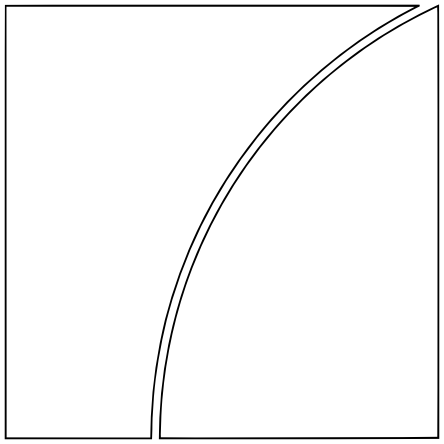
Basel Committee on Banking Supervision

SCO

Scope and definitions

This standard describes the scope of application of the Basel Framework.



BANK FOR INTERNATIONAL SETTLEMENTS

Contents

SCO10

Introduction

First version in the format of the consolidated framework.

Version effective as of 15 Dec 2019

First version in the format of the consolidated framework.

10.1 This framework will be applied on a consolidated basis to internationally active banks. Consolidated supervision is the best means to provide supervisors with a comprehensive view of risks and to reduce opportunities for regulatory arbitrage.

10.2 The scope of application of the framework will include, on a fully consolidated basis, any holding company that is the parent entity within a banking group to ensure that it captures the risk of the whole banking group.[1] Banking groups are groups that engage predominantly in banking activities and, in some countries, a banking group may be registered as a bank.
Footnotes

[1] *A holding company that is a parent of a banking group may itself have a parent holding company. In some structures, this parent holding company may not be subject to this framework because it is not considered a parent of a banking group.*

10.3 The framework will also apply to all internationally active banks at every tier within a banking group, also on a fully consolidated basis (see illustrative chart at the end of this section).[2]
Footnotes

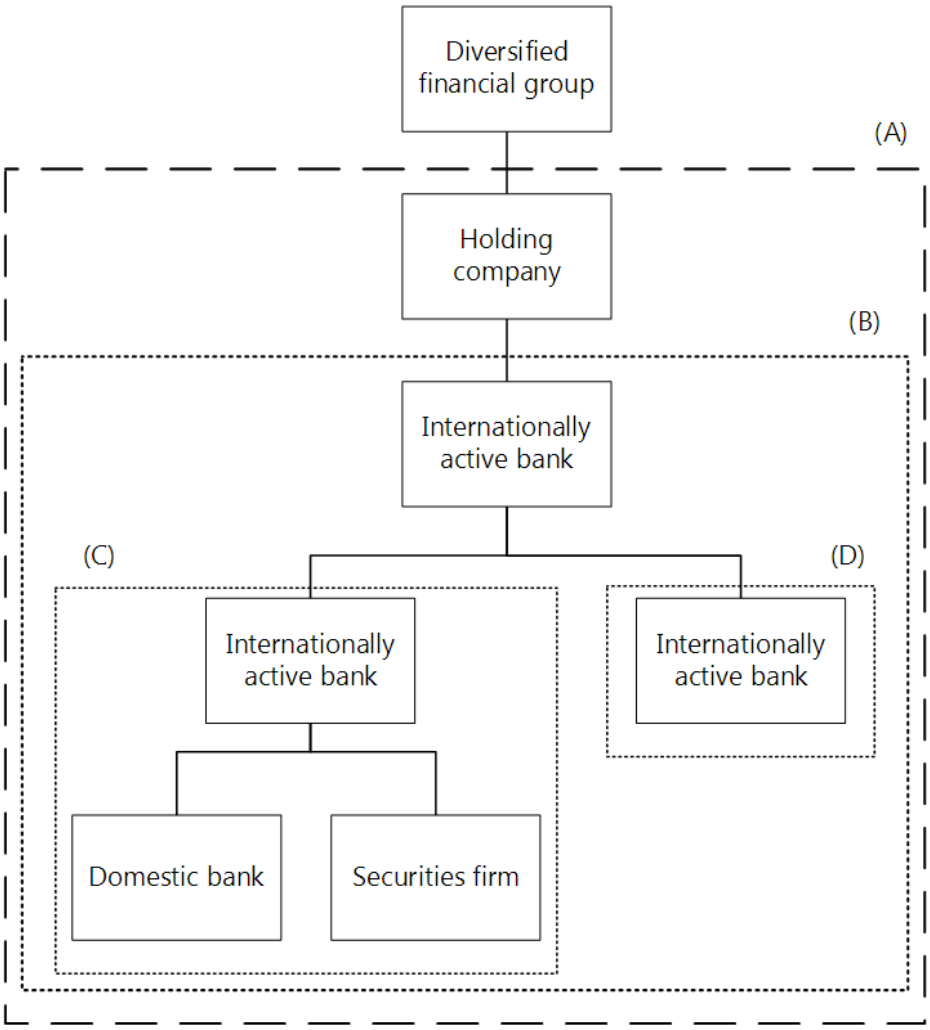
[2] *As an alternative to full sub-consolidation, the application of this framework to the stand-alone bank (ie on a basis that does not consolidate assets and liabilities of subsidiaries) would achieve the same objective, providing the full book value of any investments in subsidiaries and significant minority-owned stakes is deducted from the bank's capital.*

10.4 Further, to supplement consolidated supervision, it is essential to ensure that capital recognised in capital adequacy measures is adequately distributed amongst legal entities of a banking group. Accordingly, supervisors should test that individual banks are adequately capitalised on a stand-alone basis.
FAQ

FAQ1 *How should banks treat investments in banks, insurance companies and other financial institutions that are included in the consolidated group in computing the capital ratio for the stand-alone parent bank entity?*

The Basel framework is applied on a consolidated basis to internationally active banks. It captures the risks of a whole banking group. Although the framework recognises the need for adequate capitalisation on a stand-alone basis, it does not prescribe how to measure the solo capital requirements which is left to individual supervisory authorities.

10.5 The diagram below illustrates the scope of application of this framework, where (A) represents the boundary of the predominant banking group, to which the framework is to be applied on a consolidated basis (ie up to holding company level, as described in [SCO10.2]). With respect to (B), (C) and (D), the framework is also to be applied at lower levels to all internationally active banks on a consolidated basis.


Diversified financial group
(A)
Holding company
(B)
Internationally active bank
(C)
(D)
Internationally active bank
Internationally active bank
Domestic bank
Securities firm

SCO30

Banking, securities and other financial subsidiaries

First version in the format of the consolidated framework.

Version effective as of 15 Dec 2019

First version in the format of the consolidated framework.

Consolidation

30.1 To the greatest extent possible, all banking and other relevant financial activities[1] (both regulated and unregulated) conducted within a group containing an internationally active bank will be captured through consolidation. Thus, majority-owned or -controlled banking entities, securities entities (where subject to broadly similar regulation or where securities activities are deemed banking activities) and other financial entities[2] should generally be fully consolidated. The treatment of minority interests and other capital issued out of consolidated subsidiaries that is held by third parties is set out in [CAP10].

Footnotes

1 *"Financial activities" do not include insurance activities and "financial entities" do not include insurance entities.*

2 *Examples of the types of activities that financial entities might be involved in include financial leasing, issuing credit cards, portfolio management, investment advisory, custodial and safekeeping services and other similar activities that are ancillary to the business of banking.*

30.2 There may be instances where it is not feasible or desirable to consolidate certain securities or other regulated financial entities. This would be only in cases where such holdings are acquired through debt previously contracted and held on a temporary basis, are subject to different regulation, or where non-consolidation for regulatory capital purposes is otherwise required by law. In such cases, it is imperative for the bank supervisor to obtain sufficient information from supervisors responsible for such entities.

30.3 If any majority-owned securities and other financial subsidiaries are not consolidated for capital purposes, all equity and other regulatory capital (or, if applicable, other total loss-absorbing capacity) investments in those entities attributable to the group will be deducted (as described in [CAP30]), and the assets and liabilities, as well as third-party capital investments in the subsidiary will be removed from the bank's balance sheet. Supervisors will ensure that an entity that is not consolidated and for which the capital investment is deducted meets regulatory capital requirements. Supervisors will monitor actions taken by the subsidiary to correct any capital shortfall and, if it is not corrected in a timely manner, the shortfall will also be deducted from the parent bank's capital.

30.4 Significant minority investments in banking, securities and other financial entities, where control does not exist, will be excluded from the banking group's capital by deduction of the equity and other regulatory investments (as described in [CAP30]). Alternatively, such investments might be, under certain conditions, consolidated on a pro rata basis. For example, pro rata consolidation may be appropriate for joint ventures or where the supervisor is satisfied that the parent is legally or de facto expected to support the entity on a proportionate basis only and the other significant shareholders have the means and the willingness to proportionately support it. The threshold above which minority investments will be deemed significant and be thus either deducted or consolidated on a pro-rata basis is to be determined by national accounting and/or regulatory practices. As an example, the threshold for pro-rata inclusion in the European Union is defined as equity interests of between 20% and 50%.

Insurance entities

30.5 A bank that owns an insurance subsidiary bears the full entrepreneurial risks of the subsidiary and should recognise on a group-wide basis the risks included in the whole group. When measuring regulatory capital for banks, the Committee believes that it is, in

principle, appropriate to deduct banks' equity and other regulatory capital investments in insurance subsidiaries and also significant minority investments in insurance entities. Under this approach the bank would remove from its balance sheet assets and liabilities, as well as third party capital investments in an insurance subsidiary. The bank's equity or other capital investment in the insurance subsidiary is then treated according to [CAP30.21] to [CAP30.34]. Alternative approaches that can be applied should, in any case, include a group-wide perspective for determining capital adequacy and avoid double counting of capital. Banks should also disclose the national regulatory approach used with respect to insurance entities in determining their reported capital positions (see [DIS30]).

FAQ

FAQ1 *Can significant investments in insurance entities, including fully owned insurance subsidiaries, be consolidated for regulatory purposes as an alternative to the deduction treatment set out in [CAP30.28] to [CAP30.34]?*

Jurisdictions can permit or require banks to consolidate significant investments in insurance entities as an alternative to the deduction approach on the condition that the method of consolidation results in a minimum capital standard that is at least as conservative as that which would apply under the deduction approach, ie the consolidation method cannot result in banks benefiting from higher capital ratios than would apply under the deduction approach.

In order to ensure this outcome, banks that apply a consolidation approach are required to calculate their capital ratios under both the consolidation approach and the deduction approach, at each period that they report or disclose these ratios.

In cases when the consolidation approach results in lower capital ratios than the deduction approach (ie consolidation has a more conservative outcome than deduction), banks will report these lower ratios. In cases when the consolidation approach results in any of the bank's capital ratios being higher than the ratios calculated under the deduction approach (ie consolidation has a less conservative outcome than deduction), the bank must adjust the capital ratio downwards through applying a regulatory adjustment (ie a deduction) to the relevant component of capital.

30.6 The capital invested in a majority-owned or -controlled insurance entity may exceed the amount of regulatory capital required for such an entity (surplus capital). Supervisors may permit the recognition of such surplus capital in calculating a bank's capital adequacy, under limited circumstances and subject to disclosure (see [DIS30]).[3] National regulatory practices will determine the parameters and criteria, such as legal transferability, for assessing the amount and availability of surplus capital that could be recognised in bank capital. Other examples of availability criteria include: restrictions on transferability due to regulatory constraints, to tax implications and to adverse impacts on external credit assessment institutions' ratings. Where a bank does not have a full ownership interest in an insurance entity (eg 50% or more but less than 100% interest), surplus capital recognised should be proportionate to the percentage interest held. Surplus capital in significant minority-owned insurance entities will not be recognised, as the bank would not be in a position to direct the transfer of the capital in an entity which it does not control.

Footnotes

[3] *In a deduction approach, the amount deducted for all equity and other regulatory capital investments will be adjusted to reflect the amount of capital in those entities that is in surplus to regulatory requirements, ie the amount deducted would be the lesser of the investment or the regulatory capital requirement. The amount representing the surplus capital, ie the difference between the amount of the*

investment in those entities and their regulatory capital requirement, would be risk-weighted as an equity investment. If using an alternative group-wide approach, an equivalent treatment of surplus capital will be made.

30.7 Supervisors will ensure that majority-owned or controlled insurance subsidiaries, which are not consolidated and for which capital investments are deducted or subject to an alternative group-wide approach, are themselves adequately capitalised to reduce the possibility of future potential losses to the bank. Supervisors will monitor actions taken by the subsidiary to correct any capital shortfall and, if it is not corrected in a timely manner, the shortfall will also be deducted from the parent bank's capital.

SCO40

Global systemically important banks

Methodology updated to give effect to the changes to the G-SIB framework published in July 2018 and the change to the review process published in November 2021.

Version effective as of 09 Nov 2021

Methodology updated to give effect to the changes to the G-SIB framework published in July 2018 and the change to the review process published in November 2021.

Introduction

40.1 The negative externalities associated with institutions that are perceived as not being allowed to fail due to their size, interconnectedness, complexity, lack of substitutability or global scope are well recognised. In maximising their private benefits, individual financial institutions may rationally choose outcomes that, on a system-wide level, are suboptimal because they do not take into account these externalities. Moreover, the moral hazard costs associated with implicit guarantees derived from the perceived expectation of government support may amplify risk-taking, reduce market discipline and create competitive distortions, and further increase the probability of distress in the future. As a result, the costs associated with moral hazard add to any direct costs of support that may be borne by taxpayers.

40.2 In addition, given the potential cross-border repercussions of a problem in any of the global systemically important banks (G-SIBs) on the financial institutions in many countries and on the global economy at large, this is not uniquely a problem for national authorities, and therefore requires a global minimum agreement.

40.3 Because there is no single solution to the externalities posed by G-SIBs, the official community is addressing these issues through a multipronged approach. The broad aim of the policies is to:

(1) reduce the probability of failure of G-SIBs by increasing their going-concern loss-absorbency (addressed by the measures in this chapter, [RBC40] and other G-SIB-specific measures in the Basel framework); and

(2) reduce the extent or impact of failure of G-SIBs, by improving global recovery and resolution measures (where work is led by the Financial Stability Board, or FSB).

Assessing systemic importance

40.4 The Basel Committee's methodology for assessing the systemic importance of G-SIBs relies on an indicator-based measurement approach. The selected indicators are chosen to reflect the different aspects of what generates negative externalities and makes a bank critical for the stability of the financial system. The advantage of the multiple indicator-based measurement approach is that it encompasses many dimensions of systemic importance, is relatively simple and is more robust than currently available model-based measurement approaches and methodologies that rely on only a small set of indicators or market variables.

40.5 Given the focus of the framework on cross-border spillovers and negative global externalities that arise from the failure of a globally active bank, the reference system for assessing systemic impact is the global economy. Consequently, systemic importance is assessed based on data that relate to the consolidated group (ie the unit of analysis is the consolidated group). To be consistent with this approach, the higher loss absorbency requirement applies to the consolidated group. However, as with the minimum requirement and the capital conservation and countercyclical buffers, application at the consolidated level does not rule out the option for the host jurisdictions of subsidiaries of the group also to apply the requirement at the individual legal entity or consolidated level within their jurisdiction.

40.6 The Committee is of the view that global systemic importance should be measured in terms of the impact that a bank's failure can have on the global financial system and wider economy, rather than the likelihood that a failure could occur. This can be thought of as a global, system-wide, loss-given-default (LGD) concept rather than a probability of default

(PD) concept.

40.7 The methodology gives an equal weight of 20% to each of five categories of systemic importance, which are: size, cross-jurisdictional activity, interconnectedness, substitutability/financial institution infrastructure and complexity. With the exception of the size category, the Committee has identified multiple indicators in each of the categories, with each indicator equally weighted within its category, except for the substitutability category. That is, where there are two indicators in a category, each indicator is given a 10% overall weight; where there are three, the indicators are each weighted 6.67% (ie 20/3). In the substitutability category, two indicators are weighted 6.67% (assets under custody and payment activity), while underwritten transactions in debt and equity markets and the new trading volume indicator each weigh 3.33%. This split reflects the complementary role of the trading volume indicator, which is to capture potential disruptions in the provision of liquidity in the secondary market for some exposures, while the underwriting indicator captures liquidity in the primary market.

40.8 In 2013, the Committee found that, relative to the other categories that make up the G-SIB framework, the substitutability category has a greater impact on the assessment of systemic importance than the Committee intended for banks that are dominant in the provision of payment, underwriting and asset custody services. Therefore, the Committee decided to apply a cap to the substitutability category by limiting the maximum score to 500 basis points.

40.9 The global systemically important insurers framework does not formally capture the insurance subsidiaries of banking groups. Furthermore, some jurisdictions include insurance subsidiaries in their regulatory scope of consolidation whilst others do not, which may create an inconsistency in the systemic assessment of banking groups across jurisdictions. Against this background, the Committee has decided to include insurance activities for the following indicators: total exposures, intra-financial system assets, intra-financial system liabilities, securities outstanding, notional amount of over-the-counter (OTC) derivatives and level 3 assets in the size, interconnectedness and complexity categories. The approach therefore includes the following indicators with the following weights:

Indicator-based measurement approach — Table 1

Category (and weighting)	Individual indicator	Indicator weighting
Cross-jurisdictional activity (20%)	Cross-jurisdictional claims	10%
	Cross-jurisdictional liabilities	10%
Size (20%)	Total exposures as defined for use in the Basel III leverage ratio*	20%
Interconnectedness (20%)	Intra-financial system assets*	6.67%
	Intra-financial system liabilities*	6.67%
	Securities outstanding*	6.67%
Substitutability/financial institution infrastructure (20%)	Assets under custody	6.67%
	Payments activity	6.67%
	Underwritten transactions in debt and equity markets	3.33%
	Trading volume	3.33%
Complexity (20%)	Notional amount of OTC derivatives*	6.67%

	Level 3 assets*	6.67%
	Trading and available-for-sale securities	6.67%
* Extended scope of consolidation to include insurance activities.		

40.10 For each bank, the score for a particular indicator is calculated by dividing the individual bank amount (expressed in EUR) by the aggregate amount for the indicator summed across all banks in the sample.[1] This amount is then multiplied by 10,000 to express the indicator score in terms of basis points. For example, if a bank's size divided by the total size of all banks in the sample is 0.03 (ie the bank makes up 3% of the sample total) its score will be expressed as 300 basis points. Each category score for each bank is determined by taking a simple average of the indicator scores in that category. The overall score for each bank is then calculated by taking a simple average of its five category scores and then rounding to the nearest whole basis point.[2] The maximum total score, ie the score that a bank would have if it were the only bank in sample, is 10,000 basis points (ie 100%).[3]

Footnotes

1 *See [SCO40.19] for a description of how the sample of banks is determined.*

2 *Fractional values between 0 and 0.5 are rounded down, while values from 0.5 to 1 are rounded up.*

3 *This ignores the impact of the cap on the substitutability category. The impact of the cap is such that the actual maximum score if there were only one bank in the sample is 8,000 basis points plus one fifth of the maximum substitutability score.*

40.11 When calculating a bank's indicators, the data must be converted from the reporting currency to euros using the exchange rates published on the Basel Committee website. These rates should not be rounded in performing the conversions, as this may lead to inaccurate results.

40.12 There are different sets of currency conversions on the website, each corresponding to a different fiscal year-end. Within each set, there are two conversion tables. The first is a point-in-time, or spot, conversion rate corresponding to the following fiscal year-ends: 30 September, 30 October, 31 December, and 31 March (of the following year). The second set is an average of the exchange rates over the relevant fiscal year. Unless the bank decides to collect the daily flow data in the reporting currency directly and convert the data using a consistent set of daily exchange rate quotations, the average rates over the bank's fiscal year should be used to convert the individual payments data into the bank's reporting currency. The 31 December spot rate should be used to convert each of the 12 indicator values (including total payments activity) to the G-SIB assessment methodology reporting currency (ie euros).

Cross-jurisdictional activity

40.13 Given the focus on G-SIBs, the objective of this indicator is to capture banks' global footprint. Two indicators in this category measure the importance of the bank's activities outside its home (headquarter) jurisdiction relative to overall activity of other banks in the sample:

(1) cross-jurisdictional claims; and

(2) cross-jurisdictional liabilities.

40.14 The idea is that the international impact of a bank's distress or failure would vary in line with its share of cross-jurisdictional assets and liabilities. The greater a bank's global reach, the more difficult it is to coordinate its resolution and the more widespread the spillover effects from its failure.

Size

40.15 A bank's distress or failure is more likely to damage the global economy or financial markets if its activities comprise a large share of global activity. The larger the bank, the more difficult it is for its activities to be quickly replaced by other banks and therefore the greater the chance that its distress or failure would cause disruption to the financial markets in which it operates. The distress or failure of a large bank is also more likely to damage confidence in the financial system as a whole. Size is therefore a key measure of systemic importance. One indicator is used to measure size: the measure of total exposures used in the Basel III leverage ratio, including exposures arising from insurance subsidiaries.

Interconnectedness

40.16 Financial distress at one institution can materially increase the likelihood of distress at other institutions given the network of contractual obligations in which these firms operate. A bank's systemic impact is likely to be positively related to its interconnectedness vis-à-vis other financial institutions. Three indicators are used to measure interconnectedness, all of which include insurance subsidiaries:

(1) intra-financial system assets;

(2) intra-financial system liabilities; and

(3) securities outstanding.

Substitutability / financial institution infrastructure

40.17 The systemic impact of a bank's distress or failure is expected to be negatively related to its degree of substitutability as both a market participant and client service provider, ie it is expected to be positively related to the extent to which the bank provides financial institution infrastructure. For example, the greater a bank's role in a particular business line, or as a service provider in underlying market infrastructure (eg payment systems), the larger the disruption will likely be following its failure, in terms of both service gaps and reduced flow of market and infrastructure liquidity. At the same time, the cost to the failed bank's customers in having to seek the same service from another institution is likely to be higher for a failed bank with relatively greater market share in providing the service. Four indicators are used to measure substitutability/financial institution infrastructure:

(1) assets under custody;

(2) payments activity;

(3) underwritten transactions in debt and equity markets; and

(4) trading volume.

Complexity

40.18 The systemic impact of a bank's distress or failure is expected to be positively related to its overall complexity – that is, its business, structural and operational complexity. The more complex a bank is, the greater are the costs and time needed to resolve the bank. Three indictors are used to measure complexity, the first two of which include insurance

subsidiaries:

(1) notional amount of OTC derivatives;

(2) Level 3 assets; and

(3) trading and available-for-sale securities.

Sample of banks

40.19 The indicator-based measurement approach uses a large sample of banks as its proxy for the global banking sector. Data supplied by this sample of banks is then used to calculate banks' scores. Banks fulfilling any of the following criteria will be included in the sample and will be required to submit the full set of data used in the assessment methodology to their supervisors:

(1) Banks that the Committee identifies as the 75 largest global banks, based on the financial year-end Basel III leverage ratio exposure measure, including exposures arising from insurance subsidiaries.

(2) Banks that were designated as G-SIBs in the previous year (unless supervisors agree that there is compelling reason to exclude them).

(3) Banks that have been added to the sample by national supervisors using supervisory judgment (subject to certain criteria).

Bucketing approach

40.20 Banks that have a score produced by the indicator-based measurement approach that exceeds a cutoff level are classified as G-SIBs. Supervisory judgment may also be used to add banks with scores below the cutoff to the list of G-SIBs. This judgment will be exercised according to the principles set out in [SCO40.23] to [SCO40.26].

40.21 Each year, the Committee runs the assessment and, if necessary, reallocates G-SIBs into different categories of systemic importance based on their scores and supervisory judgment. G-SIBs are allocated into equally sized buckets based on their scores of systemic importance, with varying levels of higher loss absorbency requirements applied to the different buckets as set out in [RBC40.4] and [RBC40.5]. The cutoff score for G-SIB designation is 130 basis points and the buckets corresponding to the different higher loss absorbency requirements each have a range of 100 basis points.[4]

Footnotes

[4] *Cutoff scores and bucket thresholds are available at www.bis.org/bcbs/gsib/cutoff.htm .*

40.22 The number of G-SIBs, and their bucket allocations, will evolve over time as banks change their behaviour in response to the incentives of the G-SIB framework as well as other aspects of Basel III and country-specific regulations. Moreover, if a bank's score increases such that it exceeds the top threshold of the fourth bucket, new buckets will be added to accommodate the bank. New buckets will be equal in size in terms of scores to each of the existing buckets, and will have incremental higher loss absorbency requirements, as set out in [RBC40.4] and [RBC40.5], to provide incentives for banks to avoid becoming more systemically important.

Criteria for supervisory judgment

40.23 Supervisory judgment can support the results derived from the indicator-based measurement approach of the assessment methodology. The Committee has developed

four principles for supervisory judgment:

(1) The bar for judgmental adjustment to the scores should be high: in particular, judgment should only be used to override the indicator-based measurement approach in exceptional cases. Those cases are expected to be rare.

(2) The process should focus on factors pertaining to a bank's global systemic impact, ie the impact of the bank's distress/failure and not the probability of distress/failure (ie the riskiness) of the bank.

(3) Views on the quality of the policy/resolution framework within a jurisdiction should not play a role in this G-SIB identification process.[5]

(4) The judgmental overlay should comprise well documented and verifiable quantitative as well as qualitative information.

Footnotes

[5] *However, this is not meant to preclude any other actions that the Committee, the FSB or national supervisors may wish to take for global systemically important financial institutions to address the quality of the policy/resolution framework. For example, national supervisors could impose higher capital surcharges beyond the higher loss absorbency requirements for G-SIBs that do not have an effective and credible recovery and resolution plan.*

Ancillary indicators

40.24 The Committee has identified a number of ancillary indicators relating to specific aspects of the systemic importance of an institution that may not be captured by the indicator-based measurement approach alone. These indicators can be used to support the judgment overlay.

40.25 The ancillary indicators are set out in the reporting template and related instructions, which are available on the Committee's website.[6]

Footnotes

[6] *www.bis.org/bcbs/gsib*

Qualitative supervisory judgment

40.26 Supervisory judgment can also be based on qualitative information. This is intended to capture information that cannot be easily quantified in the form of an indicator, for example, a major restructuring of a bank's operation. Qualitative judgments should also be thoroughly explained and supported by verifiable arguments.

Process for incorporating supervisory judgment

40.27 The supervisory judgmental overlay can be incorporated using the following sequential steps to the score produced by the indicator-based measurement approach:

(1) Collection of the data[7] and supervisory commentary for all banks in the sample.

(2) Mechanical application of the indicator-based measurement approach and corresponding bucketing.

(3) Relevant authorities[8] propose adjustments to the score of individual banks on the basis of an agreed process.

(4) The Committee develops recommendations for the FSB.

(5) The FSB and national authorities, in consultation with the Basel Committee, make final

decisions.

Footnotes

[7] *The data collection can start in the second quarter and be finalised in third quarter each year, subject to consultation with national supervisors.*

[8] *Relevant authorities mainly refer to home and host supervisors.*

40.28 The supervisory judgment input to the results of the indicator-based measurement approach should be conducted in an effective and transparent way and ensure that the final outcome is consistent with the views of the Committee as a group. Challenges to the results of the indicator-based measurement approach should only be made if they involve a material impact in the treatment of a specific bank (eg resulting in a different loss absorbency requirement). To limit the risk that resources are used ineffectively, when the authority is not the bank's home supervisor it would be required to take into account the views of the bank's home and major host supervisors. These could be, for instance, the members of the institution's college of supervisors.

40.29 In addition to the materiality and consultation requirements, proposals to challenge the indicator-based measurement approach will be subject to the following modalities. Proposals originating from the home supervisor that result in a lower loss absorbency requirement would be scrutinised and would require a stronger justification than those resulting in a higher loss absorbency requirement. The reverse would apply to proposals originating from other authorities: those recommending a higher loss-absorbency requirement would be subject to higher standards of proof and documentation. The rationale for this asymmetric treatment follows the general principle that the Committee is setting minimum standards.

Periodic review and refinement

40.30 The methodology, including the indicator-based measurement approach itself, the cutoff/ threshold scores and the size of the sample of banks, are regularly monitored and reviewed by the Committee in order to ensure that they remain appropriate in light of: (i) developments in the banking sector; (ii) progress in methods and approaches for measuring systemic importance; (iii) structural changes; and (iv) any evidence of material unintended consequences or material deficiencies with respect to the objectives of the framework. As regards the structural changes in regional arrangements – in particular in the European Banking Union – they will be reviewed as actual changes are made.

40.31 The Committee expects national jurisdictions to prepare a framework in which banks are able to provide high-quality data for the indicators. In order to ensure the transparency of the methodology, the Committee expects banks to disclose relevant data and has set out disclosure requirements in [SCO40.32] to [SCO40.34]. The Committee discloses the values of the cutoff scores, the threshold scores for buckets, the denominators used to normalise the indicator values and the G-SIB indicators of all banks so that banks, regulators and market participants can understand how actions banks take could affect their systemic importance score and thereby the applicable magnitude of the HLA requirement.

Disclosure requirements

40.32 For each financial year-end, all banks with a leverage ratio exposure measure, including exposures arising from insurance subsidiaries, that exceeded EUR 200 billion in the previous year-end (using the exchange rate applicable at the financial year-end) should be required by national authorities to make publicly available the 13 indicators used in the

assessment methodology. Banks should note in their disclosures that those figures are subject to revision and restatement.

40.33 Banks below this threshold that have been added to the sample owing to supervisory judgment or as a result of being classified as a G-SIB in the previous year would also be required to comply with the disclosure requirements.

40.34 Banks should also be required by national authorities to publicly disclose if the data used to calculate the G-SIB scores differ from the figures previously disclosed. To the extent that a revision to the data is required, banks should disclose the accurate figures in the financial quarter immediately following the finalisation of the Committee's G-SIB score calculation.

Operational timetable

40.35 The assessment methodology set out in this chapter applies from 2021, based on end-2020 data. The corresponding higher loss absorbency requirement (defined in [RBC40]) applies from 1 January 2023.

SCO50

Domestic systemically important banks

First version in the format of the consolidated framework.

Version effective as of 15 Dec 2019

First version in the format of the consolidated framework.

Introduction

50.1 The Committee has developed a set of principles that constitutes the domestic systemically important bank (D-SIB) framework. The 12 principles can be broadly categorised into two groups: the first group ([SCO50.5]) focuses mainly on the assessment methodology for D-SIBs while the second group ([RBC40.7]) focuses on higher loss absorbency (HLA) for D-SIBs.[1]

Footnotes

[1] *HLA refers to higher loss absorbency relative to the Basel III requirements for internationally active banks. For domestic banks that are not internationally active, HLA is relative to requirements for domestic banks.*

50.2 The principles were developed to be applied to consolidated groups and subsidiaries. However, national authorities may apply them to branches in their jurisdictions in accordance with their legal and regulatory frameworks.[2]

Footnotes

[2] *While the application to branches of the principles regarding the assessment of systemic importance should not pose any specific problem, the range of policy responses that host authorities have available to deal with systemic branches in their jurisdiction may be more limited.*

50.3 The additional requirements applied to global systemically important banks (G-SIBs), which apply over and above the Basel requirements applying to all internationally active banks, are intended to limit the cross-border negative externalities on the global financial system and economy associated with the most globally systemic banking institutions. Similar externalities can apply at a domestic level. There are many banks that are not significant from an international perspective, but nevertheless could have an important impact on their domestic financial system and economy compared to non-systemic institutions. Some of these banks may have cross-border externalities, even if the effects are not global in nature.

50.4 A D-SIB framework is best understood as taking the complementary perspective to the G-SIB regime by focusing on the impact that the distress or failure of banks (including by international banks) will have on the domestic economy. As such, it is based on the assessment conducted by the local authorities, who are best placed to evaluate the impact of failure on the local financial system and the local economy. This point has two implications:

(1) The first is that, in order to accommodate the structural characteristics of individual jurisdictions, the assessment and application of policy tools should allow for an appropriate degree of national discretion. This contrasts with the prescriptive approach in the G-SIB framework.

(2) The second implication is that, because a D-SIB framework is still relevant for reducing cross-border externalities due to spillovers at regional or bilateral level, the effectiveness of local authorities in addressing risks posed by individual banks is of interest to a wider group of countries. A D-SIB framework, therefore, should establish a minimum set of principles, which ensures that it is complementary with the G-SIB framework, addresses adequately cross-border externalities and promotes a level playing field.

Principles on the D-SIB assessment methodology

50.5 The principles on the D-SIB assessment methodology are set out below:

(1) National authorities should establish a methodology for assessing the degree to which banks are systemically important in a domestic context.

(2) The assessment methodology for a D-SIB should reflect the potential impact of, or externality imposed by, a bank's failure.

(3) The reference system for assessing the impact of failure of a D-SIB should be the domestic economy.

(4) Home authorities should assess banks for their degree of systemic importance at the consolidated group level, while host authorities should assess subsidiaries in their jurisdictions, consolidated to include any of their own downstream subsidiaries, for their degree of systemic importance.

(5) The impact of a D-SIB's failure on the domestic economy should, in principle, be assessed having regard to bank-specific factors. National authorities can consider other measures / data that would inform the bank-specific indicators within each of the below factors, such as size of the domestic economy:

(a) size;

(b) interconnectedness;

(c) substitutability / financial institution infrastructure (including considerations related to the concentrated nature of the banking sector); and

(d) complexity (including the additional complexities from cross-border activity).

(6) National authorities should undertake regular assessments of the systemic importance of the banks in their jurisdictions to ensure that their assessment reflects the current state of the relevant financial systems and that the interval between D-SIB assessments not be significantly longer than the G-SIB assessment frequency.

(7) National authorities should publicly disclose information that provides an outline of the methodology employed to assess the systemic importance of banks in their domestic economy.

Principles 1 and 2: assessment methodologies

50.6 A starting point for the development of principles for the assessment of D-SIBs is a requirement that all national authorities should undertake an assessment of the degree to which banks are systemically important in a domestic context. The rationale for focusing on the domestic context is outlined in [SCO50.10].

50.7 [SCO40.6] states that “global systemic importance should be measured in terms of the impact that a failure of a bank can have on the global financial system and wider economy rather than the likelihood that a failure can occur. This can be thought of as a global, system-wide, loss-given-default (LGD) concept rather than a probability of default (PD) concept.” Consistent with the G-SIB methodology, the Committee is of the view that D-SIBs should also be assessed in terms of the potential impact of their failure on the relevant reference system. One implication of this is that to the extent that D-SIB indicators are included in any methodology, they should primarily relate to “impact of failure” measures and not “risk of failure” measures.

Principles 3 and 4: reference system and scope of assessment

50.8 Two key aspects that shape the D-SIB framework and define its relationship to the G-SIB framework relate to how it deals with two conceptual issues with important practical

implications:

(1) what is the reference system for the assessment of systemic impact; and

(2) what is the appropriate unit of analysis (ie the entity which is being assessed)?

50.9 For the G-SIB framework, the appropriate reference system is the global economy, given the focus on cross-border spillovers and the negative global externalities that arise from the failure of a globally active bank. As such this allowed for an assessment of the banks that are systemically important in a global context. The unit of analysis was naturally set at the globally consolidated level of a banking group ([SCO40.5] states that "systemic importance is assessed based on data that relate to the consolidated group").

50.10 Correspondingly, a process for assessing systemic importance in a domestic context should focus on addressing the externalities that a bank's failure generates at a domestic level. Thus, the Committee is of the view that the appropriate reference system should be the domestic economy, ie that banks would be assessed by the national authorities for their systemic importance to that specific jurisdiction. The outcome would be an assessment of banks active in the domestic economy in terms of their systemic importance.

50.11 In terms of the unit of analysis, the Committee is of the view that home authorities should consider banks from a (globally) consolidated perspective. This is because the activities of a bank outside the home jurisdiction can, when the bank fails, have potential significant spillovers to the domestic (home) economy. Jurisdictions that are home to banking groups that engage in cross-border activity could be impacted by the failure of the whole banking group and not just the part of the group that undertakes domestic activity in the home economy. This is particularly important given the possibility that the home government may have to fund/resolve the foreign operations in the absence of relevant cross-border agreements. This is in line with the concept of the G-SIB framework.

50.12 When it comes to the host authorities, the Committee is of the view that they should assess foreign subsidiaries in their jurisdictions, also consolidated to include any of their own downstream subsidiaries, some of which may be in other jurisdictions. For example, for a cross-border financial group headquartered in country X, the authorities in country Y would only consider subsidiaries of the group in country Y plus the downstream subsidiaries, some of which may be in country Z, and their impact on the economy Y. Thus, subsidiaries of foreign banking groups would be considered from a local or sub-consolidated basis from the level starting in country Y. The scope should be based on regulatory consolidation as in the case of the G-SIB framework. Therefore, for the purposes of assessing D-SIBs, insurance or other non-banking activities should only be included insofar as they are included in the regulatory consolidation.

50.13 The assessment of foreign subsidiaries at the local consolidated level also acknowledges the fact that the failure of global banking groups could impose outsized externalities at the local (host) level when these subsidiaries are significant elements in the local (host) banking system. This is important since there exist several jurisdictions that are dominated by foreign subsidiaries of internationally active banking groups.

Principle 5: assessing the impact of a D-SIB's failure

50.14 The G-SIB methodology identifies five broad categories of factors that influence global systemic importance: size, cross-jurisdictional activity, interconnectedness, substitutability/ financial institution infrastructure and complexity. The indicator-based approach and weighting system in the G-SIB methodology was developed to ensure a consistent

international ranking of G-SIBs. The Committee is of the view that this degree of detail is not warranted for D-SIBs, given the focus is on the domestic impact of failure of a bank and the wide ranging differences in each jurisdiction's financial structure hinder such international comparisons being made. This is one of the reasons why the D-SIB framework has been developed as a principles-based approach.

50.15 Consistent with this view, it is appropriate to list, at a high level, the broad category of factors (eg size) that jurisdictions should have regard to in assessing the impact of a D-SIB's failure. Among the five categories in the G-SIB framework, size, interconnectedness, substitutability/financial institution infrastructure and complexity are all relevant for D-SIBs as well. Cross-jurisdictional activity, the remaining category, may not be as directly relevant, since it measures the degree of global (cross-jurisdictional) activity of a bank which is not the focus of the D-SIB framework.

50.16 In addition, national authorities may choose to also include some country-specific factors. A good example is the size of a bank relative to domestic gross domestic product (GDP). If the size of a bank is relatively large compared to the domestic GDP, it would make sense for the national authority of the jurisdiction to identify it as a D-SIB whereas a same-sized bank in another jurisdiction, which is smaller relative to the GDP of that jurisdiction, may not be identified as a D-SIB.

50.17 National authorities should have national discretion as to the appropriate relative weights they place on these factors depending on national circumstances.

Principle 6: regular assessment of systemic importance

50.18 The Committee believes it is good practice for national authorities to undertake a regular assessment as to the systemic importance of the banks in their financial systems. The assessment should also be conducted if there are important structural changes to the banking system such as, for example, a merger of major banks. A national authority's assessment process and methodology will be reviewed by the Committee's implementation monitoring process.

50.19 It is also desirable that the interval of the assessments not be significantly longer than that for G-SIBs (ie one year). For example, a systemically important bank could be identified as a G-SIB but also a D-SIB in the same jurisdiction or in other host jurisdictions. Alternatively, a G-SIB could drop from the G-SIB list and become/continue to be a D-SIB. In order to keep a consistent approach in these cases, it would be sensible to have a similar frequency of assessments for the two frameworks.

Principle 7: transparency on the methodology

50.20 The assessment process used needs to be clearly articulated and made public so as to set up the appropriate incentives for banks to seek to reduce the systemic risk they pose to the reference system. This was the key aspect of the G-SIB framework where the assessment methodology and the disclosure requirements of the Committee and the banks were set out in the G-SIB rules text. By taking these measures, the Committee sought to ensure that banks, regulators and market participants would be able to understand how the actions of banks could affect their systemic importance score and thereby the required magnitude of additional loss absorbency. The Committee believes that transparency of the assessment process for the D-SIB framework is also important, even if it is likely to vary across jurisdictions given differences in frameworks and policy tools used to address the systemic importance of banks.

SCO60

Cryptoasset exposures

First version in the consolidated Basel Framework.

Version effective as of 01 Jan 2025

First version in the consolidated Basel Framework.

Introduction

60.1 This chapter sets out how the Basel Framework is to be applied in respect of banks' exposures to cryptoassets. Cryptoassets are defined as private digital assets that depend on cryptography and distributed ledger technologies (DLT) or similar technologies. Digital assets are a digital representation of value, which can be used for payment or investment purposes or to access a good or service.

60.2 Dematerialised securities (securities that have been moved from physical certificates to electronic book-keeping) that are issued through DLT or similar technologies are considered to be within the scope of this chapter and are referred to as tokenised traditional assets, whereas those dematerialised securities that use electronic versions of traditional registers and databases which are centrally administered are not within scope.

60.3 The prudential treatment of central bank digital currencies (CBDCs) is not described within the Basel Framework. The Committee will give further consideration to the treatment of CBDCs as they are issued.

60.4 For the purposes of this chapter, the term "exposure" includes on- or off-balance sheet amounts that give rise to credit, market, operational and/or liquidity risks. Certain parts of the chapter, such as the operational risk requirements and the risk management and supervisory review sections, are also applicable to banks' cryptoasset activities, such as custodial services involving the safekeeping or administration of client cryptoassets on a segregated basis, that do not generally give rise to credit, market or liquidity requirements.

60.5 The remainder of this chapter is organised according to the following sections:

(1) Classification conditions: [SCO60.6] to [SCO60.22].

(2) Banking/trading book boundary, use of internal models and accounting classification: [SCO60.23] to [SCO60.25].

(3) Minimum capital requirements for credit risk for Group 1 cryptoassets: [SCO60.26] to [SCO60.39].

(4) Minimum capital requirements for market risk for Group 1 cryptoassets: [SCO60.40] to [SCO60.51].

(5) Add-on for infrastructure risk for Group 1 cryptoassets: [SCO60.52] to [SCO60.53].

(6) Minimum capital requirements for Group 2 cryptoassets: [SCO60.54] to [SCO60.86].

(7) Minimum capital requirements for credit valuation adjustment (CVA) risk: [SCO60.87] to [SCO60.92].

(8) Minimum capital requirements for counterparty credit risk: [SCO60.93] to [SCO60.99].

(9) Minimum capital requirements for operational risk: [SCO60.100].

(10) Minimum liquidity risk requirements: [SCO60.101] to [SCO60.112].

(11) Leverage ratio requirements: [SCO60.113] to [SCO60.114].

(12) Large exposure requirements: [SCO60.115].

(13) Group 2 exposure limit: [SCO60.116] to [SCO60.119].

(14) Bank risk management and supervisory review: [SCO60.120] to [SCO60.127].

(15) Disclosure requirements: [SCO60.128] to [SCO60.130].

(16) Definitions: [SCO60.131].

Classification conditions

60.6 In certain areas of this chapter, most notably for the purposes of credit, market and liquidity risk, the prudential treatment of a bank's cryptoasset exposures varies according to the prudential classification of the cryptoassets. To determine the prudential classification, cryptoassets must be screened on an ongoing basis and classified into two broad groups:

(1) Group 1 cryptoassets are those cryptoassets that meet the classification conditions set out in [SCO60.8] to [SCO60.19]. Group 1 cryptoassets consist of:

(a) Group 1a: Tokenised traditional assets[1] that meet the classification conditions.

(b) Group 1b: Cryptoassets with effective stabilisation mechanisms that meet the classification conditions.

(2) Group 2 cryptoassets are those cryptoassets that fail to meet the classification conditions set out in [SCO60.8] to [SCO60.19]. Group 2 cryptoassets consist of:

(a) Group 2a: Cryptoassets (including tokenised traditional assets, stablecoins and unbacked cryptoassets) that fail to meet the classification conditions, but pass the Group 2a hedging recognition criteria.

(b) Group 2b: All other cryptoassets (ie tokenised traditional assets, stablecoins and unbacked cryptoasset that fail to meet the classification conditions and fail the Group 2a hedging recognition criteria).

Footnotes

[1] *Traditional assets are those assets that are captured within the Basel Framework that are not classified under this chapter as cryptoassets.*

60.7 To be classified as Group 1a or Group 1b, cryptoassets must meet on an ongoing basis the classification conditions in [SCO60.8] to [SCO60.19] below.

Classification condition 1

60.8 : The cryptoasset is either: (i) a tokenised traditional asset; or (ii) has a stabilisation mechanism that is effective at all times in linking its value to a traditional asset or a pool of traditional assets (ie reference asset(s)).

60.9 Tokenised traditional assets will only meet classification condition 1 if they satisfy all of the following requirements:

(1) They are digital representations of traditional assets using cryptography, DLT or similar technology to record ownership.

(2) They pose the same level of credit and market risk as the traditional (non-tokenised) form of the asset. In practice, this means the following for tokenised traditional assets:

(a) Bonds, loans, claims on banks (including in the form of deposits),[2] equities and derivatives. The cryptoasset must confer the same level of legal rights as ownership of these traditional forms of financing (eg rights to cash flows, claims in insolvency etc). In addition, there must be no feature of the cryptoasset that could prevent obligations to the bank being paid in full when due as compared with a traditional (non-tokenised) version of the asset.

(b) Commodities. The cryptoasset must confer the same level of legal rights as traditional account-based records of ownership of a physical commodity.

(c) Cash held in custody. The cryptoassets must confer the same level of legal rights as cash held in custody.

Footnotes

[2] *In certain jurisdictions bank-issued tokenised payment assets that are backed by the general assets of the bank and not by a pool of reserve assets may be referred to as "stablecoins." Notwithstanding how they may generally be referred to within the jurisdiction, these assets may be included in Group 1a provided they meet all the requisite conditions and would not be assigned to Group 1b based solely on their commonly used local name.*

60.10 Cryptoassets do not meet the condition set out in [SCO60.9](2) above if they:

(1) first need to be redeemed or converted into traditional assets before they receive the same legal rights as direct ownership of traditional assets; or

(2) through their specific construction, they involve additional counterparty credit risks relative to traditional assets.

60.11 Cryptoassets that have a stabilisation mechanism will only meet classification condition 1 if they satisfy all of the following requirements:

(1) The cryptoasset is designed to be redeemable for a predefined amount of a reference asset or assets (eg 1 USD, 1 oz gold) or cash equal to the current market value of the reference asset(s) (eg USD value of 1 oz gold). The value of the reference asset(s) to which one unit of the cryptoasset is designed to be redeemable is referred to as the "peg value".

(2) The stabilisation mechanism is designed to minimise fluctuations in the market value of the cryptoassets relative to the peg value. In order to satisfy the "effective at all times" condition, banks must have a monitoring framework in place verifying that the stabilisation mechanism is functioning as intended.

(3) The stabilisation mechanism enables risk management similar to the risk management of traditional assets, based on sufficient data or experience. For newly established cryptoassets, there may be insufficient data and/or practical experience to perform a detailed assessment of the stabilisation mechanism. Evidence must be provided to satisfy supervisors of the effectiveness of the stabilisation mechanism, including the composition, valuation and frequency of valuation of the reserve asset(s) and the quality of available data.

(4) There exists sufficient information that banks use to verify the ownership rights of the reserve assets upon which the stable value of the cryptoasset is dependent. In the case of underlying physical assets, banks must verify that these assets are stored and managed appropriately. This monitoring framework must function regardless of the cryptoasset issuer. Banks may use the assessments of independent third parties for the purposes of verification of ownership rights only if they are satisfied that the assessments are reliable.

(5) The cryptoasset passes the redemption risk test set out in [SCO60.12] and the issuer is supervised and regulated by a supervisor that applies prudential capital and liquidity requirements to the issuer. The Committee considered also requiring cryptoassets with stabilisation mechanisms to meet a "basis risk test", but as yet has chosen not to implement this test.[3] The Committee will further study whether there are statistical tests that can reliably identify low-risk stablecoins, and if such a test is identified, will consider it as an additional requirement.

Footnotes

[3] *For a description of the basis risk test, see the second consultative document on*

bank exposures to cryptoasset: https://www.bis.org/bcbs/publ/d533.htm

60.12 . The objective of this test is to ensure that the reserve assets are sufficient to enable the cryptoassets to be redeemable at all times for the peg value, including during periods of extreme stress. To pass the redemption risk test, the bank must ensure that the cryptoasset arrangement meets the following conditions:

(1) Value and composition of reserve assets. The value of the reserve assets (net all non cryptoasset claims on these assets) must at all times, including during periods of extreme stress, equal or exceed the aggregate peg value of all outstanding cryptoassets. If the reserve assets expose the holder to risk in addition to the risks arising from the reference assets,[4] the value of the reserve assets must sufficiently overcollateralise the redemption rights of all outstanding cryptoassets. The level of overcollateralisation must be sufficient to ensure that even after stressed losses are incurred on the reserve assets, their value exceeds the aggregate value of the peg of all outstanding cryptoassets.

(2) Asset quality criteria for reserve assets. For cryptoassets that are pegged to one or more currencies, the reserve assets must be comprised of assets with minimal market and credit risk. The assets shall be capable of being liquidated rapidly with minimal adverse price effect. For example, these assets may be defined as Level 1 HQLA as stipulated in [LCR30.41]. Further, reserve assets must be denominated in the same currency or currencies in the same ratios as the currencies used for the peg value. A de minimis portion of the reserve assets may be held in a currency other than the currencies used for the peg value, provided that the holding of such currency is necessary for the operation of the cryptoasset arrangement and all currency mismatch risk between the reserve assets and peg value has been appropriately hedged.

(3) Management of reserve assets. The governance arrangements relating to the management of reserve assets must be comprehensive and transparent. They must ensure that:

(a) The reserve assets are managed and invested with an explicit legally enforceable objective of ensuring that all cryptoassets can be redeemed promptly at the peg value, including under periods of extreme stress.

(b) A robust operational risk and resilience framework exists to ensure the availability and safe custody of the reserve assets.

(c) A mandate that describes the types of assets that may be included in the reserve must be publicly disclosed and kept up to date.

(d) The composition and value of the reserve assets are publicly disclosed on a regular basis. The value must be disclosed at least daily and the composition must be disclosed at least weekly.

(e) The reserve assets are subject to an independent external audit at least annually to confirm they match the disclosed reserves and are consistent with the mandate.

Footnotes

[4] *For example, consider a cryptoasset that is redeemable for a given currency amount (ie the currency amount is the reference asset) but is backed by bonds denominated in the same currency (ie the bonds are the reserve asset). The reserve assets will give rise to credit, market and liquidity risks that may result in losses relative to the value of the reference asset.*

60.13 Stabilisation mechanisms that: (i) reference other cryptoassets as underlying assets

(including those that reference other cryptoassets that have traditional assets as underlying); or (ii) use protocols to increase or decrease the supply of the cryptoasset[5] do not meet classification condition 1.

Footnotes

[5] *Cryptoassets that use protocols to maintain their value are in some cases referred to as "algorithm-based stablecoins".*

Classification condition 2

60.14 : All rights, obligations and interests arising from the cryptoasset arrangement are clearly defined and legally enforceable in all the jurisdictions where the asset is issued and redeemed. In addition, the applicable legal framework(s) ensure(s) settlement finality. Banks are required to conduct a legal review of the cryptoasset arrangement to ensure this condition is met, and make the review available to their supervisors upon request.

60.15 To meet classification condition 2, the following requirements must be met:

(1) At all times the cryptoasset arrangements must ensure full transferability and settlement finality. In addition, cryptoassets with stabilisation mechanisms must provide a robust legal claim against the issuer and/or underlying reserve assets and must ensure full redeemability (ie the ability to exchange cryptoassets for amounts of pre-defined assets such as cash, bonds, commodities, equities or other traditional assets) at all times and at their peg value. In order for a cryptoasset arrangement to be considered as having full redeemability, it must allow for the redemption to be completed within 5 calendar days of the redemption request at all times.

(2) At all times the cryptoasset arrangements are properly documented. For cryptoassets with stabilisation mechanisms, cryptoasset arrangements must clearly define which parties have the right to redeem; the obligation of the redeemer to fulfil the arrangement; the timeframe for this redemption to take place; the traditional assets in the exchange; and how the redemption value is determined. These arrangements must also be valid in instances where parties involved in these arrangements may not be located in the same jurisdiction where the cryptoasset is issued and redeemed. At all times, settlement finality in cryptoasset arrangements must be properly documented such that it is clear when key financial risks are transferred from one party to another, including the point at which transactions are irrevocable. The documentation described in this paragraph must be publicly disclosed by the cryptoasset issuer. If the offering of the cryptoasset to the public has been approved by the relevant regulator on the basis of this public disclosure, the condition in [SCO60.15](2) will be considered fulfilled. Otherwise, an independent legal opinion would be needed to confirm [SCO60.15](2) has been met.

Classification condition 3

60.16 : The functions of the cryptoasset and the network on which it operates, including the distributed ledger or similar technology on which it is based, are designed and operated to sufficiently mitigate and manage any material risks.

60.17 To meet classification condition 3, the following requirements must be met:

(1) The functions of the cryptoasset, such as issuance, validation, redemption and transfer of the cryptoassets, and the network on which it runs, do not pose any material risks that could impair the transferability, settlement finality or, where applicable, redeemability of the cryptoasset. To this end, entities performing activities associated with these functions[6] must follow robust risk governance and risk control policies and

practices to address risks including, but not limited to: credit, market and liquidity risks; operational risk (including outsourcing, fraud and cyber risk) and risk of loss of data; various non-financial risks, such as data integrity; operational resilience (ie operational reliability and capacity); third-party risk management; and Anti-Money Laundering/ Countering the Financing of Terrorism (AML/CFT).

(2) All key elements of the network must be well-defined such that all transactions and participants are traceable. Key elements include: (i) the operational structure (ie whether there is one or multiple entities that perform core function(s) of the network); (ii) degree of access (ie whether the network is restricted or un-restricted); (iii) technical roles of the nodes (including whether there is a differential role and responsibility among nodes); and (iv) the validation and consensus mechanism of the network (ie whether validation of a transaction is conducted with single or multiple entities).

Footnotes

[6] *Examples of these entities include but are not limited to: issuers, operators of the transfer and settlement systems for the cryptoasset; administrators of the cryptoasset stabilisation mechanism and custodians of any underlying assets supporting the stabilisation mechanism.*

Classification condition 4

60.18 : Entities that execute redemptions, transfers, storage or settlement finality of the cryptoasset, or manage or invest reserve assets, must: (i) be regulated and supervised, or subject to appropriate risk management standards; and (ii) have in place and disclose a comprehensive governance framework.

60.19 Entities subject to condition 4 include operators of the transfer and settlement systems for the cryptoasset, wallet providers and, for cryptoassets with stabilisation mechanisms, administrators of the stabilisation mechanism and custodians of the reserve assets. Node validators may be subject to appropriate risk management standards as an alternative to being regulated and supervised.

Responsibilities for determining and monitoring compliance with the classification conditions

60.20 Banks, on an ongoing basis, are responsible for assessing whether the cryptoassets to which they are exposed are compliant with the classification conditions set out in [SCO60.6] to [SCO60.19] and the hedging recognition criteria set out in [SCO60.55]. These assessments will determine whether the cryptoassets are classified as Group 1a, Group 1b, Group 2a or Group 2b. To this end, banks must have in place the appropriate risk management policies, procedures, governance, human and IT capacities to evaluate the risks of engaging in cryptoassets and implement these accordingly on an ongoing basis and in accordance with internationally accepted standards. Banks must fully document the information used in determining compliance with the classification conditions and make this available to supervisory authorities on request. In addition:

(1) Regarding cryptoassets to which a bank is already exposed on the implementation date of [SCO60], the bank must inform their supervisor of the classification decisions they have reached for each cryptoasset. This information should ideally be sent well before the implementation date of [SCO60]. If providing the information is not possible in advance of implementation of [SCO60], it must be sent as soon as practical afterwards. Specifically, it must be sent with sufficient time for the supervisor to review and, if necessary, override the classification decision reached by the bank prior to the publication of the bank's first set of Pillar 3 disclosures after the implementation of

[SCO60]. Authorities may wish to specify a suitable deadline for banks in their jurisdiction with cryptoasset exposures that takes into consideration available supervisory resources and bank reporting schedules.

(2) Regarding cryptoassets that a bank may wish to acquire after the implementation date of [SCO60], in advance of any acquisition of cryptoassets the bank must inform their supervisor of their classification assessment of the cryptoassets. This must occur with sufficient time for the supervisor to review and, if necessary, override the classification decision reached prior to the bank's acquisition of the cryptoasset. Authorities may wish to specify a suitable time period for such notifications that takes into consideration available supervisory resources.

60.21 Supervisors are responsible for: (i) reviewing and assessing banks' analysis and risk management and measurement approaches; and (ii) reviewing banks' classification decisions (as outlined in [SCO60.20]). A bank's supervisor may rely on other regulators or supervisors overseeing the entities' management of risks attributable to the functions mentioned above; as well as independent third-party assessors determined to have the required expertise and skills, to evaluate the specific risk characteristics of cryptoasset arrangements. Supervisory authorities must also have the power to override banks' classification decisions, if they do not agree with the assessments undertaken by banks. The override should be exercised in a consistent way across banks. The override may be used at any time by the supervisory authority. In certain cases, authorities may wish to set a future date at which the override comes into effect, to allow banks time to prepare for its impact.

60.22 To ensure consistent application across jurisdictions, authorities will routinely compare and share their supervisory information on banks' assessments of cryptoassets against the classification conditions.

Banking/trading book boundary, use of internal models and accounting classification

60.23 [RBC25] must be used to determine the allocation of cryptoassets between the banking book and trading book, subject to the following specifications and exceptions:

(1) Group 1a cryptoassets must be assigned to the banking book or trading book based on the application of the boundary criteria to the non-tokenised equivalent traditional assets.

(2) Group 1b cryptoassets must be assigned to the banking book or trading book based on the application of the boundary criteria to the reference asset(s).

(3) Group 2a cryptoassets must be treated according to the proposed market risk rules, independent of whether they stem from trading or banking book instruments (ie similar to FX and commodities risk).

(4) Group 2b cryptoassets must be treated according to the standardised conservative prudential treatment outlined in [SCO60.83] to [SCO60.86].

60.24 [CRE] and [MAR] are used to determine whether Group 1 cryptoasset exposures are treated according to standardised or internal model-based approaches to credit and market risk respectively. Models-based approaches must not be applied to Group 2 cryptoassets.

60.25 Cryptoasset exposures are not subject to the deduction requirement that applies to intangible assets set out in [CAP30.7] and [CAP30.8], even in cases where the cryptoasset is classified as an intangible under the applicable accounting standard.

Minimum capital requirements for credit risk for Group 1 cryptoassets

60.26 This section describes how the minimum risk-based capital requirements for credit risk ([CRE]) are to be applied to cryptoasset exposures.

Group 1a cryptoassets (tokenised traditional assets)

60.27 Group 1a cryptoassets (tokenised traditional assets) held in the banking book will generally be subject to the same rules to determine credit risk-weighted assets (RWA) as non-tokenised traditional assets (ie the rules set out in the credit risk standard [CRE]). For example, a tokenised corporate bond held in the banking book will be subject to the same risk weight as the non-tokenised corporate bond held in the banking book.

60.28 The treatment outlined in [SCO60.27] above is based on the assumption that if two exposures confer the same level of legal rights (to cash flows, claims in insolvency, ownership of assets etc) and the same likelihood of paying the owner all amounts due on time (including amounts due in case of default), they will likely have very similar values and pose a similar risk of credit losses. However, there are areas of the credit standards that aim to capture risks that are not directly related to the legal rights of an asset held by a bank or likelihood of timely payment. Banks must separately assess the tokenised traditional asset against these rules, and not assume qualification for a given treatment simply because the traditional (non-tokenised) asset qualifies. For example, a tokenised asset may have different market liquidity characteristics than the traditional (non-tokenised) asset. This could arise because the pool of potential investors that are able to hold tokenised assets might be different to non-tokenised assets.

60.29 The potential for market liquidity characteristics and market values of tokenised assets to differ from non-tokenised assets is important in considering whether Group 1a cryptoassets meet the requirements for the purposes of credit risk mitigation within the credit risk standards. Also, the speed with which a secured creditor could take possession of cryptoasset collateral may be different than for a traditional asset. Therefore, before such assets are recognised as collateral for the purposes of credit risk mitigation, banks must separately assess whether they comply with the relevant eligibility requirements for collateral recognition, such as whether the collateral can be liquidated promptly and legal certainty requirements ([CRE22.9]). In addition to assessing whether tokenised assets held as collateral are eligible to be recognised as credit risk mitigation, banks must analyse the period of time over which they can be liquidated and the depth of market liquidity during a period of downturn. Cryptoassets shall only be recognised as collateral where volatility in values and holding periods under distressed market conditions can be confirmed to not be materially increased compared with the traditional asset or pool of traditional assets. Otherwise the cryptoasset shall not be eligible for recognition of credit risk mitigation unless a bank has received permission from its supervisor for reflecting any material increase in relevant parameters as part of own LGD estimates under the IRB approach.

60.30 [CRE22] sets out the list of eligible forms of financial collateral for the purposes of recognition as a credit risk mitigant under the standardised approach to credit risk. The list is also the basis of eligible financial collateral under the foundation internal ratings-based approach. Only Group 1a cryptoassets that are tokenised versions of the instruments included on the list of eligible financial collateral set out in [CRE22] may qualify for recognition as eligible collateral (subject to also meeting the requirements described above).

Group 1b cryptoassets (cryptoassets with stabilisation mechanisms)

60.31 As a result of the classification conditions, Group 1b cryptoassets must be designed to be redeemable for a predefined amount of a reference asset or assets, or cash equal to the value of the reference asset(s). In addition, the cryptoasset arrangement must include a sufficient pool of reserve assets to ensure the redemption claims of cryptoasset holders can be met. Aside from these common elements, Group 1b cryptoassets may be structured in a variety of different ways. Banks that have banking book exposures to Group 1b cryptoassets must analyse their specific structures and identify all risks that could result in a loss. Each credit risk must be separately capitalised by banks using the credit risk standards set out in [CRE]. Paragraphs [SCO60.32] to [SCO60.39] below describe various ways in which credit risks may arise from banks' exposures to Group 1b cryptoassets and the capital requirements that would apply in each case. The list is not exhaustive, and it is the responsibility of banks to comprehensively assess and document the full range of risks arising from each of its exposures to Group 1b cryptoassets.

60.32 . If the reference asset for a Group 1b cryptoasset gives rise to credit risk (eg a bond), banks may suffer a loss from the default of the reference asset's issuer. Banks must therefore include in credit RWA the RWA that would apply under [CRE] to a direct holding of the reference asset. If the reference asset gives rise to foreign exchange or commodities risk (eg foreign currency denominated financial assets or physical commodities), banks must calculate market RWA for the exposure equal to the market RWA that would apply under [RBC20.9](1) to a direct holding of the underlying traditional asset.

60.33 For Group 1b cryptoassets that reference a pool of traditional assets, banks must apply the requirements applicable to equity investments in funds (see [CRE60]) to determine the RWA applicable for a direct holding of the referenced pool of traditional assets, as required in [SCO60.32] above. The look-through approach and the mandate-based approach of [CRE60] are available for cryptoassets that fulfil all requirements for these approaches. Otherwise, the fall-back approach (ie a 1250% risk weight) must be applied.

60.34 . Group 1b cryptoassets must be redeemable and if the entity that performs the redemption function (the "redeemer") fails, the cryptoassets may become worthless. The capital treatment[7] of banks' exposures to the redeemer depends on the nature of the exposures:

(1) If the bank holding the cryptoasset has an unsecured claim on the redeemer in case of default, the bank must calculate credit RWA for its exposure to the redeemer. The credit RWA in this case must be equal to the RWA that would apply under [CRE] to a direct unsecured loan to the redeemer. For this purpose the loan amount should equal the redemption claim (ie peg value) of the cryptoasset.

(2) If the bank holding the cryptoasset has a secured claim on the redeemer in case of default, the bank must calculate credit RWA for its exposure to the redeemer. The credit RWA in this case must be equal to the RWA that would apply under CRE to a direct secured loan to the redeemer. For this purpose the loan amount, before any recognition of credit risk mitigation, should equal the redemption claim (ie peg value) of the cryptoasset. All conditions on the eligibility of collateral for the purposes of recognising credit risk mitigation set out in [CRE] apply.

Footnotes

[7] *The capital requirements outlined in this section relate to the calculation of credit RWA. The sections of [SCO60] relating to market risk RWA note that credit RWA must be calculated for instruments in the trading book that give rise to credit risk as a result of potential default of the redeemer.*

60.35 Certain Group 1b cryptoassets may be structured to avoid the cryptoasset holders being exposed to the credit risk (either directly or indirectly) of the redeemer. Banks are not required to calculate credit RWA in respect of the risk outlined in [SCO60.34] above if the following conditions are met:

(1) The underlying reserve assets are held in a bankruptcy remote special purpose vehicle (SPV) on behalf of the holders of cryptoassets who have direct claims on the underlying reserve asset(s).

(2) The bank has obtained an independent legal opinion for all laws relevant to involved parties, including the redeemer, the SPV and custodian, affirming that relevant courts would recognise underlying assets held in a bankruptcy remote manner as those of the cryptoasset holder.

60.36 . Group 1b cryptoassets may be structured such that only a subset of holders ("members") are allowed to transact directly with the redeemer to redeem the cryptoasset. Holders that cannot transact directly with the redeemer ("non-member holders") are therefore reliant on the members for the cryptoassets to maintain their value relative to the reference asset. This type of structure itself may include variants, for example:

(1) The members may issue a legally binding commitment to buy cryptoassets from non-member holders at a price equal to the reference asset(s).

(2) The members may not make a commitment, but may be incentivised to purchase the cryptoassets from non-member holders because they know they can exchange them with the redeemer for cash/assets (as long as the redeemer does not fail).

60.37 Banks that are members of cryptoasset arrangements as described in [SCO60.36] above ("member banks"), must calculate risk weighted assets for their own cryptoasset holdings in the same way as required for holders in cryptoassets arrangements in which all holders can deal directly with the redeemer (ie as set out in [SCO60.34] to [SCO60.35] above). In addition, member banks may be exposed to the risk that the redeemer fails and they are committed to purchase cryptoassets from non-member holders. In such cases, a member bank must also include the RWA that would apply if the bank held all of the cryptoassets that it could be obliged to purchase (ie as set out in [SCO60.36](1) above). Even if there is no legal obligation for a member bank to purchase cryptoassets from non-member holders, banks and supervisors must consider whether in practice the member bank would be obliged to step-in and purchase them in order to satisfy the expectations of non-member holders and protect the bank's reputation. Where such step-in risk exists, banks must include within RWA the amount that would apply if legally binding commitments have been made. Exceptions would only be made if the bank can demonstrate to the supervisor that such step-in risk does not exist.

60.38 The risks to bank holders of cryptoassets that cannot deal directly with the redeemer (ie non-member holders) depend on whether the members have committed to purchase cryptoassets from all non-member holders in unlimited amounts (ie they have made a standing and irrevocable offer to purchase all outstanding cryptoassets from non-member holders):

(1) If members have committed to buy cryptoassets in unlimited amounts, the non-member holders are exposed to: (i) the risk arising from the changing value or potential default of the reference asset; and (ii) the risk that all members default, leaving non-member holders with no way to redeem their cryptoassets. When banks are non-member holders they must sum the RWA calculated for the two risks. The first risk must be calculated as the RWA that would arise from a direct exposure to the underlying (see [SCO60.32]). The calculation of the RWA for the default of the members

is more complex given that there may potentially be multiple members that have made commitments to purchase the cryptoassets (ie the holder can choose whether to sell the cryptoasset to any one of a number of members). If there is just one member, the RWA must be calculated as the cryptoasset holding multiplied by the risk weight applicable to an unsecured loan to the member. If there are multiple members, the risk weight to be used must be the risk weight that would be applicable to an unsecured loan to the member with the highest credit rating (ie lowest risk weight).[8]

(2) If members have not committed to purchase cryptoassets in unlimited amounts from all non-member holders, the latter are exposed to: (i) the risk arising from the changing value or potential default of the reference asset; (ii) the risk that all the members default, leaving non-member holders with no way to redeem their cryptoassets assets; and (iii) the risk that the redeemer defaults (because if it failed, the members would no longer have the incentive to purchase the cryptoassets from the non-member holders). In such cases, the non-member bank holder must include in RWA the sum of RWA for all three separate exposures. The RWA for the first two risks must be calculated in the same way as described in (1) above. The RWA for the third risk must be calculated as the RWA that would arise from a direct loan to the redeemer.

Footnotes

[8] *For example, consider the situation in which there is only one member and it has a high credit rating (and therefore a low risk weight). Its low risk weight should be used to determine the credit risk of non-member holders. Now consider an additional member is added that has a low credit rating (and therefore a high risk weight). The addition of this new member does not increase the risk to non-member holders (in fact it decreases it by giving them more options for redeeming their assets). Thus, the low risk weight of the first member can continue to be used to determine the credit risk to non-member holders.*

60.39 Group 1b cryptoassets, including those that can be redeemed for traditional instruments that are included on the list of eligible financial collateral, are not eligible forms of collateral in themselves for the purposes of recognition as credit risk mitigation. This is because, as outlined above, the process of redemption may add counterparty risk that is not present in a direct exposure to a traditional asset.

Minimum capital requirements for market risk for Group 1 cryptoassets

60.40 This section describes how the minimum risk-based capital requirements for market risk ([MAR]) are to be applied to Group 1 cryptoasset exposures under the Simplified Standardised Approach ([MAR40]), the Standardised Approach ([MAR20] to [MAR23]), and the Internal Models Approach ([MAR30] to [MAR33]).

Application of the Simplified Standardised Approach to Group 1 cryptoassets

60.41 When calculating market risk capital requirements for Group 1 cryptoassets under the Simplified Standardised Approach, as defined in [MAR40], banks must apply the following specifications:

(1) All instruments, including derivatives and off-balance sheets positions that are affected by changes in Group 1 cryptoassets prices must be included;

(2) Banks will first have to express each Group 1 cryptoasset position in terms of their quantity, then convert at the current spot price into the bank's reporting currency;

(3) Banks must consider for Group 1 cryptoassets the same risk classes as the one used for traditional assets they digitally represent (ie interest rate risk, equity risk, FX risk

and commodities risk), as defined in [MAR40.3] to [MAR40.73].

(4) Banks must consider for Group 1 cryptoassets the same treatment for options as the one defined for traditional assets they digitally represent (see [MAR40.74] to [MAR40.86]).

(5) Netting and hedging are recognised between Group 1a cryptoassets and the traditional assets they digitally represent, and both must be mapped to the same risk class. Netting and hedging are recognised between Group 1b cryptoassets and the traditional asset that the cryptoasset references, and both must be mapped to the same risk class.

(6) If present in a Group 1b cryptoasset, the risk of default of the redeemer and the risks arising when intermediaries perform the redemption function should be treated in line with the minimum risk-based capital requirements for credit risk.

Application of the Standardised Approach to Group 1 cryptoassets

60.42 When calculating market risk capital requirements for Group 1 cryptoassets under the Standardised Approach, as defined in [MAR20] to [MAR23], banks must apply the specifications set out in [SCO60.43] to [SCO60.45] below.

60.43 Group 1 cryptoassets must be mapped to the current risk classes set out in the sensitivities-based method. Specifically:

(1) Each tokenised instrument in Group 1 should be decomposed into the same risk factors as the traditional asset it digitally represents. For the tokenised asset, its sensitivities to the traditional risk factors should be identical to those of the traditional asset it digitally represents within the respective current risk classes.

(2) Each stablecoin instrument in Group 1 should be decomposed into the same risk factors as the traditional asset(s) that it references. Its sensitivities to the traditional risk factors should be identical to those of the traditional asset(s) that it references within the current risk classes.

60.44 For the default risk capital (DRC) requirement, Group 1 cryptoassets should have its gross jump-to-default (JTD) considered as equivalent to those from the traditional asset it digitally represents or references.

60.45 If present in a Group 1b cryptoasset, the risk of default of the redeemer and the risks arising when intermediaries perform the redemption function should be treated in line with the minimum risk-based capital requirements for credit risk.

Application of the Internal Models Approach to Group 1 cryptoassets

60.46 When calculating market risk capital requirements for Group 1 cryptoassets under the Internal Models Approach (IMA), as defined in [MAR30] to [MAR33], banks must apply the specifications set out in [SCO60.47] to [SCO60.51] below.

60.47 To determine the aggregate capital requirement under the IMA banks need to calculate a default risk capital (DRC) requirement according to [MAR33.21] and an aggregate non-DRC requirement according to [MAR33.41]. For the latter, the bank will need to determine an aggregate stressed expected shortfall (SES) capital measure according to [MAR33.17] for the non-modellable risk factors and an aggregate capital requirement for modellable risk factors (IMCC) according to [MAR33.15].

60.48 The use of the IMA for instruments referencing Group 2 cryptoassets is not permitted.

60.49 The capital treatment prescribed for the non-DRC requirement allows mapping of exposures to risk factors as follows:

(1) Each tokenised instrument in Group 1 must be decomposed into the same risk factors as the traditional asset it digitally represents within the respective current risk classes.

(2) Each stablecoin instrument in Group 1 must be decomposed into the same risk factors as the traditional asset(s) that they reference within the respective current risk classes.

60.50 For the DRC requirement, tokenised asset and non-tokenised asset are regarded as different instruments to the same obligor. Similarly, traditional assets referenced by stablecoins and the stablecoin themselves are regarded as different instruments to the same obligor. The DRC requirement must account for different losses in the different instruments based on [MAR33.25]. Differences in instruments should be reflected in LGD estimates. Maturity mismatches between tokenised and non-tokenised assets, and between stablecoins and the traditional assets they reference, need to be captured based on [MAR33.28].

60.51 If present in a Group 1b cryptoasset, the risk of default of the redeemer and the risks arising when intermediaries perform the redemption function must be treated in line with the minimum risk-based capital requirements for credit risk.

Add-on for infrastructure risk for Group 1 cryptoassets

60.52 The technological infrastructure that underlies all cryptoassets, such as the DLT, is still relatively new and may pose various additional risks even in cases where the cryptoassets comply with the Group 1 classification conditions. Therefore, authorities must have the power to apply an add-on to the capital requirement for exposures to Group 1 cryptoassets.

60.53 The add-on for infrastructure risk described above will initially be set as zero but will be increased by authorities based on any observed weakness in the infrastructure used by Group 1 cryptoassets.

Minimum capital requirements for credit and market risk for Group 2 cryptoassets

60.54 Group 2 cryptoassets are divided into:

(1) Group 2a: cryptoassets that meet the hedging recognition criteria set out in [SCO60.55] below. Group 2a cryptoassets are subject to modified versions of the Simplified Standardised Approach or the Standardised Approach to market risk set out in [SCO60.57] to [SCO60.82] below. The treatment permits some recognition of hedging. The Internal Models Approach is not applicable to Group 2a cryptoassets.

(2) Group 2b: cryptoassets that do not meet the hedging recognition criteria. Group 2b cryptoassets are subject to a new conservative treatment set out in [SCO60.83] to [SCO60.86] below, which does not permit banks to recognise hedging. A Group 2 cryptoasset must be classified as Group 2b, unless a bank demonstrates to the supervisor that the cryptoasset meets hedging recognition criteria.

Group 2a hedging recognition criteria

60.55 Group 2 cryptoassets that are assessed to meet all three of the following hedging recognition criteria, will be classified as Group 2a:

(1) The bank's cryptoasset exposure is one of the following:

(a) A direct holding of a spot Group 2 cryptoasset where there exists a derivative or

exchange-traded fund(ETF)/exchange-traded note (ETN) that is traded on a regulated exchange that solely references the cryptoasset.

(b) A derivative or ETF/ETN that references a Group 2 cryptoasset, where the derivative or ETF/ETN has been explicitly approved by a jurisdiction's markets regulators for trading or the derivative is cleared by a qualifying central counterparty (QCCP).

(c) A derivative or ETF/ETN that references a derivative or ETF/ETN that meets criterion (b) above.

(d) A derivative or ETF/ETN that references a cryptoasset-related reference rate published by a regulated exchange.

(2) The bank's cryptoasset exposure, or the cryptoasset referenced by the derivative or ETF/ETN, is highly liquid. Specifically, both of the following must apply:

(a) The average market capitalisation was at least USD10 billion over the previous year.

(b) The 10% trimmed mean of daily trading volume with major fiat currencies is at least USD50 million over the previous year.

(3) Sufficient data is available over the previous year. Specifically, both of the following must apply:

(a) There are at least 100 price observations over the previous year. The price observations must be "real" as defined in the four criteria of [MAR31.12].

(b) There are sufficient data on trading volumes and market capitalisation.

60.56 The capital requirements for Group 2a cryptoassets may be calculated according to:

(1) a modified version of the Simplified Standardised Approach (SSA) in the market risk standard set out in [SCO60.57] to [SCO60.65] below; or

(2) a modified version of the Standardised Approach (SA) in the market risk standard set out in [SCO60.66] to [SCO60.82] below.

Capital requirements Group 2a cryptoassets: simplified standardised approach (SSA)

60.57 For Group 2a cryptoassets, the SSA ([MAR40]) will include a separate risk class with its capital requirement determined based on the specifications set out in [SCO60.58] to [SCO60.65] below.

60.58 All instruments, including derivatives and off-balance sheets positions that are affected by changes in Group 2a cryptoasset prices must be included.

60.59 Banks must first express each Group 2a cryptoasset position in terms of its quantity, and then convert it at the current spot price into the bank's reporting currency.

60.60 When consolidated, positions for each Group 2a cryptoasset in different markets or exchanges must not be offset, meaning those sensitivities will be calculated as separate long and short gross consolidated positions. In addition, only the products listed in [SCO60.55](1) may be used for the purposes of offsetting and for the purposes of calculating the net position set out in [SCO60.61] below. Other products that reference Group 2a cryptoassets are subject to the capital requirements that apply to Group 2b cryptoassets.

60.61 For each Group 2a cryptoasset a net position must be determined based on the following formula:

$$Net\ position_k = \max\left(Long\ position_k, \left|Short\ position_k\right|\right) - 0.65 \cdot \min\left(Long\ position_k, \left|Short\ position_k\right|\right)$$

60.62 The capital requirement for position risk of a Group 2a cryptoasset will be 100% of its respective net position.

60.63 The total capital requirement for position risk consists of the simple sum of all Group 2a cryptoasset capital requirements.

60.64 Options with a Group 2a cryptoasset as their underlying asset must be treated under the scenario approach, in accordance with [MAR40.81] to [MAR40.86], using ±100% for the underlying price change and ±100% for the relative volatility change.

60.65 The Group 2a risk class total capital requirement must be aggregated in accordance with [MAR40.2]. Instead of the scaling factors in [MAR40.2], a scaling factor of 1 shall apply to the Group 2a risk class total capital requirement.

Capital requirements Group 2a cryptoassets: standardised approach (SA)

60.66 For Group 2a cryptoassets the SA ([MAR20] to [MAR23]) will include a separate risk class with its capital requirement determined based on the specifications set out in [SCO60.67] to [SCO60.82] below.

60.67 All risk factors, including those related to derivatives and off-balance sheets positions that are affected by changes in Group 2a cryptoasset prices must be included.

60.68 Banks must first express each Group 2a cryptoasset position in terms of its quantity, and then convert it at their current spot price into the bank's reporting currency.

60.69 When consolidated, sensitivities for each Group 2a cryptoasset in different markets or exchanges must not be offset, meaning those sensitivities will be calculated as separate long and short gross consolidated sensitivities. In addition, only the products listed in [SCO60.55](1) may be used for the purposes of offsetting and for the purposes of calculating the net capital set out in [SCO60.71] to [SCO60.82] below. Other products that reference Group 2a cryptoassets are subject to the capital requirements that apply to Group 2b cryptoassets.

60.70 The computation of the sensitivities-based method for Group 2a cryptoassets includes new specifications of delta, vega and curvature risk factors. The sensitivity definitions are also extended to include that of Group 2a cryptoassets. Finally, a new bucket structure is introduced, composed of multiple buckets, one for each Group 2a cryptoasset, containing only its respective sensitivities.

60.71 : the sensitivity is measured by changing the Group 2a cryptoasset spot price by 1 percentage point (ie 0.01 in relative terms) and dividing the resulting change in the market value of the instrument V by 0.01 (ie 1%) as follows, where:

(1) k is a given Group 2a cryptoasset;

(2) CRYPTO(G2a)k is the market value of the Group 2a cryptoasset k; and

(3) Vi is the market value of instrument i as a function of the price of the Group 2a cryptoasset k.

$$s_k = \frac{V_i(1.01 \cdot CRYPTO(G2a)_k) - V_i(CRYPTO(G2a)_k)}{0.01}$$

60.72 : the option-level vega risk sensitivity to a given Group 2a cryptoasset must be determined as prescribed by [MAR21.25].

60.73 : the new risk class will comprise "n" buckets, where each bucket corresponds to the aggregate positions in a specific Group 2a cryptoasset; this is reflected in the following tables.

Delta cryptoasset buckets and risk weights		
Bucket number	*Group 2a cryptoasset*	*Risk weight*
1	Cryptoasset X_1	100%
...	...	...
n	Cryptoasset X_n	100%

Vega cryptoasset buckets and risk weights		
Bucket number	*Group 2a cryptoasset*	*Risk weight*
1	Cryptoasset X_1	100%
...	...	...
n	Cryptoasset X_n	100%

60.74 : Delta sensitivities must be determined based on a risk factor structure ([MAR21.13]) considering two dimensions[9]:

(1) Exchange; and

(2) time to maturity, at the following tenors: 0 years, 0.25 years, 0.5 years, 1 year, 2 years, 3 years, 5 years, 10 years, 15 years, 20 years and 30 years.

Footnotes

[9] *That is, distinct risk factors need to be considered for identical contracts traded on different exchanges or at different tenors, so that no perfect offsetting is permitted between risk factors arising from different exchanges or different tenors.*

60.75 For vega sensitivities, no differentiation by exchange or underlying maturity is considered. Group 2a cryptoasset vega risk factors are defined along one dimension, the maturity of the option, mapped to one or more of the following tenors: 0.5 years, 1 year, 3 years, 5 years and 10 years.

60.76 In order to calculate the delta (or vega) capital requirements for a single bucket b .
$\rho_{kl} = 94\%$

60.77 The delta capital requirement, K, for a single bucket b is calculated as follows:

$$K_b = \sqrt{\max\left(0, \sum_k WS_k^2 + \sum_k \sum_{k \neq l} \rho_{kl} WS_k WS_l\right)}$$

60.78 The delta capital requirement for the Group 2a cryptoasset risk class is , taking into account that there is no recognition of diversification between different Group 2a cryptoassets.
$\sum_b K_b$

60.79 : for the curvature risk capital requirement, the delta buckets specified above must be used. The curvature sensitivities must be calculated by shifting all tenors in parallel (ie no term structure decomposition is required). For calculating the net curvature risk capital requirement CVR for the risk factor k for the Group 2a cryptoasset, the curvature risk weight, which is the size of a shock to the given risk factor, is a relative shift equal to the delta risk weight.

60.80 For aggregating curvature risk positions within a bucket, the following formula must be used:

$$K_b = \max\left(K_b^+, K_b^-\right), where$$
$$K_b^+ = \sum_k \left|CVR_k^+\right|$$
$$K_b^- = \sum_k \left|CVR_k^-\right|$$

60.81 Curvature risk cannot be diversified across buckets. The total curvature risk capital across the entire portfolio is .
$\sum_b K_b$

60.82 Group 2a cryptoassets are not subject to the DRC capital requirement. In case of a stablecoin included in Group 2a, the risk of default of the redeemer and the risks arising when intermediaries perform the redemption function must be treated in line with the minimum risk-based capital requirements for the credit risk (CRE) section.

Capital requirements Group 2b cryptoassets

60.83 There is no separate trading book and banking book treatment for Group 2b cryptoassets. The conservative treatment is intended to capture both credit and market risk, including credit valuation adjustment (CVA) risk. For consistency, the RWA calculated under this approach must all be reported as part of the bank's credit RWA. In addition to direct exposures, the conservative prudential treatment set out in [SCO60.84] to [SCO60.86] below also applies to:

(1) Funds of Group 2b cryptoassets (eg Group 2b cryptoasset ETFs) and other entities, the material value of which is primarily derived from the value of Group 2b cryptoassets.

(2) Equity investments, derivatives or short positions in the above funds or entities.

60.84 For each separate Group 2b cryptoasset to which they are exposed, banks must apply a risk weight of 1250% to the greater of the absolute value of the aggregate long positions and the absolute value of the aggregate short positions in the cryptoasset. That is, RWA for each separate cryptoasset to which the bank is exposed is calculated as follows:

$$\text{RWA} = \text{RW} \cdot \max\left[\left|\text{Long exposure}\right|, \left|\text{Short exposure}\right|\right]$$

60.85 For each cryptoasset derivative (ie a derivative with a Group 2b cryptoasset as the underlying asset), the exposure value used in the above formula is the value of its underlying cryptoassets. For leveraged derivatives (ie a derivative that returns a multiple of the value of the underlying), the exposure value of the underlying position must be adjusted upward to take account of the leverage. The exposure value calculated according to this paragraph can be capped at the maximum possible loss on the cryptoasset derivative.

60.86 The application of the 1250% risk weight set out in [SCO60.84] will ensure that banks are

required to hold minimum risk-based capital at least equal in value to their Group 2b cryptoasset exposures. For simplicity, the formula also applies the 1250% risk weight to short positions. Theoretically, short positions and certain other types of exposures could lead to unlimited losses. Thus, in some circumstances, the formula could require capital that is insufficient to cover potential future losses. Banks will be responsible for demonstrating the materiality of these risks under the supervisory review of cryptoassets and whether risks are materially underestimated. Supervisors will be responsible for considering an additional capital charge in the form of a Pillar 1 add-on in cases where banks have material exposures to short positions in cryptoassets or to cryptoasset derivatives that could give rise to losses that exceed the capital required by the 1250% risk weight. In those cases, the capital add-on will be calibrated by requiring banks to calculate aggregate capital requirements under the Committee's market risk framework (applying a 100% risk weight for delta, vega, and curvature) and Basic CVA risk framework (BA-CVA) and to use this amount if the result is higher than the requirement based on a 1250% risk weight.

Minimum capital requirements for Credit Valuation Adjustment (CVA) risk

60.87 This section describes how the minimum risk-based capital requirements for CVA risk ([MAR]) are to be applied to cryptoasset derivatives exposures and material and fair-valued securities financing transactions (SFTs) referencing cryptoassets, as described in [MAR50].

Group 1a (tokenised traditional assets)

60.88 Derivatives and SFTs on Group 1a cryptoassets will generally be subject to the same rules to determine CVA RWA as non-tokenised traditional assets (ie the rules set out in the market risk standard [MAR50]). In other words, if a bank holds a derivative or an SFT on a tokenised asset having a price close to the traditional asset and being subject to CVA risk as set out in [MAR 50], it will be reflected in the CVA risk charge in the same way as a derivative or SFT on the non-tokenised traditional asset.

60.89 Banks must assess the tokenised traditional asset itself against the rules set out in [MAR50]. Qualification for a given treatment cannot be derived from the respective traditional (non-tokenised) asset. This requirement of individual assessment includes, but is not limited to, the liquidity characteristics. Different liquidity characteristics between the traditional (non-tokenised) asset and the tokenised asset could result in a higher basis risk between the two. In case of insufficient data availability to model the impact of these different liquidity characteristics on their market values, especially of the exposure underlying CVA, the SA-CVA cannot be applied for calculating CVA risk, ie such tokenised assets are subject to the BA-CVA.

Group 1b cryptoassets (cryptoassets with stabilisation mechanisms)

60.90 Derivatives on Group 1b cryptoassets will be subject to the same rules to determine CVA RWA as non-tokenised traditional assets (ie the rules set out in the market risk standard [MAR50]).

Group 2a cryptoassets

60.91 Group 2a cryptoassets will be only subject to the rules set out in the market risk standard [MAR50.1] to [MAR50.26]. The use of SA-CVA is not permitted to be used for derivatives and SFTs referencing Group 2a cryptoassets.

Group 2b cryptoassets

60.92 The treatment of CVA risk for Group 2b cryptoassets is covered in [SCO60.83] to [SCO60.86] above.

Minimum capital requirements for Counterparty Credit risk (CCR)

60.93 This section describes how the minimum risk-based capital requirements for counterparty credit risk (CCR) are to be applied to derivatives referencing cryptoassets.

60.94 For SFTs, banks must apply the comprehensive approach formula set out in the credit risk mitigation section of the standardised approach to credit risk (ie [CRE22.45] to [CRE22.65]). As noted in [SCO60.30], only Group 1a cryptoassets that are tokenised versions of the instruments included on the list of eligible financial collateral set out in [CRE22] may qualify for recognition as eligible collateral. Group 1b, Group 2a and Group 2b cryptoassets are not eligible forms of collateral in the comprehensive approach and therefore when banks receive them as collateral they will receive no recognition for the purposes of the net exposure calculation to the counterparty. As with all non-eligible collateral, banks that lend Group 1b, Group 2a or Group 2b cryptoassets as part of an SFT must apply the same haircut that is used for equities that are not traded on a recognised exchange (ie a haircut of 25%).

Group 1a (tokenised traditional assets)

60.95 Derivatives on Group 1a cryptoassets will generally be subject to the same rules to determine CCR as non-tokenised traditional assets (ie the rules set out in [CRE50] to [CRE56]), which includes the Internal Models Method (IMM), where the same requirements apply for tokenised assets as for traditional assets.

60.96 For the cases described in [SCO60.89] for CVA risk, especially in presence of significant valuation differences between the traditional and the tokenised asset and in presence of significant basis risk, there could be limitations to apply the IMM in case of missing data or too short history or in presence of data quality problems, which then requires to apply the SA-CCR as described below for Group 2a cryptoassets.

Group 1b cryptoassets (cryptoassets with stabilisation mechanisms)

60.97 Derivatives on Group 1b cryptoassets will be subject to the same rules to determine CCR RWA as non-tokenised traditional assets (ie the rules set out in the credit risk standards [CRE50] to [CRE56]).

Group 2a cryptoassets

60.98 Derivatives on Group 2a cryptoassets will be subject to the SA-CCR (ie the rules set out in the credit risk standard [CRE52]), amended by the following:

(1) The replacement cost (RC) takes legally enforceable netting of all transaction types in the netting set into account, which may include derivatives on Group 2a cryptoassets.

(2) In order to calculate the potential future exposure (PFE) add-on, a new asset class "crypto" will be created in the SA-CCR.

(a) The mathematical structure for calculating the PFE add-on for this asset class will be in line with the structure used in the foreign exchange asset class, but with different parameters.

(b) There are separate hedging sets for each crypto currency priced in applicable fiat currencies or in another Group 2a crypto currency.

(c) The supervisory factor calibrated in line with those for traditional assets in SA-

CCRwill be 32% for all cryptocurrency-fiat currency and cryptocurrency-cryptocurrency pairs, and the supervisory option volatilities will equal 120%.

(d) The calculation of the adjusted notional will be set to the cryptoasset's notional expressed in the domestic fiat currency of each bank. For the case of a cryptocurrency priced in another cryptocurrency, the larger of the two adjusted notionals will apply.[10]

(e) The calculation of the supervisory delta adjustment and the maturity factor will be the same as for the other asset classes.

(f) The aggregation of the hedging sets PFE add-ons of class "crypto" will be the same as for the other asset classes by summing up.

Footnotes

10 *If pairs to the domestic currency are not liquidly traded, the most liquid fiat currency needs to be taken with FX spot rates against the domestic fiat currency.*

Group 2b cryptoassets

60.99 For the purpose of calculating counterparty credit risk for derivative exposures that have Group 2b cryptoassets as the underlying or that are priced in units of a Group 2b cryptoasset, the exposure will be the Replacement Cost (RC)[11] plus the Potential Future Exposure (PFE), both multiplied by the alpha factor specified in [CRE52.1], where the PFE is to be calculated as 50% of the gross notional amount. When calculating the RC, netting is permitted within eligible and enforceable netting sets only between exposures to the same Group 2b cryptoassets. Netting sets containing both derivatives related to Group 2b cryptoassets and other asset transactions, must be split into two: one containing the derivatives related to cryptoassets; and one containing derivatives related to the other asset transactions. When calculating the PFE for Group 2b cryptoassets, the 50% of the gross notional amount must be applied per transaction - Group 2b cryptoassets must not form part of any hedging set.

Footnotes

11 *The replacement cost is subject to a floor of zero.*

Minimum capital requirements for operational risk

60.100 The operational risk resulting from cryptoasset activities should generally be captured by the operational risk standardised approach (OPE25) through the Business Indicator – which should include income and expenses resulting from activities relating to cryptoassets – and through the Internal Loss Multiplier – which should include the operational losses resulting from cryptoasset activities. To the extent that operational risks relating to cryptoassets are insufficiently captured by the minimum capital requirements for operational risk and by the internal risk management process of the banks, banks and supervisors should take appropriate steps to ensure capital adequacy and sufficient resilience in the context of supervisory review process ([SRP]). Some key dimensions of this issue elaborated in [SCO60.120] to [SCO60.127].

Minimum liquidity risk requirements

60.101 For the liquidity coverage ratio (LCR) and net stable funding ratio (NSFR) requirements, cryptoasset exposures, including assets, liabilities and contingent exposures, must generally follow a treatment that is consistent with existing approaches for traditional exposures with economically equivalent risks. At the same time, the treatment must also

appropriately reflect the additional risks that may be present with these assets in comparison to traditional assets, and the relative lack of historical data. Accordingly, the treatment of cryptoassets largely relies on the principles and calibrations set forth in the LCR and NSFR standards (see [LCR] and [NSF]). However, these standards require additional clarification and elaboration to address the novel and unique risks associated with cryptoassets.

Treatment as high-quality liquid assets (HQLA)

60.102 Group 1a cryptoassets that are a tokenised version of HQLA as defined in [LCR30.40] to [LCR30.47] may only be considered as HQLA to the extent both the underlying assets in their traditional form and the tokenised form of the assets satisfy the characteristics of HQLA in [LCR30.2] to [LCR30.12]. An example of such a Group 1a cryptoasset could be a tokenised bond that meets these HQLA eligibility criteria and temporarily resides on a distributed ledger to facilitate transfer.
Footnotes

[12] *Note that to be considered in the LCR's stock of HQLA, these assets must also satisfy the operational requirements in [LCR30.13] to [LCR30.28].*

60.103 Group 1b and Group 2 cryptoassets, by contrast, must not be considered HQLA.

General considerations for the application of the LCR and NSFR frameworks

60.104 The appropriate classification and calibration of LCR outflow and inflow rates and NSFR available stable funding (ASF) and required stable funding (RSF) factors of cryptoassets and cryptoliabilities depend on factors such as the structure of the cryptoasset or cryptoliability, its commercial function in practice and the nature of a bank's exposure to the cryptoasset or cryptoliability.

60.105 In general, exposures involving Group 1a cryptoassets and cryptoliabilities must be treated the same as exposures involving their equivalent non-tokenised traditional assets and liabilities, including the assignment of inflows, outflows, RSF factors and ASF factors.

60.106 As set out in [SCO60.107] to [SCO60.112] below, the LCR and NSFR treatment of exposures involving cryptoassets and cryptoliabilities varies according to whether they are:

(1) Tokenised claims on a bank.

(2) Stablecoins.

(3) Other cryptoassets.

60.107 . Group 1a tokenised claims on a bank must be treated as an unsecured funding instrument when they are: (i) issued by a regulated and supervised bank; (ii) represent a legally binding claim on the bank; (iii) redeemable in fiat currency at par value; and (iv) have a stable value supported by the creditworthiness and asset-liability profile of the issuing bank rather than a segregated pool of assets. The treatment as an unsecured funding instrument is subject to the following considerations:

(1) The maturity of the claim on a bank must be determined based upon the contractual redemption rights available to the holder.

(2) For liabilities from own-issued tokenised claims on a bank:

(a) The bank must assign LCR outflow rates and NSFR ASF factors based on the earliest date upon which the liability could be redeemed and the counterparty

type of the holder, in accordance with the treatment of retail funding and unsecured wholesale funding in [LCR40] and [NSF30].

(b) To the extent the issuing bank can identify, at all times, the holder of the cryptoasset, then the bank must apply the applicable outflow rate and ASF factor based on the counterparty classification of the funds provider. However, the issuing bank must not treat the liabilities associated with their cryptoassets as stable retail deposits. If the issuing bank is unable to identify, at all times, the holder of the cryptoasset, it must treat the liability as unsecured wholesale funding provided by other legal entity customers (see [LCR40.42]).

(c) Tokenised claims on a bank that are used primarily as a means of payment and created as part of an operational relationship between the issuing bank and its wholesale customers must follow the categorisation methodology in [LCR40.26] to [LCR40.35]. These liabilities are not eligible for the lower outflow rate specified in [LCR40.36].

(3) When a bank holds another bank's issuance of such a tokenised liability:

(a) The holder must not recognise inflows in the LCR if the cryptoasset is not redeemable within 30 days.

(b) The holder must not recognise inflows in the LCR and must assign a minimum RSF factor of 50% in the NSFR if the cryptoasset is held for operational purposes, in alignment with [LCR40.89] and [NSF30.29]. The holder may recognise inflows in the LCR and an RSF factor of 15% in the NSFR if the cryptoasset is not held for operational purposes, in alignment with [LCR40.89] and [NSF30.28](2).

(4) Notwithstanding the clarifications above, supervisors must apply more stringent LCR and NSFR treatment if, having considered the features and liquidity risk profiles of a tokenised claim on a bank, they conclude that there may be additional liquidity risk inherent in a given liability (eg if some characteristics of the cryptoasset may increase the propensity of a holder to seek redemption during a period of stress, or alternatively constrain a holder from redeeming its funds, etc.). For example, this conclusion may be based upon factors including, but not limited to, the technical design of the liability (eg reliance on non-regulated entities as wallet providers or third-party blockchain operators and usage characteristics of stablecoin implementations, etc.) and the local circumstances of the banking sector.

60.108 . Group 1b cryptoassets, and certain Group 2[13] cryptoassets that are fully collateralised by a segregated pool of underlying assets that do not count toward the bank's stock of HQLA, must be treated similar to securities, subject to the following considerations:

(1) When a bank is an issuer of such a stablecoin and the stablecoin issuance represents a legally binding claim on the bank:

(a) The issuing bank must recognise 100% outflows in the LCR if the stablecoin is redeemable within 30 days. The issuing bank must assign an ASF factor in accordance with [NSF30.10], [NSF30.13] and [NSF30.14] based upon the earliest date upon which the stablecoin could be redeemed.

(b) The issuing bank may recognise reduced outflows in the LCR to the extent the stablecoin is backed by HQLA that is not included in its eligible HQLA amount, but would be unencumbered and freely available to be liquidated upon a redemption of the stablecoin. The reduction in outflows must incorporate the haircuts specified in [LCR30] and must not result in net inflows.

(c) The assets segregated to support the value of the stablecoin must be assigned a

minimum RSF factor for encumbered assets as specified in [NSF30.20] based upon the earliest date upon which the stablecoin could be redeemed.

(2) When a bank holds such a stablecoin on its balance sheet:

(a) As non-HQLA these stablecoins must be subject to at least an 85% RSF in the NSFR and not result in inflows under the LCR.

(b) However, a holder of the stablecoin may recognise inflows in the LCR or a reduced RSF factor in the NSFR to the extent that, similar to a debt security, the stablecoin has a final contractual maturity and the maturity of the stablecoin would result in an inflow of fiat currency within the 30-day or 1-year time horizon. A bank must not assume it exercises an option to redeem the stablecoin prior to any final contractual maturity.

Footnotes

[13] *Stablecoins that do not qualify as Group 1b cryptoassets due to redemption restrictions (ie minimum notice periods) will be included in Group 2. They will, however, be eligible for the treatment outlined in this paragraph provided they satisfy all criteria for classification under Group 1b except the requirement to be redeemable at all times, as specified in [SCO60.12].*

60.109 . The treatment of Group 2 cryptoassets that do not qualify for the treatment outlined in [SCO60.107] and [SCO60.108] above must be aligned with the treatment of other non-HQLA applicable in the LCR and NSFR standards, subject to the following considerations:

(1) A bank that holds other Group 2 cryptoassets or loans denominated in these assets on its balance sheet must assign 100% RSF to the carrying value of these assets in the NSFR and must not recognise any inflows associated with the liquidation, redemption or maturity of these assets.

(2) A bank that has borrowed other Group 2 cryptoassets on an unsecured basis and has an obligation to return these assets within 30 days must apply a 100% outflow rate against the market value of the asset that must be returned to the bank's customer or counterparty, unless the obligation can be settled with certainty from the bank's own unencumbered inventory of the same Group 2 cryptoasset. Similarly, borrowings denominated in other Group 2 cryptoassets must be assigned 0% ASF in the NSFR.

60.110 Supervisors should also consider adjusting outflow rates and stable funding requirements to account for contingent risks that may arise due to a bank's role in issuing or transacting in cryptoassets, such as the risk that a bank may provide non-contractual liquidity support for the redemption of certain stablecoins where it is the issuer or a material service provider to protect its franchise or otherwise avoid negative signalling effects.

60.111 The treatments outlined in [SCO60.108] to [SCO60.110] are not intended to modify the application of the LCR and NSFR frameworks where the types of exposures are not explicitly mentioned. These types of transactions include the following:

(1) Derivatives where the reference asset is a cryptoasset

(2) Secured funding and lending of fiat currency with cryptoassets as collateral

(3) Collateral swaps involving cryptoassets

(4) Commitments to lend cryptoassets

60.112 For the transactions listed in [SCO60.111], the treatment must be aligned with the

existing framework, which generally applies consistently for all non-HQLA instruments.

Leverage ratio requirements

60.113 Consistent with the leverage ratio standard, cryptoassets are included in the leverage ratio exposure measure according to their value for financial reporting purposes, based on applicable accounting treatment for exposures that have similar characteristics. For the cases where the cryptoasset exposure is an off-balance sheet item, the relevant credit conversion factor set out in the leverage ratio framework will apply in calculating the exposure measure. Exposures for cryptoasset derivatives must follow the treatment of the risk-based capital framework.

60.114 For Group 1b cryptoassets, if the bank is involved in the cryptoasset network as a member who is able to deal directly with the redeemer and has promised to purchase cryptoassets from non-member holders, the member also needs to include the total current value of all the off-balance cryptoassets that the bank could be obliged to purchase from holders (as set out in [SCO60.37]).

Large exposures requirements

60.115 For large exposures purposes, the treatment for cryptoassets will follow the same principles as for other exposures as set out in [LEX]. Consistent with the requirements set out in [LEX], cryptoasset exposures that give rise to a credit risk exposure are included in the large exposure measure according to their accounting value as set out in [LEX30.3]. The bank must identify and apply the large exposure limits to each specific counterparty or group of connected counterparties to which it is exposed under the risk-based capital framework. Where the cryptoasset exposes the bank to the risk of default of more than one counterparty, the bank must compute for each counterparty the respective amount to which it is exposed to default risk for large exposure purposes. When the cryptoasset also entails a default risk of reference assets, these will be considered for the purpose of the large exposures framework and the bank must follow the existing large exposures rules applicable to transactions with underlying assets (see [LEX30.41] to [LEX30.53]). Cryptoassets that do not expose banks to default risk (such as physical exposures of gold, other commodities or currencies, and exposures of some forms of cryptoassets with no issuer) do not give rise to a large exposures requirement; however, the counterparty credit risk exposures arising from derivative contracts that reference cryptoassets with no issuer will fall in the scope of the large exposure requirement.

Group 2 exposure limit

60.116 Banks' exposures to Group 2 cryptoassets will be subject to an exposure limit. Banks must apply the exposure limit to their aggregate exposures to Group 2 cryptoassets, including both direct holdings (cash and derivatives) and indirect holdings (eg those via investment funds, ETF/ETN, or any legal arrangements designed to provide exposures to cryptoassets).

60.117 A bank's total exposure to Group 2 cryptoassets should not generally be higher than 1% of the bank's Tier 1 capital and must not exceed 2% of the bank's Tier 1 capital.

60.118 Breaches of the Group 2 exposure limit threshold of 1% should not generally occur and banks must have arrangements in place to ensure compliance with the limit. Any breach that does occur must be communicated immediately to the supervisor and must be rapidly rectified. Until compliance with the 1% limit is restored, the bank's exposures that are in excess of the threshold will be subject to the capital requirements that apply to

Group 2b cryptoasset exposures (as set out in [SCO60.83] to [SCO60.85]). If a bank's exposures exceed 2% of its Tier 1 capital, all Group 2 cryptoasset exposures will be subject to the capital requirements that apply to Group 2b cryptoasset exposures.

60.119 For the purposes of assessing compliance with the Group 2 exposure limit threshold:

(1) Exposures must be measured using the same methodology that applies for determining the Group 2b capital treatment outlined in [SCO60.83] to [SCO60.85]. That is, exposures to all Group 2 cryptoassets (Group 2a and Group 2b) must be measured using the higher of the absolute value of the long and short exposures in each separate cryptoasset to which the bank is exposed. Derivative exposures must be measured using a delta-equivalent methodology.

(2) Tier 1 capital is defined in [CAP10.2].

Bank risk management and supervisory review

60.120 This section describes how the supervisory review process ([SRP]) is to be applied in the case of banks' exposures to cryptoassets. It considers the responsibilities of both banks and supervisors and sets out potential supervisory actions in cases where risks are not sufficiently covered by minimum requirements or bank risk management is insufficient.

Bank risk management

60.121 Cryptoasset activities introduce new kinds of risk and increase certain traditional risks. Banks with direct or indirect exposures or that provide related services to any form of cryptoasset must establish policies and procedures to identify, assess and mitigate the risks (including operational risks, credit risks, liquidity risks including funding concentration risk and market risks) related to cryptoassets or related activities on an ongoing basis. The policies and procedures followed by banks for cryptoasset activities must be informed by existing Basel Committee statements on operational risk management generally and cryptoassets in particular.[14] In accordance with these policies and procedures, banks' operational risk management practices must include, but are not limited to, conducting assessments of these risks (ie how material these risks are, and how they are managed) and taking relevant mitigation measures to improve their operational resilience capabilities (specifically regarding information, communication, and technology (ICT) and cyber risks). The decision to hold cryptoassets (either under trading or banking book) and provide services to cryptoasset operators must be fully consistent with the bank's risk appetite and strategic objectives as set down and approved by the board, as well as with senior management's assessment of the bank's risk management capabilities, in particular for market and counterparty risk (including CVA), liquidity risk (including funding concentration risk) and operational risk.

Footnotes

[14] *See Principles for the Sound Management of Operational Risk; Principles for Operational Resilience; and Statement on Cryptoassets.*

60.122 Considering the particular features of cryptoassets and their markets as well as the potential difficulties in adopting standard arrangements for managing related market risk and counterparty risk including credit valuation adjustment risk, banks must conduct ex-ante a prudent assessment of any cryptoasset exposures they intend to take on and verify the adequateness of existing processes and procedures. The bank must have a sound risk management approach for managing the risks of cryptoassets, including limits and hedging strategies, together with clearly assigned responsibilities for the management of these risks. Particular attention must be paid to the assessment of the

effectiveness of any hedging techniques banks may adopt.

60.123 Banks must also inform their supervisory authorities of their policies and procedures, assessment results, as well as their actual and planned cryptoasset exposures or activities in a timely manner and to demonstrate that they have fully assessed the permissibility of such activities, the associated risks and how they have mitigated such risks.

60.124 The mapping of risks relating to cryptoasset activities to the risk categories of the Basel capital framework (credit risk, market risk, and operational risk in particular) depends on how these risks manifest. Many of the risks introduced or increased by cryptoasset activities are covered by the operational risk framework (eg ICT and cyber risks, legal risks, money laundering and financing of terrorism). A mapping of the technological risks of cryptoassets to Basel risk categories would depend on the circumstances. If the triggering event leading to a loss is due to processes or systems outside of the bank's control and the loss to the bank manifests through the value of a bank position in cryptoassets, such losses would be covered by the credit risk framework (for banking book positions) or the market risk framework (for trading book positions). When losses result from inadequate or failed processes, people or systems of the bank (eg loss of a private cryptographic key by the bank), such losses would be operational losses.

60.125 Risks that banks need to consider in their risk management of cryptoassets activities include, but are not limited to, the following:

(1) Cryptoasset technology risk: Banks must closely monitor the risks inherent to the supporting technology, whether cryptoasset activities are conducted directly or through third parties, including but not limited to:

(a) Stability of the DLT or similar technology network: The reliability of the source code, governance around protocols and integrity of the technology are among key factors related to stability of the network. Key considerations include capacity constraints, whether self-imposed or due to insufficient computing resources; digital storage considerations; scalability of the underlying ledger technology; whether the underlying technology has been tested and had time to mature in a market environment; and robust governance around changes to the terms and conditions of the distributed ledger or cryptoassets (eg so-called 'forks' that change the underlying 'rules' of a protocol). In addition, the type of consensus mechanism (ie for a transaction to be processed and validated) is an important consideration as it relates to the security of the network and whether it is safe to accept a transaction as 'final'.

(b) Validating design of the DLT, permissionless or permissioned: Cryptoassets may rely on a public ('permissionless') ledger, whereby the validation of transactions can be done by any participating agent, or distributed among several agents or intermediaries, which could be unknown to the users. In contrast, a private ('permissioned') ledger restricts and pre-defines the scope of validators, with the validating entities known to the users. On a permissionless ledger, there may be less control of technology and on a permissioned ledger there may be a small group of validators with greater control. Risks related to the validating design of the DLT include the accuracy of the transaction records, settlement failure, security vulnerabilities, privacy/confidentiality, and the speed and cost of transaction processing.

(c) Service accessibility: One of the distinguishing features of cryptoassets is its accessibility to holders of these assets. A holder of cryptoassets is assigned a set

of unique cryptographic keys, which allow that party to transfer the cryptoassets to another party. If those keys are lost, a holder will generally be unable to access the cryptoassets. This increases the possibility of fraudulent activities such as a third-party gaining access to cryptographic keys and using the keys to transfer the cryptoasset to themselves or another unauthorised entity. Furthermore, the risk of a large-scale cyber-attack could leave banks' customers unable to access or recover cryptoasset funds.

(d) Trustworthiness of node operators and operator diversity: Since the underlying technology and node operators facilitate the transfer of cryptoassets and keep records of transactions that take place across the network, their role is essential in designating and sizing the amounts that are held by the holder. Whether nodes are run by a single operator or are distributed among many operators and whether the operators are trustworthy (eg whether the nodes are run by public/ private institutions or individuals) are relevant considerations in third-party risk management.

(2) General information, communication and technology (ICT) and cyber risks: A bank holding cryptoassets may be exposed to additional ICT and cyber risks that include but are not limited to cryptographic key theft, compromise of login credentials, and distributed denial-of-service (DDoS) attacks. The results of ICT failure and cyber-threats may lead to consequences such as unrecoverable loss or unauthorised transfers of cryptoassets.

(3) Legal risks: Cryptoasset activities are still recent and quickly evolving. Thus, their legal framework remains uncertain and banks' legal exposure is heightened, especially in the following dimensions:

(a) Accounting: There may be legal risk arising from a lack of accounting standards for cryptoassets, which could result in fines due to the underpayment of taxes or failure to comply with tax reporting obligations.

(b) Taking control/ownership: There is substantial legal uncertainty around cryptoassets, which could raise questions as to whether banks that take cryptoassets as collateral can take possession in the event of default/margin call.

(c) Disclosure and consumer protection: Banks that issue/redeem or provide dealer or advisor services for cryptoassets can face legal risk around the disclosures they provide for the cryptoassets (including cryptoassets that are considered to be securities), particularly as regulations and laws continue to evolve (eg those around data privacy and data retention).

(d) Uncertain legal status: Jurisdictions can decide (and have decided) to ban cryptoasset mining for a variety of reasons, including its environmental impact. Such developments could reduce the amount of computing power available to secure a network.

(4) Money laundering and financing of terrorism: Banks in their role of providing banking services to Virtual Asset Service Providers (VASP) or to customers involved in Virtual Asset activities, or through engaging in VASP activities themselves need to apply the risk-based approach as set out by the Financial Action Task Force (FATF) for the purposes of Anti-Money Laundering (AML) and Countering the Financing of Terrorism (CFT). Inadequate compliance with AML or CFT laws (including sanctions) and best practices could result in operational losses and reputational damages for banks.

(5) Valuation: Many cryptoassets pose valuation challenges, due (among other things) to their volatility and variable pricing on different exchanges, particularly given that most

of the cryptoassets are currently traded on unregulated marketplaces. These challenges can result in losses for banks in a variety of contexts tied to mispricing due to inadequate operational processes.

Supervisory review

60.126 : Under Pillar 2, supervisors evaluate how well banks assess their capital needs relative to their risks and take measures, where appropriate. As cryptoasset activities are relatively recent and evolving, their related risks are also evolving. Supervisory evaluation is therefore particularly relevant regarding these activities. Thus, supervisors should review the appropriateness of banks' policies and procedures for identifying and assessing those risks and the adequacy of their assessment results. Supervisors should exercise their authority to require banks to address any deficiencies in their identification or assessment process of cryptoasset risks. In addition, supervisors may recommend that banks undertake stress testing or scenario analysis to assess risks resulting from cryptoasset exposures. Such analyses can inform assessments of the bank's capital adequacy.

60.127 Upon the identification of capital inadequacy or shortcomings in bank risk management, the specific supervisory action may vary according to the circumstances. The types of response that supervisors may consider include the following:

(1) Additional capital charges: Supervisors may impose additional capital charges to individual banks for risks not sufficiently captured under the minimum capital requirements for operational risk, credit risk, or market risk. Also, add-ons may be needed in cases where the bank risk management of cryptoassets is considered inadequate.

(2) a Provisioning: Supervisors may request banks to provision for losses related to cryptoassets where such losses are foreseeable and estimable.

(3) Supervisory limit or other mitigation measures: Supervisors may impose mitigation measures on banks, such as requiring a bank to establish an internal limit to contain the risks not adequately identified or assessed in the bank's risk management framework.

Disclosure requirements

60.128 The disclosure requirements for banks' exposures to cryptoassets or related activities must follow the five general guiding principles for banks' disclosures set out in [DIS10]. As such, in addition to the quantitative information described above, banks must provide qualitative information that sets out an overview of the bank's activities related to cryptoassets and main risks related to their cryptoasset exposures, including descriptions of:

(1) business activities related to cryptoassets, and how these business activities translate into components of the risk profile of the bank;

(2) risk management policies of the bank related to cryptoasset exposures;

(3) scope and main content of the bank's reporting related to cryptoassets; and

(4) most significant current and emerging risks relating to cryptoassets and how those risks are managed.

60.129 In accordance with the general guiding principles, banks must disclose information regarding any material Group 1a, Group 1b, Group 2a and Group 2b cryptoasset

exposures on a regular basis, including for each specific type of cryptoasset exposure information on:

(1) the direct and indirect exposure amounts (including the gross long and short components of net exposures);

(2) the capital requirements; and

(3) the accounting classification.

60.130 In addition to the separate disclosure requirements set out above that apply to all Group 1a, Group 1b, Group 2a and Group 2b cryptoassets, banks must include exposures to Group 1 cryptoassets in the relevant existing disclosure templates that apply to traditional assets (eg for credit risk and market risk).

Definitions

60.131 Set out below are definitions of various terms used in [SCO60]:

(1) Cryptoassets: private digital assets that depend primarily on cryptography and distributed ledger or similar technology.

(2) Digital assets: a digital representation in value which can be used for payment or investment purposes or to access a good or service. This does not include digital representations of fiat currencies.

(3) Nodes: typically participants (entities including individuals) in distributed ledger networks that record and share data across multiple data stores (or ledgers).

(4) Operators: typically a single administrative authority in charge of managing a cryptoasset arrangement, performing functions that may include issuing (putting into circulation) a centralised cryptoasset, establishing the rules for its use; maintaining a central payment ledger; and redeeming (withdraw from circulation) the cryptoasset.

(5) Stablecoins: cryptoasset that aims to maintain a stable value relative to a specified asset, or a pool or basket of assets.

(6) Redeemers: entities responsible for exchanging the cryptoasset for the traditional asset. It does not necessarily need to be the same as the entity responsible for organising the issuance of the cryptoasset.

(7) Validators: an entity that commits transactions blocks to the distributed ledger network.

SCO95

Glossary and abbreviations

Updated to include new terminology introduced in the December 2017 Basel III publication with revised implementation date announced on 27 March 2020.

Version effective as of 01 Jan 2023

Updated to include new terminology introduced in the December 2017 Basel III publication with revised implementation date announced on 27 March 2020.

A-IRB	Advanced internal ratings-based
ABCP	Asset-backed commercial paper
ABS	Asset-backed securities
ADC	Acquisition, development and construction
ALCO	Asset and liability management committee
AML	Anti-money-laundering
APL	Actual profit and loss
ARS	Argentine peso
ASF	Available stable funding
AT1	Additional Tier 1
AUD	Australian dollar
AUF	Additional utilisation factor
BA-CVA	Basic approach to credit valuation adjustment risk
BCP	Basel Core Principle
BF	Balance factor
BI	Business indicator
BIC	Business indicator component
BIS	Bank for International Settlements
BOR	Interbank offered rates
bp	Basis points
BRL	Brazilian real
CAD	Canadian dollar
CCBS	Cross-currency basis spread
CCF	Credit conversion factor
CCP	Central counterparty
CCR	Counterparty credit risk
CDD	Customer due diligence
CDO	Collateralised debt obligation
CDR	Cumulative default rate
CDS	Credit default swap
CDX	Credit default swap index
CET1	Common Equity Tier 1
CF	Commodities finance
CFP	Contingency funding plan
CFT	Combating the financing of terrorism
CHF	Swiss franc
CLF	Committed liquidity facility
CLO	Collateralised loan obligation

CM	Clearing member
CMBS	Commercial mortgage-backed securities
CNY	Chinese yuan renminbi
CPR	Conditional prepayment rate
CRO	Chief risk officer
CRM	Credit risk mitigation
CSR	Credit spread risk
CSRBB	Credit spread risk in the banking book
CTP	Correlation trading portfolio
CUSIP	Committee on Uniform Security Identification Procedures
CVA	Credit valuation adjustment
D-SIB	Domestic systemically important bank
DAR	Detailed assessment report
DRC	Default risk charge
DSCR	Debt service coverage ratio
DTA	Deferred tax asset
DTL	Deferred tax liability
DvP	Delivery-versus-payment
EAD	Exposure at default
ECA	Export credit agency
ECAI	External credit assessment institution
ECL	Expected credit loss
ECRA	External credit risk assessment approach
EEPE	Effective expected positive exposure
EL	Expected loss
ELGD	Expected loss-given-default
EONIA	Euro overnight index average
EPC	Engineering and procurement contract
EPE	Expected positive exposure
ES	Expected shortfall
EUR	Euro
Euribor	Euro Interbank Offered Rate
EV	Economic value
EVaR	Economic value-at-risk
EVE	Economic value of equity
F-IRB	Foundation internal ratings-based
FAQ	Frequently asked question
FATF	Financial Action Task Force

FBA	Fall-back approach
FC	Financial component
FSAP	Financial Sector Assessment Program
FSB	Financial Stability Board
FX	Foreign exchange
G-SIB	Global systemically important bank
GAAP	Generally accepted accounting practice
GBP	British pound sterling
GDP	Gross domestic product
GIRR	General interest rate risk
GSE	Government-sponsored entity
HBR	Hedge benefit ratio
HKD	Hong Kong dollar
HLA	Higher loss absorbency
HPL	Hypothetical profit and loss
HQLA	High-quality liquid assets
HVCRE	High-volatility commercial real estate
HY	High yield
IA	Independent amount
IAA	Internal assessment approach
IADI	International Association of Deposit Insurers
IAS	International accounting standard
ICA	Independent collateral amount
ICAAP	Internal capital adequacy assessment process
IDR	Indonesian rupiah
IFRS	International financial reporting standard
IG	Investment grade
ILDC	Interest, leases and dividend component
ILM	Internal loss multiplier
IM	Initial margin
IMA	Internal models approach
IMF	International Monetary Fund
IMM	Internal models method
IMS	Internal measurement systems
INR	Indian rupee
IOSCO	International Organization of Securities Commissions
I/O	Interest-only strips
IPRE	Income-producing real estate

IRB	Internal ratings-based
IRRBB	Interest rate risk in the banking book
ISDA	International Swaps and Derivatives Association
ISIN	International Securities Identification Number
IT	Information technology
JPY	Japanese yen
JTD	Jump-to-default
KRW	Korean won
KS	Kolmogorov-Smirnov
LC	Loss component
LCR	Liquidity Coverage Ratio
LF	Limit factor
LGD	Loss-given-default
LIBOR	London Interbank Offered Rate
LST	Long settlement transaction
LTA	Look-through approach
LTV	Loan-to-value ratio
LVPS	Large-value payment system
M	Effective maturity
MBA	Mandate-based approach
MBS	Mortgage-backed security
MDB	Multilateral development bank
MF	Maturity factor
MIS	Management information system
MNA	Master netting agreement
MPE	Multiple point of entry
MPOR	Margin period of risk
MSR	Mortgage servicing right
MTA	Minimum transfer amount
MTM	Mark-to-market
MXN	Mexican peso
NA	Not applicable
NGR	Net-to-gross ratio
NICA	Net independent collateral amount
NII	Net interest income
NMD	Non-maturity deposit
NMRF	Non-modellable risk factor
NOK	Norwegian krone

NR	Non-rated
NSFR	Net stable funding ratio
NZD	New Zealand dollar
O&M	Operations and maintenance
OBS	Off-balance-sheet
OC	Overcollateralisation
OECD	Organisation for Economic Cooperation and Development
OF	Object finance
OIS	Overnight index swaps
ORC	Operational risk capital requirements
OTC	Over-the-counter
P&L	Profit and loss
PD	Probability of default
PF	Project finance
PFE	Potential future exposure
PLA	Profit and loss attribution
PONV	Point of non-viability
PSE	Public sector entity
PV	Present value
PVA	Prudential valuation adjustment
QCCP	Qualifying central counterparty
QRRE	Qualifying revolving retail exposures
RC	Replacement cost
RCLF	Restricted-use committed liquidity facility
RFET	Risk factor eligibility test
RMBS	Residential mortgage-backed security
ROSC	Report on the Observance of Standards and Codes
ROU	Right-of-use
RRAO	Residual risk add-on
RSF	Required stable funding
RTPL	Risk-theoretical profit and loss
RUB	Russian ruble
RWA	Risk-weighted assets
S&P	Standard and Poor's
SA	Standardised approach
SA-CCR	Standardised approach for counterparty credit risk
SA-CVA	Standardised approach to credit valuation adjustment risk
SAR	Saudi Arabian riyal

SC	Services component
SCRA	Standardised credit risk assessment approach
SEC-SA	Securitisation standardised approach
SEC-ERBA	Securitisation external ratings-based approach
SEC-IRBA	Securitisation internal ratings-based approach
SEK	Swedish krona
SES	Stressed expected shortfall
SF	Supervisory factor
SFT	Securities financing transaction
SGD	Singapore dollar
SIB	Systemically important bank
SIV	Structured investment vehicle
SL	Specialised lending
SME	Small or medium-sized entity
SPE	Special purpose entity
SPV	Special purpose vehicle
STC	Simple, transparent and comparable
STM	Settled-to-market
TDRR	Term deposit redemption rate
TLAC	Total loss-absorbing capacity
TRS	Total return swap
TRY	Turkish lira
UCITS	Undertakings for collective investments in transferable securities
UL	Unexpected loss
ULF	Undrawn limit factor
USD	United States dollar
VaR	Value-at-risk
VM	Variation margin
WTI	West Texas Intermediate
ZAR	South African rand