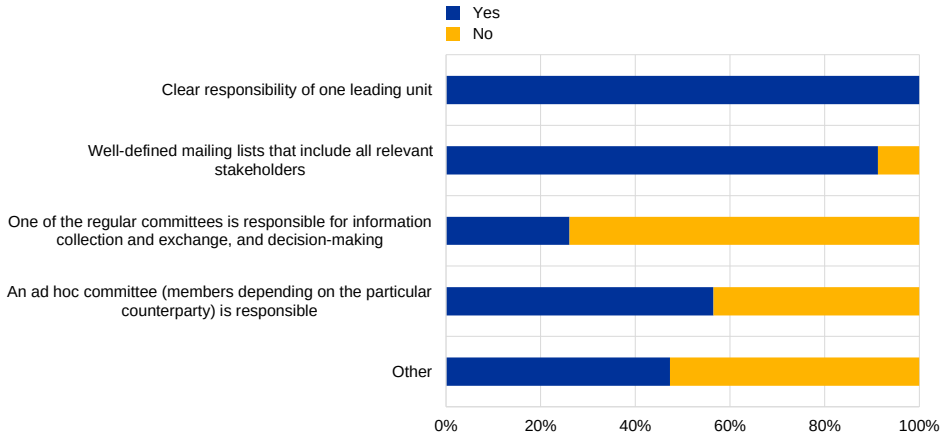
Source: Questionnaire submitted by banks in the sample.

Other measures may be negotiated or imposed on a case-by-case basis (e.g. request for additional guarantees or letters of credit, measures considered in the context of overall client exposure, or forms of business termination).

Most institutions have dedicated default management policies and procedures in place. These policies are usually covered by the internal governance framework, with a clearly defined ownership. Roles, responsibilities and escalation procedures are clearly described in the policies, which sometimes contain specific distribution lists.

Chart 11

Tools ensuring effective and efficient information-sharing and decision-making in the DMP



Source: Questionnaire submitted by banks in the sample.

If the process allows for discretionary steps, there is a clear allocation of responsibilities for decision-making.

Most banks evaluate the practical effectiveness of the DMP by means of regular fire drills, for example. These are usually performed at least every two years, sometimes even annually. Very few banks do not perform any testing of their internal procedures or limit these tests to exposures to CCPs or participation in CCP fire drills.

Only a few institutions do not have a clear policy in place governing the DMP or rely on policies that cover general credit risk elements and do not consider the particularities of CCR. For some institutions, elements of the DMP are scattered across different documents or are contained in internal checklists that have never been approved by management. For those institutions, the governance of the policy is usually not clear either and internal procedures are not tested.

Most institutions have sufficient close-out capabilities to execute the termination of their most complex client portfolios. However, some institutions would have to rely on external capabilities, e.g. external brokers or market-makers. This is also relevant for some SSM banking subsidiaries which rely on the resources and trading capabilities of their group.

6.2 Sound practices for watchlist and default management processes

The ECB has identified the following sound practices for watchlist and default management processes:

32. Documented watchlist policy

The process for including or excluding counterparties in or from a watchlist is documented in a policy or procedure (standalone or as part of the DMP policy). The process description includes:

- governance, reporting lines and clear responsibilities for updating the watchlist;
- a list of mandatory or optional indicators supporting the inclusion and exclusion of counterparties in or from the watchlist;
- a definition of the minimum reassessment period for each indicator;
- a clear reporting line to committees and/or senior management responsible in the event of amendments to the watchlist indicators;
- a description of the link between different watchlist levels and required regulatory/accounting treatment of positions (IFRS 9, stages for expected credit loss (ECL), credit valuation adjustments (CVA), formal default status).

33. Definition of relevant watchlist indicators including CCR

Watchlist definitions include sufficient quantitative and qualitative indicators, relevant for the specificities of derivatives and SFT counterparties. To sufficiently consider the specificities of capital market activities, these indicators include, as a minimum, compliance with contractual covenants (as agreed in netting agreements) and collateral payment discipline.

34. Defined actions based on watchlist classification

Institutions enumerate mandatory and optional risk-mitigating measures applied to clients that are moved into a higher alert watchlist category.

35. A posteriori review of watchlist performance

Institutions periodically assess the effectiveness and discriminatory power of the watchlist process by analysing a posteriori the cases of counterparties that have entered or exited the watchlist, as well as the actions taken or not taken for new entries.

36. Clear ownership of DMP policy

Institutions have a documented policy for their DMP summarising the actions to be taken to decide on and manage a close-out of derivatives and SFT positions if a counterparty default event occurs. This DMP policy is subject to robust governance,

with clearly defined ownership. The institution's senior management grants the initial approval of the DMP policy.

37. DMP policy implementing governance of default management

The DMP policy complements the framework in place for the management of counterparties classified in default according to the prudential regulatory framework.

The policy covers at a minimum:

- regular and ad hoc organisational structures (e.g. committees, teams) organising and executing close-out and restructuring cases;
- preparatory steps ahead of a potential default event (including reference to a watchlist process, ongoing and ad hoc required analyses, fire drills, etc.);
- description of proactive actions that should be considered;
- mandatory and optional process steps once a default event occurs;
- steps to ensure accurate data aggregation in a timely manner.

38. Description of a binding process and identification of clear responsibilities

The DMP policy describes a binding process with clearly defined responsibilities for each of the process steps (including decision-making) during the close-out of a derivatives or SFT portfolio. As a complement to the DMP policy, there is a clear information distribution list supporting the DMP to enable quick and coordinated action.

The DMP policy sets out the responsibilities of the legal department to safeguard the DMP from legal risks (e.g. clarifying the use of non-public material information during the DMP). Senior legal experts are involved in all cases of counterparty default.

If the DMP includes discretionary elements, mandates and escalations are clearly described in the DMP policy.

39. Integration of risk management functions in DMP decision-making

If the close-out of a position after a default event has occurred is an option for the institution, the risk management functions are involved in the decision-making process, especially when a close-out is delayed, since these decisions might have an impact on the future evolution of the underlying CCR exposure.

40. Procedures conducive to effective information flows and default management

Default management procedures covering CCR are in place to ensure the timely identification of default events and expedite close-out decisions. Since several circumstances can trigger the occurrence of a default event, the centralisation of information flows is conducive to prompt identification of defaults and timely close-

out decisions. Such procedures are supported by adequate availability of the relevant data at the required granularity.

41. Post-default process ensuring minimal losses and legal risks

Once a decision has been made to execute a close-out, default management procedures are put in place with the objective of maximising recoveries and minimising losses. Procedures reflecting the specificities of CCR ensure that (i) limits are revised to prevent any new business with a defaulting party, (ii) no undue payment is made to a defaulting counterparty, and (iii) legal risks in the execution of the close-out and the liquidation of the collateral are minimised.

42. For market-makers, assessment of (local) close-out capabilities

Market-makers in derivatives and SFTs regularly assess their own capabilities to close out positions, both under business-as-usual and in stressed markets, to ensure their ongoing ability to close out large hedging and collateral instruments. Safeguards and monitoring are set up for illiquid positions in the portfolio or in the collateral pool. The definition of collateral eligibility criteria allows for collateral to be liquidated promptly. Senior management ensures that a regular verification of the institution's access to markets with sufficient depth allows the most concentrated positions in the portfolio to be closed out in a timely manner.

43. Regular fire drills for the DMP

Institutions regularly validate the performance of the DMP by executing end-to-end fire drills at least once a year. These mock-up tests include all relevant staff involved in the close-out of different counterparties, including counterparties with complex portfolios covering several asset classes and/or business lines, or counterparties with specific risk profiles.

6.3 Results of the assessment of watchlist and default management processes

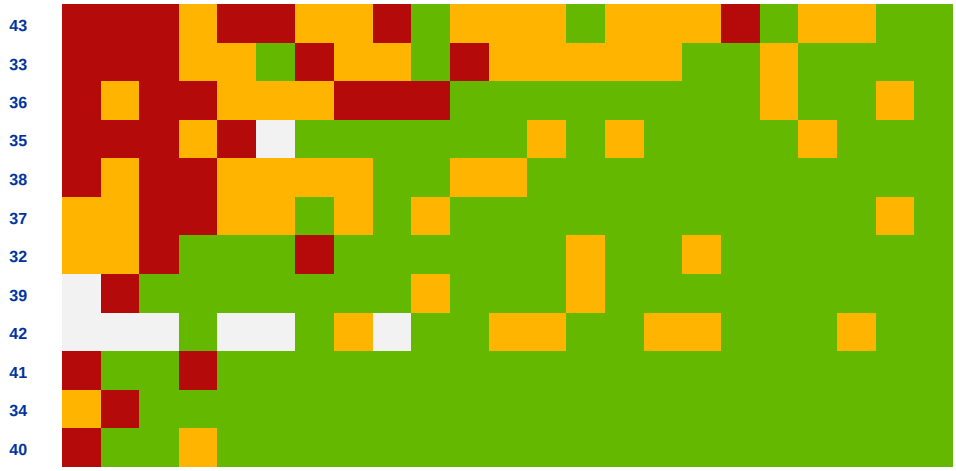
The overall outcome of the assessment is satisfactory for roughly two-thirds of the institutions, which is similar to the overall results for the CCR governance area.

Chart 12 shows that institutions are broadly aligned with sound practices for information flows and the DMP. Some room for improvement was identified regarding the review of watchlist performance and the documentation of DMP policy. More efforts to align with sound practices are necessary when it comes to the definition of watchlist indicators for CCR and the testing of the DMP in the form of regular fire drills.

Chart 12

Watchlist and default management processes: overview of observed deviations from sound practices per bank and practice

(red = significant room for improvement, amber = moderate room for improvement, green = aligned with sound practice)



Source: Assessment as performed by the targeted review central team.
Notes: See Table 3 for the numbering of practices.
Ranking follows the two dimensions of practice and bank: sound practices (rows) are sorted in the chart on the basis of the extent to which banks (columns) were observed to deviate from them in the targeted review. The highest degree of deviation is shown in the top left corner.

Annex

List of abbreviations

Abbreviation	Description
AIG	American International Group
ALM	Asset and liability management
AVA	Additional valuation adjustment
BCBS	Basel Committee on Banking Supervision
CCP	Central counterparty
CCR	Counterparty credit risk
CET1	Common Equity Tier 1
CRD	Capital Requirements Directive (2013/36/EU)
CRMPG	Counterparty Risk Management Policy Group
CRR	Capital Requirements Regulation (2013/575/EU)
CVA	Credit valuation adjustment
DMP	Default management process
EAD	Exposure at default
EBA	European Banking Authority
ECB	European Central Bank
ECL	Expected credit loss
EEPE	Effective expected positive exposure
EGAM	ECB Guide on assessment methodology
EMIR	European Market Infrastructure Regulation
FSB	Financial Stability Board
FX	Foreign exchange
G-SIB	Global systematically important bank
GWWR	General wrong-way risk
ICAAP	Internal Capital Adequacy Assessment Process
IG	Investment grade
IMM	Internal model method
JST	Joint Supervisory Team
LGD	Loss given default
LoD	Line of defence
LTCM	Long-Term Capital Management
MPOR	Margin period of risk
NBFI	Non-bank financial intermediation
PBS	Prime brokerage services
PD	Probability of default
PFE	Potential future exposure
RAF	Risk appetite framework
RAS	Risk appetite statement
RWEA	Risk-weighted exposure amount
SA-CCR	Standardised approach for measuring CCR
SFT	Securities financing transaction
SREP	Supervisory Review and Evaluation Process
SSM	Single Supervisory Mechanism
SWWR	Specific wrong-way risk
WWR	Wrong-way risk

Postal address 60640 Frankfurt am Main, Germany
Telephone +49 69 1344 0
Website www.bankingsupervision.europa.eu

For specific terminology please refer to the SSM glossary (available in English only).