Attachment 3

Guidance – Financial Stability Standards for Central Counterparties

Introduction

This guidance is issued in relation to the *Financial Stability Standards for Central Counterparties* (CCP Standards) determined under section 827D(1) of the *Corporations Act 2001* (the Act). The CCP Standards apply to all holders of an Australian Clearing and Settlement (CS) Facility Licence, under Part 7.3 of the Act, that operate a central counterparty. Separate financial stability standards apply to CS facility licensees that operate a securities settlement facility. For the purposes of the CCP Standards, a central counterparty is a CS facility operated by an Australian CS facility licensee where the CS facility licensee interposes itself between counterparties to contracts traded in one or more financial markets, becoming the buyer to every seller and the seller to every buyer, and thereby ensuring the performance of open contracts. Unless the contrary intention appears, obligations on a central counterparty arising from the CCP Standards should be interpreted as being obligations on the CS facility licensee, as operator of the central counterparty.

The objective of this document is to provide guidance to central counterparties to assist in the interpretation and application of the CCP Standards, and to elaborate on matters that the Reserve Bank of Australia (Reserve Bank) considers relevant in meeting the CCP Standards. The guidance contains general information in relation to certain matters concerning the CCP Standards and applicable legislation, but is not intended to be exhaustive. It does not elaborate on all aspects of the CCP Standards, and should therefore be read in conjunction with the text of the CCP Standards to provide appropriate context. The guidance does not itself constitute a standard and is not intended to contain obligations that are binding on central counterparties; nor does it constitute legal advice, and should not be treated as such. The Reserve Bank encourages users to obtain independent professional advice in relation to the CCP Standards and relevant legislation as they apply to the users and their particular circumstances.

Note: This guidance is based largely on the Committee on Payment and Settlement Systems (CPSS) and the Technical Committee of the International Organization of Securities Commissions (IOSCO) Principles for Financial Market Infrastructures *(FMIs) (the Principles).*[1] *The Reserve Bank has, in parts, added to and amended the text of the Principles and associated explanatory notes.*[2]

Standard 1: Legal basis

A central counterparty should have a well-founded, clear, transparent and enforceable legal basis for each material aspect of its activities in all relevant jurisdictions.

1 CPSS-IOSCO (2012), *Principles for Financial Market Infrastructures*, CPSS Publications No 101, Bank for International Settlements, April, available at <http://www.bis.org/publ/cpss101.htm>.

2 A marked-up version of this guidance, indicating where additions and alterations have been made to the text of the Principles, will be made available at <http://www.rba.gov.au/payments-system/clearing-settlement/standards/201212-new-fss-ris/index.html> by end 2012.

Guidance

A robust legal basis for a central counterparty's activities in all relevant jurisdictions is critical to a central counterparty's overall soundness. The legal basis defines, or provides the foundation for relevant parties to define, the rights and obligations of the central counterparty, its participants, and other relevant parties, such as its participants' customers, custodians, money settlement agents and service providers. Most risk management mechanisms are based on assumptions about the manner and time at which these rights and obligations arise through the central counterparty. Therefore, if risk management is to be sound and effective, the enforceability of rights and obligations relating to a central counterparty and its risk management should be established with a high degree of certainty. If the legal basis for a central counterparty's activities and operations is inadequate, uncertain or opaque, then the central counterparty, its participants and their customers may face unintended, uncertain or unmanageable credit or liquidity risks, which may also create or amplify systemic risks.

1.1 A central counterparty should be a legal entity which is separate from other entities that may expose it to risks unrelated to those arising from its function as a central counterparty.

1.1.1 In general, a central counterparty should not provide services that have a distinct risk profile from, and potentially pose material additional risks to, its activity of operating the central counterparty. This may require that the central counterparty provide any such services in a legally and financially separate entity, or take other equivalent action. Where a central counterparty performs, or wishes to perform, functions that, while having a distinct risk profile, are complementary or necessarily ancillary to its activity as a central counterparty, it should consult the Reserve Bank and demonstrate that any potential risks posed to its activity as a central counterparty are appropriately and effectively managed.

1.1.2 The identification of the central counterparty as a separate legal entity is of particular importance in circumstances in which an entity related to the central counterparty is experiencing operational or financial difficulties, including external administration. Related activities that may expose the central counterparty to additional financial risks unrelated to those arising from its function as a central counterparty include banking-like activities or investment management.

1.1.3 The legal separation of the central counterparty may also provide protection to those other activities should the central counterparty itself experience operational or financial difficulties. This Standard does not assume or suggest, however, that legal separation will remove all risks that may arise as a result of operational or financial difficulties faced by a central counterparty or a related entity.

1.2 The legal basis should provide a high degree of certainty for each material aspect of a central counterparty's activities in all relevant jurisdictions.

Legal basis

1.2.1 The legal basis should provide a high degree of certainty for each material aspect of a central counterparty's activities in all relevant jurisdictions.[3] The legal basis consists of the legal framework and the central counterparty's rules, procedures and contracts. The legal framework includes general laws and regulations that govern, among other things, property, contracts, insolvency, corporations, securities, banking, secured interests and liability. In some cases, the legal framework that governs competition and consumer and investor protection may also be relevant. Laws and regulations specific

3 An aspect of a central counterparty's activities is or becomes material if it can be a source of a material risk, especially, but not limited to, credit, liquidity, general business, custody, investment or operational risk.

to a central counterparty's activities include those governing: its authorisation, regulation, supervision and oversight; rights and interests in financial instruments; settlement finality; close out; novation; netting; arrangements for delivery versus payment (DvP), payment versus payment (PvP) or delivery versus delivery (DvD); collateral arrangements (including margin arrangements); default procedures; and the resolution of a central counterparty. A central counterparty should establish rules, procedures and contracts that are clear, understandable and consistent with the legal framework and provide a high degree of legal certainty. A central counterparty also should consider whether the rights and obligations of the central counterparty, its participants and, as appropriate, other parties, as set forth in its rules, procedures and contracts, are consistent with relevant industry standards and market protocols.

Rights and interests

1.2.2 The legal basis should clearly define the rights and interests of a central counterparty, its participants, and, where relevant, its participants' customers in the financial instruments, such as cash and securities, or other relevant assets held in custody, directly or indirectly, by the central counterparty. It is not sufficient for key rights and obligations to be implied. The legal basis should fully protect both a participant's assets held in custody by the central counterparty and, where appropriate, a participant's customer's assets held by or through the central counterparty, from the insolvency of relevant parties and other relevant risks. It should also protect these assets when held at a custodian or linked FMI. In particular, consistent with CCP Standard 13 on segregation and portability, the legal basis should protect the assets and positions of a participant's customers. In addition, the legal basis should provide certainty with respect to: a central counterparty's interests in, and rights to use and dispose of, collateral; a central counterparty's authority to transfer ownership rights or property interests; and a central counterparty's rights to make and receive payments, in all cases, notwithstanding the bankruptcy or insolvency of its participants, participants' customers, or a custodian bank.[4] Also, the central counterparty should structure its operations so that its claims against collateral provided to it by a participant should have priority over all other claims, and the claims of the participant to that same collateral should have priority over the claims of third-party creditors.

Mitigating legal risk

1.2.3 In general, there is no substitute for full legal certainty supported by applicable legislation in all jurisdictions relevant to a central counterparty's activities. However, in some practical situations, such as might arise where a central counterparty offers services outside its home jurisdiction, or where participants are located in another jurisdiction to that of the central counterparty, it may not be possible, notwithstanding an independent legal opinion, to be confident of full legal certainty for all aspects of a central counterparty's operations. In this case, a central counterparty should investigate steps to mitigate its legal risk through the selective use of alternative risk management tools that do not suffer from the legal uncertainty identified. These could include, in appropriate circumstances, participant

4 Collateral arrangements may involve either a pledge or a title transfer, including transfer of full ownership. If a central counterparty accepts a pledge, it should have a high degree of certainty that the pledge has been validly created in the relevant jurisdiction and validly perfected, if necessary. If a central counterparty relies on a title transfer, including transfer of full ownership, it should have a high degree of certainty that the transfer is validly created in the relevant jurisdiction and will be enforced as agreed and not recharacterised, for example, as an invalid or unperfected pledge or some other unintended category of transaction. A central counterparty should also have a high degree of certainty that the transfer itself is not voidable as an unlawful preference under insolvency law. See also CCP Standard 5 on collateral, CCP Standard 6 on margin, and CCP Standard 12 on participant default rules and procedures.

requirements, exposure limits, collateral requirements and prefunded default arrangements. If such controls are insufficient or not feasible, a central counterparty could, as appropriate, apply activity limits, restrict access, or not perform the problematic activity until the legal situation is addressed.

1.3 A central counterparty should have rules, procedures and contracts that are clear, understandable and consistent with relevant laws and regulations.

1.3.1 The operating rules and procedures of a central counterparty play a key role in enabling participants to understand the risks they incur. The rules need to be clear, comprehensive and up to date to facilitate understanding by participants and prospective participants of the risks they can face through participation in the system. Explanatory material written in plain language can aid understanding of the central counterparty's design and processes, thus improving understanding of risks that may arise through participation.

1.3.2 The rules and procedures should describe the roles of participants and the central counterparty and the procedures that will be followed in various circumstances (for example, which parties are to be notified of specific events and the timetables for decision-making and notification). They should make clear the degree of discretion parties are able to exercise in taking decisions that can have a direct effect on the operation of the system. There should be clear processes for changing rules and procedures. The degree of discretion the central counterparty can exercise to make unilateral changes to the rules or procedures, and any period of notice it must give to participants, should be clear.

1.4 A central counterparty should be able to articulate the legal basis for its activities to the Reserve Bank and other relevant authorities, participants and, where relevant, participants' customers, in a clear and understandable way.

1.4.1 One recommended approach to articulating the legal basis for each material aspect of a central counterparty's activities is to obtain well-reasoned and independent legal opinions or analyses. A central counterparty should consider, subject to any restrictions, sharing these legal opinions and analyses with its participants in an effort to promote confidence among participants and transparency in the system. In addition, a central counterparty should seek to ensure that its activities are consistent with the legal basis in all relevant jurisdictions. These jurisdictions could include: those where a central counterparty is conducting business (including through linked FMIs); those where its participants are incorporated, located or otherwise conducting business for the purposes of participation; those where collateral is located or held; and those indicated in relevant contracts.

1.5 A central counterparty should have rules, procedures and contracts that are enforceable in all relevant jurisdictions. There should be a high degree of certainty that actions taken by the central counterparty under such rules and procedures will not be voided, reversed or subject to stays, including in the event that the central counterparty enters into external administration or that one or more of its participants defaults or is suspended.

Settlement finality

1.5.1 There should be a clear legal basis regarding the timing of final settlement of a central counterparty's obligations in order to define when key financial risks are transferred in the system, including the point at which transactions are irrevocable. Settlement finality is an important building block for risk management systems (see also CCP Standard 8 on settlement finality). A central counterparty should consider, in particular, the actions that would need to be taken in the event of a participant's

insolvency. A key question is whether transactions of an insolvent participant would be honoured as final, or could be considered void or voidable by liquidators and relevant authorities. In some countries, for example, so-called 'zero-hour rules' in insolvency law can have the effect of reversing a payment, notwithstanding that it has successfully been processed by a payment system. Because this possibility can lead to credit and liquidity risks, a central counterparty should ensure that the finality of settlement is not affected by the operation of zero-hour rules in any relevant jurisdiction. A central counterparty should ensure that settlement obligations are subject to the protections of the *Payment Systems and Netting Act 1998* (if operating in Australia), or equivalent legislation in other jurisdictions. A central counterparty also should consider the legal basis for the external settlement mechanisms it uses, such as funds transfer or securities transfer systems. The laws of the relevant jurisdictions should support the provisions of the central counterparty's legal agreements with its participants and money settlement agents relating to finality.

Netting arrangements

1.5.2 If a central counterparty has a netting arrangement, the enforceability of the netting arrangement should have a sound and transparent legal basis. In general, netting offsets obligations between or among participants in the netting arrangement, thereby reducing the number and value of payments or deliveries needed to settle a set of transactions. Netting can reduce potential losses in the event of a participant default and may reduce the probability of a default. Netting arrangements should be designed to be explicitly recognised and supported under the law and enforceable against a central counterparty and a central counterparty's failed participants in bankruptcy. In particular, if the central counterparty has arrangements involving the netting of transactions, then it should seek the benefit of the Payment Systems and Netting Act (if operating in Australia), or equivalent legislation in another jurisdiction. Without such legal underpinnings, net obligations may be challenged in judicial or administrative insolvency proceedings. If these challenges were successful, the central counterparty and its participants could face gross exposures and settlement obligations, which in some circumstances could be many multiples of net obligations.

Assumption of risk

1.5.3 Novation, open offer or other similar legal devices utilised by a central counterparty should be founded on a sound legal basis. The nature and scope of the legal device adopted, as well as the point in the clearing process at which the central counterparty assumes risk, must be legally certain and well understood by all participants. In novation (and substitution), the original contract between the buyer and seller is discharged and two new contracts are created: one between the central counterparty and the buyer, and the other between the central counterparty and the seller. The central counterparty thereby assumes the original parties' contractual obligations to each other. In an open offer system, the central counterparty extends an open offer to act as a counterparty to market participants and thereby is interposed between participants at the time a trade is executed. If all pre-agreed conditions are met in an open offer system, there is never a contractual relationship between the buyer and seller. Where supported by the legal framework, novation, open offer and other similar legal devices give market participants legal certainty that a central counterparty is supporting the transaction.

Enforceability

1.5.4 The rules, procedures and contracts related to a central counterparty's operation should be enforceable in all relevant jurisdictions. In particular, the legal basis should support the enforceability of the participant default rules and procedures that a central counterparty would use to handle a defaulting or insolvent participant, especially any transfers and close outs of a direct or indirect participant's assets or positions (see also CCP Standard 12 on participant default rules and procedures). A central counterparty should have a high degree of certainty that actions taken under such rules and procedures will not be voided, reversed or subject to stays, including with respect to the resolution regimes applicable to its participants.[5] Ambiguity about the enforceability of procedures could delay and possibly prevent a central counterparty from taking actions to fulfil its obligations to non-defaulting participants or to minimise its potential losses. The central counterparty should obtain a written and reasoned independent legal opinion as to the enforceability of the central counterparty's arrangements under the laws of each relevant jurisdiction.

1.5.5 A central counterparty should also establish rules, procedures and contracts related to its operations that would be enforceable in the event that the central counterparty had to implement its plans for recovery or orderly wind-down, and in the event of external administration. Where relevant, these should adequately address issues and associated risks resulting from foreign and cross-border participation and interoperability of FMIs. There should be a high degree of certainty that any actions taken by the central counterparty under such rules and procedures would not be voided, reversed or subject to stays. Ambiguity about the enforceability of procedures that facilitate the implementation of the central counterparty's plans for recovery or orderly wind-down, or the resolution of the central counterparty, could delay and possibly prevent the central counterparty or the Reserve Bank and other relevant authorities from taking appropriate actions and hence increase the risk of a disruption to its critical services or a disorderly wind-down of the central counterparty.

Default or suspension of participants

1.5.6 The rules applying in the event of the default or suspension of a participant should be set out in advance: this enhances the certainty of obligations placed on participants and thus minimises the opportunity for surviving participants to challenge their liability; in a default situation, there are likely to be strong incentives to undertake behaviour to minimise any contribution, and this could amplify systemic risks (see CCP Standard 12 on participant default rules and procedures).

External administration

1.5.7 Where a participant or the central counterparty is in external administration or is otherwise facing difficulties, there is scope for instability in the broader financial system. A high degree of certainty in the legal framework concerning such events can help to limit the capacity for such instability.

1.6 A central counterparty conducting business in multiple jurisdictions should identify and mitigate the risks arising from any potential conflicts of law across jurisdictions. A central counterparty should provide the Reserve Bank with a legal opinion that demonstrates the enforceability of its rules and addresses relevant conflicts of law across the jurisdictions in

5 However, rights triggered only because of entry into resolution or the exercise of resolution powers may be subject to stays in some jurisdictions.

which it operates. This should be reviewed on a periodic basis or when material changes occur that may have an impact on the opinion, and updated where appropriate.

Conflicts of law

1.6.1 Legal risk due to conflicts of law may arise if a central counterparty is, or reasonably may become, subject to the laws of various other jurisdictions (for example, when it accepts participants established in those jurisdictions, when assets are held in multiple jurisdictions, or when business is conducted in multiple jurisdictions). In such cases, a central counterparty should identify and analyse potential conflicts of law and develop rules and procedures to mitigate associated risks (see paragraph 1.6.2 on obtaining a legal opinion). For example, the rules governing a central counterparty's activities should clearly indicate the law that is intended to apply to each aspect of its operations. The central counterparty and its participants should be aware of applicable constraints on their abilities to choose the law that will govern the central counterparty's activities when there is a difference in the substantive laws of relevant jurisdictions. For example, such constraints may exist because of jurisdictions' differing laws on insolvency and irrevocability.

Legal opinion

1.6.2 A central counterparty operating in multiple jurisdictions should obtain a well-reasoned, independent legal opinion(s) covering potential conflicts of law, as well as the enforceability of its rules and its ability to satisfy its regulatory obligations in all relevant jurisdictions. Any opinion relevant to the central counterparty's operations in Australia should be shared with the Reserve Bank. At least every two years, the legal opinion obtained under this Standard should be reviewed, updated where appropriate, and where relevant provided to the Reserve Bank. Between periodic reviews, the legal opinion should be reviewed whenever there is a material change to the central counterparty's operational, governance or risk management arrangements or to the legal or regulatory framework governing its activities that may impact on the opinion. Further to such a review, the opinion should be updated where appropriate and provided to the Reserve Bank. Material changes triggering a review of the legal opinion may include changes to: the nature and composition of the central counterparty's membership; its internal organisation or structure; product offerings; or applicable laws or regulations.

Standard 2: Governance

A central counterparty should have governance arrangements that are clear and transparent, promote the safety of the central counterparty, and support the stability of the broader financial system, other relevant public interest considerations and the objectives of relevant stakeholders.

Guidance

Governance is the set of relationships between a central counterparty's owners, board of directors (or equivalent), management, and other relevant parties, including participants, the Reserve Bank and other relevant authorities, and other stakeholders (such as participants' customers, other interdependent FMIs and the broader market). Governance provides the processes through which an organisation sets its objectives, determines the means for achieving those objectives, and monitors performance against those objectives. Good governance provides the proper incentives for a central counterparty's board and management to pursue objectives that are in the interests of its stakeholders and that support relevant public interest considerations.

2.1 A central counterparty should have objectives that place a high priority on the safety of the central counterparty and explicitly support the stability of the financial system and other relevant public interest considerations.

2.1.1 Given the importance of central counterparties and the fact that their decisions can have widespread impact, affecting multiple financial institutions, markets and jurisdictions, it is essential for each central counterparty to place a high priority on the safety of its operations and explicitly support financial stability and other relevant public interests. This is consistent with a central counterparty's obligations under section 821A(aa) of the *Corporations Act 2001*, which states that a CS facility must, to the extent that it is reasonably practicable to do so, not only comply with standards determined by the Reserve Bank under section 827D, but also do all other things necessary to reduce systemic risk. As a further example, in certain over-the-counter (OTC) derivatives markets, industry standards and market protocols have been developed to increase certainty, transparency and stability. If a central counterparty in such markets were to diverge from these practices, it could, in some cases, undermine the market's efforts to develop common processes to help reduce uncertainty. A central counterparty's governance arrangements should also include appropriate consideration of the interests of participants, participants' customers, the Reserve Bank and other relevant authorities, and other stakeholders. Governance arrangements should provide for fair and open access, insofar as this would not be inconsistent with the maintenance of acceptable risk control standards (see CCP Standard 17 on access and participation requirements) or the effective implementation of recovery or wind-down plans, or resolution.

2.2 A central counterparty should have documented governance arrangements that provide clear and direct lines of responsibility and accountability. These arrangements should be disclosed to owners, the Reserve Bank and other relevant authorities, participants and, at a more general level, the public.

2.2.1 Governance arrangements, which define the structure under which the board and management operate, should be clearly and thoroughly documented. These arrangements should include certain key components such as the: role and composition of the board and any board committees; senior management structure; reporting lines between management and the board; ownership structure; internal governance policy; design of risk management and internal controls; procedures for the appointment of board members and senior management; and processes for ensuring performance accountability. Governance arrangements should provide clear and direct lines of responsibility and accountability, particularly between management and the board, and ensure sufficient independence for key functions such as risk management, internal control and audit. These arrangements should be disclosed to owners, the Reserve Bank and other relevant authorities, participants, and, at a more general level, the public.

2.2.2 No single set of governance arrangements is appropriate for all central counterparties and all market jurisdictions. Arrangements may differ significantly because of national law, ownership structure or organisational form. Indeed, a central counterparty may be owned by its participants or by another organisation, may be operated as a for-profit or not-for-profit enterprise, or may be organised as a bank or non-bank entity. While specific arrangements vary, this Standard is intended to be generally applicable to all ownership and organisational structures.

2.2.3 Depending on its ownership structure and organisational form, a central counterparty may need to focus particular attention on certain aspects of its governance arrangements. For instance, a central counterparty that is, or is part of, a for-profit entity may need to place particular emphasis on managing any conflicts between income generation and safety. And a central counterparty that is part of a larger organisation or corporate group should consider any conflicts of interest or other issues that may arise from its relationship to its parent or to other affiliated entities (see CCP Standard 2.9).[6] Where relevant, any cross-border issues should also be appropriately identified, assessed and dealt with in the central counterparty's governance arrangements, both at the central counterparty level and at the level of its parent. A central counterparty's ownership structure and organisational form may also need to be considered in the preparation and implementation of its recovery or wind-down plans or in assessments of its resolvability.

2.3 The roles and responsibilities of a central counterparty's board of directors (or equivalent) should be clearly specified, and there should be documented procedures for its functioning, including procedures to identify, address and manage member conflicts of interest. The board should regularly review both its overall performance and the performance of its individual board members.

2.3.1 A central counterparty's board has multiple roles and responsibilities that should be clearly specified. These roles and responsibilities should include: establishing clear strategic aims for the entity; ensuring effective monitoring of senior management (including selecting its senior managers, setting their objectives, evaluating their performance and, where appropriate, removing them); establishing appropriate compensation policies (which should be consistent with best practices and based on long-term achievements, in particular, the safety of the central counterparty – see paragraph 2.5.2); establishing and overseeing the risk management function and material risk decisions; overseeing internal control functions (including ensuring independence and adequate resources); ensuring compliance with all supervisory and oversight requirements; ensuring consideration of financial stability and other relevant public interests; and providing accountability to the owners, participants and other relevant stakeholders (see CCP Standard 2.8). The means by which the board discharges these responsibilities may vary according to the central counterparty's organisational form. Where a central counterparty forms part of a corporate group, some of the roles and responsibilities of the board may be carried out on a group-wide basis, for instance by the board of the central counterparty's parent company. However, the central counterparty must be able to demonstrate that any such alternative governance arrangements are effective. In particular, the central counterparty should be able to demonstrate that such arrangements uphold its capacity to meet its regulatory and other obligations, and in no way compromise or subordinate the central counterparty's interests to the interests of the group (see CCP Standard 2.9).

2.3.2 Policies and procedures related to the functioning of the board should be clear and documented. These policies include the responsibilities and functioning of board committees. A board would normally be expected to have, among others, a risk committee, an audit committee and a compensation committee, or equivalents (including equivalent committees operating on a group-wide basis). All

6 If a central counterparty is wholly owned or controlled by another entity, the Reserve Bank will also consider the governance arrangements of that entity in assessing the central counterparty's observance of this Standard.

such committees should have clearly assigned responsibilities and procedures.[7] Board policies and procedures should include processes to identify, address and manage potential conflicts of interest of board members. Conflicts of interest include, for example, circumstances in which a board member has material competing business interests with the central counterparty. Further, policies and procedures should also include regular reviews of the board's performance and the performance of each individual member, as well as, potentially, periodic independent assessments of performance.

2.4 The board should comprise suitable members with the appropriate skills and incentives to fulfil its multiple roles. This typically requires the inclusion of non-executive board member(s).

2.4.1 Governance policies related to board composition, appointment and term should also be clear and documented. The board should be composed of suitable members with an appropriate mix of skills (including strategic and relevant technical skills), experience, competence and knowledge of the entity (including an understanding of the central counterparty's interconnectedness with other parts of the financial system). The nature and degree of the skills, experience and expertise required of board members will depend on the size, scope and nature of the business conducted by the central counterparty. Members should also have a clear understanding of their roles in corporate governance, be able to devote sufficient time to their roles, ensure that their skills remain up to date, and have appropriate incentives to fulfil their roles. Members should be able to exercise objective and independent judgement. A central counterparty should be able to demonstrate that its board composition provides a sufficient degree of independence from the views of management. This typically requires the inclusion of non-executive board members, including independent board members.[8] The key characteristic of independence is the ability to exercise objective, independent judgement after fair consideration of all relevant information and views and without undue influence from executives or from inappropriate external parties or interests. The precise definition of independence used by a central counterparty should be specified and publicly disclosed. A central counterparty should also specify and publicly disclose any relevant interests of its board members, as well as any arrangements that it has in place to manage any potential conflicts arising from these interests. Such interests may include relevant business or commercial interests, cross-directorships, shareholdings, or employee relationships. Further, a central counterparty should publicly disclose which board members it regards as independent. The appropriate number of independent non-executive directors on a central counterparty's board will depend on the size, scope and nature of the business conducted by the central counterparty. A central counterparty may also need to consider setting a limit on the duration of board members' terms.

2.5 The roles and responsibilities of management should be clearly specified. A central counterparty's management should have the appropriate experience, mix of skills and integrity necessary to effectively discharge its responsibilities for the operation and risk management of the central counterparty. Compensation arrangements should be structured in such a way as to promote the soundness and effectiveness of risk management.

7 Such committees would normally be composed mainly of – and, if possible, led by – non-executive or independent directors (see also CCP Standard 2.4).

8 Having non-executive members included on a board, for example, may help in balancing considerations of safety with competitiveness and, where applicable, profitability.

Roles and responsibilities of management

2.5.1 A central counterparty should have clear and direct reporting lines between its management and board in order to promote accountability, and the roles and responsibilities of management should be clearly specified. A central counterparty's management should have the appropriate experience, mix of skills and integrity necessary to discharge its responsibilities for the operation and risk management of the central counterparty. Under board direction (or equivalent alternative governance arrangements), management should ensure that the central counterparty's activities are consistent with the objectives, strategy and risk tolerance of the central counterparty, as determined by the board (or equivalent). Management should ensure that internal controls and related procedures are appropriately designed and executed in order to promote the central counterparty's objectives, and that these procedures include a sufficient level of management oversight. Internal controls and related procedures should be subject to regular review and testing by well-trained and staffed risk management and internal audit functions. Additionally, senior management should be actively involved in the risk control process and should ensure that appropriate resources are devoted to the central counterparty's risk management framework.

Compensation

2.5.2 A central counterparty should structure compensation arrangements for management to provide incentives for sound and effective risk management. The central counterparty should consider offering incentives that reward management for effective risk management and the longer-term financial soundness of the facility. Fundamentally, the central counterparty should avoid compensation arrangements that create incentives for management to pursue greater profitability by relaxing risk controls.

2.6 The board should establish a clear, documented risk management framework that includes the central counterparty's risk tolerance policy, assigns responsibilities and accountability for risk decisions, and addresses decision-making in crises and emergencies. Governance arrangements should ensure that the risk management and internal control functions have sufficient authority, independence, resources and access to the board, including through the maintenance of a separate and independent internal audit function.

Risk management governance

2.6.1 Because the board is ultimately responsible for managing a central counterparty's risks, it should establish a clear, documented risk management framework that includes the central counterparty's risk tolerance policy, assigns responsibilities and accountability for risk decisions, and addresses decision-making in crises and emergencies. The board should regularly monitor the central counterparty's risk profile to ensure that it is consistent with the central counterparty's business strategy and risk tolerance policy. In addition, the board should ensure that the central counterparty has an effective system of controls and oversight, including adequate governance and project management processes, over the models used to quantify, aggregate and manage the central counterparty's risks. Board approval should be required for material decisions that would have a significant impact on the risk profile of the entity, such as the limits for total credit exposure and large individual credit exposures. Other material decisions that may require board approval include the introduction of new products, implementation of new links, use of new crisis management frameworks, adoption of processes and templates for

reporting significant risk exposures, and adoption of processes for considering adherence to relevant market protocols. In OTC derivatives markets, central counterparties are expected to adhere to practices or arrangements that have become established market conventions or to act in a manner that does not conflict with such terms, unless the central counterparty has reasonable grounds not to do so and that does not conflict with the market's wider interest. In this regard, where a central counterparty supports a market and is expected to fully adhere to market-wide protocols and related decisions, the central counterparty should be involved in the development and establishment of such standards. It is critical that market governance processes fully reflect the role of the central counterparty in the market. The arrangements adopted by a central counterparty should be transparent to its participants and the Reserve Bank and other relevant authorities.

2.6.2 The board, and governance arrangements more generally, should support the use of clear and comprehensive rules and key procedures, including detailed and effective participant default rules and procedures (see CCP Standard 12). Governance arrangements should ensure that procedures are in place to support the board's capacity to act appropriately and immediately if any risks arise that threaten the central counterparty's viability as a going concern. The governance arrangements should also provide for effective decision-making in a crisis and support any procedures and rules designed to facilitate the recovery or orderly wind-down of the central counterparty.

2.6.3 In addition, the governance of the risk management function is particularly important. It is essential that a central counterparty's risk management personnel have sufficient independence, authority, resources and access to the board to ensure that the operations of the central counterparty are consistent with the risk management framework set by the board. The reporting lines for risk management should be clear and separate from those for other operations of the central counterparty, and there should be an additional direct reporting line to a non-executive director on the board via a chief risk officer (or equivalent). To help the board discharge its risk-related responsibilities, a central counterparty should have a risk committee responsible for advising the board on the central counterparty's overall current and future risk tolerance and strategy, or equivalent. A central counterparty's risk committee should be chaired by a sufficiently knowledgeable individual who is typically independent of the central counterparty's executive management and should typically be composed of a majority of members who are non-executive members. The committee should have a clear and public mandate and operating procedures and, where appropriate, have access to external expert advice.

Model validation

2.6.4 The board should ensure that there is adequate governance surrounding the adoption and use of models, such as for credit, collateral, margining and liquidity risk management systems. A central counterparty should validate, on an ongoing basis, the models and their methodologies used to quantify, aggregate and manage the central counterparty's risks. The validation process should be independent of the development, implementation and operation of the models and their methodologies, and should be subject to an independent review of its adequacy and effectiveness. Validation should include: an evaluation of the conceptual soundness of (including developmental evidence supporting) the models; an ongoing monitoring process that includes verification of processes and benchmarking; and an analysis of outcomes that includes backtesting.

2.7 A central counterparty's operations, risk management processes, internal control mechanisms and accounts should be subject to internal audit and, where appropriate, periodic external

independent expert review. Internal audits should be performed, at a minimum, on an annual basis. The outcome of internal audits and external reviews should be notified to the Reserve Bank and other relevant authorities.

2.7.1 Governance arrangements should establish and provide for appropriate oversight of internal controls and audit. A central counterparty should have sound internal control policies and procedures to help manage its risks. For example, as part of a variety of risk controls, governance arrangements should ensure that there are adequate internal controls to protect against the misuse of confidential information. A central counterparty should also have an effective internal audit function, with sufficient resources and independence from management to provide, among other activities, a rigorous and independent assessment of the effectiveness of a central counterparty's risk management and control processes (see also CCP Standard 3 on the framework for the comprehensive management of risks). Governance arrangements should typically establish an audit committee to oversee the internal audit function. In addition to reporting to senior management, the audit function should have regular access to the board (or equivalent) through an additional reporting line.

2.7.2 A central counterparty should engage independent and appropriately qualified external experts to review aspects of its operations, risk management processes, internal control mechanisms and accounts periodically and as required. The adequacy of and adherence to control mechanisms may also be assessed through regular independent compliance programs. In particular, external reviews may be required if internal audit processes or other internal controls identify potential areas of weakness that require additional external scrutiny and analysis. The outcomes of periodic or ad hoc external reviews should be provided to the Reserve Bank and other relevant authorities on a timely basis, and the central counterparty should advise the Reserve Bank or other relevant authorities as to how it plans to address any areas of weakness identified.

2.8 Governance arrangements should ensure that the central counterparty's design, rules, overall strategy and major decisions reflect appropriately the legitimate interests of its direct and indirect participants and other relevant stakeholders. Governance arrangements should provide for consultation and stakeholder engagement through appropriate forums on operational arrangements, risk controls and default management rules and procedures. Major decisions should be clearly disclosed to relevant stakeholders and, where there is a broad market impact, the public.

2.8.1 A central counterparty's governance arrangements should take into account all relevant stakeholders' interests, including those of its direct and indirect participants, in making major decisions, including those relating to the system's design, rules and overall business strategy. A central counterparty with cross-border operations, in particular, should ensure that the full range of views across the jurisdictions in which it operates is appropriately considered in the decision-making process. Mechanisms for involving stakeholders in decision-making processes may include stakeholder representation on the board (including direct and indirect participants), user committees and public consultation processes. Where appropriate, a central counterparty should consider establishing targeted stakeholder forums that provide opportunities for focused consultation with specific segments of the participant base, or other stakeholders, that have common interests. This might be particularly important where stakeholders vary significantly in size, location or other characteristics. These forums may provide opportunity for stakeholder input on matters such as the central counterparty's operational arrangements, risk controls

and default management rules and procedures. As opinions among interested parties are likely to differ, the central counterparty should have clear processes for identifying and appropriately managing the diversity of stakeholder views and any conflicts of interest between stakeholders and the central counterparty. Without prejudice to local requirements on confidentiality and disclosure, the central counterparty should clearly and promptly inform its owners, participants, other users and, where appropriate, the broader public, of the outcome of major decisions, and consider providing summary explanations for decisions to enhance transparency where it would not endanger candid board debate or commercial confidentiality.

2.9 A central counterparty that is part of a group of companies should ensure that measures are in place such that decisions taken in accordance with its obligations as a central counterparty cannot be compromised by the group structure or by board members also being members of the board of other entities in the same group. In particular, such a central counterparty should consider specific procedures for preventing and managing conflicts of interest, including with respect to intragroup outsourcing arrangements.

2.9.1 Where a central counterparty is part of a wider corporate group, there may be the potential for conflicts to arise between the obligations and interests of the central counterparty and those of other entities in the group (including related functions performed within the same legal entity – see CCP Standard 1.1), or the group as a whole. For example, where a central counterparty utilises staff or other resources that are employed or owned by other group entities, there may be circumstances in which it is in the interests of the group to withhold the provision of those resources – for instance, if it appears likely that the central counterparty may enter external administration. Conflicts could also arise between the risk management objectives of a central counterparty and the business interests of other group entities. A central counterparty should therefore ensure that potential conflicts will not prevent it from appropriately managing its risks and fulfilling its regulatory and other obligations. This may include consideration of whether adequate arrangements exist to manage potential conflicts arising from board composition – that is, where directors of other group entities are members of the central counterparty's board – or any intragroup outsourcing arrangements (including the sharing of staff or other resources) that exist between the central counterparty and other group entities. The central counterparty should be able to demonstrate to the Reserve Bank and other relevant authorities that its arrangements to manage potential conflicts are adequate, including through the provision of relevant documented governance policies and procedures.

Standard 3: Framework for the comprehensive management of risks

A central counterparty should have a sound risk management framework for comprehensively managing legal, credit, liquidity, operational and other risks.

Guidance

A central counterparty should take an integrated and comprehensive view of its risks, including the risks it bears from and poses to its participants and their customers, as well as the risks it bears from and poses to other entities, such as other FMIs, money settlement agents, liquidity providers and service providers (for example, matching and portfolio compression service providers). A central counterparty should consider how various risks relate to, and interact with, each other. The central counterparty should have a sound risk management

framework (including policies, procedures and systems) that enable it to identify, measure, monitor and manage effectively the range of risks that arise in or are borne by the central counterparty. A central counterparty's framework should include the identification and management of interdependencies. A central counterparty should also provide appropriate incentives and the relevant information for its participants and other entities to manage and contain their risks vis-à-vis the central counterparty. As set out in CCP Standard 2 on governance, the board of directors plays a critical role in establishing and maintaining a sound risk management framework.

3.1 A central counterparty should have risk management policies, procedures and systems that enable it to identify, measure, monitor and manage the range of risks that arise in or are borne by the central counterparty. This risk management framework should be subject to periodic review.

Identification of risks

3.1.1 To establish a sound risk management framework, a central counterparty should first identify the range of risks that arise within the central counterparty and the risks it directly bears from or poses to its participants, its participants' customers and other entities. It should identify those risks that could materially affect its ability to perform or to provide services as expected. Typically these include legal, credit, liquidity and operational risks. A central counterparty should also consider other relevant and material risks, such as market (or price), concentration and general business risks, as well as risks that do not appear to be significant in isolation, but when combined with other risks become material. The consequences of these risks may have significant reputational effects on the central counterparty and may undermine the central counterparty's financial soundness as well as the stability of the broader financial markets. In identifying risks, a central counterparty should take a broad perspective and identify the risks that it bears from other entities, such as other FMIs, money settlement agents, liquidity providers, service providers and any entities that could be materially affected by the central counterparty's inability to provide services.

Comprehensive risk policies, procedures and controls

3.1.2 A central counterparty's board and senior management are ultimately responsible for managing the central counterparty's risks (see CCP Standard 2 on governance). The board should determine an appropriate level of aggregate risk tolerance and capacity for the central counterparty. The board and senior management should establish policies, procedures and controls that are consistent with the central counterparty's risk tolerance and capacity. The central counterparty's policies, procedures and controls serve as the basis for identifying, measuring, monitoring and managing the central counterparty's risks and should cover routine and non-routine events, including the potential inability of a participant, or the central counterparty itself, to meet its obligations. A central counterparty's policies, procedures and controls should address all relevant risks, including legal, credit, liquidity, general business and operational risks. These policies, procedures and controls should be part of a coherent and consistent framework that is reviewed and updated periodically, and shared with the Reserve Bank and other relevant authorities.

Information and control systems

3.1.3 In addition, a central counterparty should employ robust information and risk control systems to provide the central counterparty with the capacity to obtain timely information necessary to apply

risk management policies and procedures. In particular, these systems should allow for the accurate and timely measurement and aggregation of risk exposures across the central counterparty, the management of individual risk exposures and the interdependencies between them, and the assessment of the impact of various economic and financial shocks that could affect the central counterparty. Information systems should also enable the central counterparty to monitor its credit and liquidity exposures, overall credit and liquidity limits, and the relationship between these exposures and limits.

3.1.4 Where appropriate, a central counterparty should also provide its participants and its participants' customers with the relevant information to manage and contain their credit and liquidity risks.[9] A central counterparty may consider it beneficial to provide its participants and its participants' customers with information necessary to monitor their credit and liquidity exposures, overall credit and liquidity limits, and the relationship between these exposures and limits. Where the central counterparty permits participants' customers to create exposures in the central counterparty that are borne by the participants, the central counterparty should provide participants with the capacity to limit such risks and the central counterparty should ensure that any large exposures are appropriately monitored and managed.

Internal controls

3.1.5 A central counterparty also should have comprehensive internal processes to help the board and senior management monitor and assess the adequacy and effectiveness of a central counterparty's risk management policies, procedures, systems and controls. While business line management serves as the first 'line of defence', the adequacy of and adherence to control mechanisms should be assessed regularly through independent compliance programs and independent external reviews.[10] A robust internal audit function can provide an independent assessment of the effectiveness of a central counterparty's risk management and control processes. An emphasis on the adequacy of controls by senior management and the board as well as internal audit can also help counterbalance a business management culture that may favour business interests over establishing and adhering to appropriate controls. In addition, proactive engagement of audit and internal control functions when changes are under consideration can also be beneficial. Specifically, central counterparties that involve their internal audit function in pre-implementation reviews will often reduce their need to expend additional resources to retrofit processes and systems with critical controls that had been overlooked during initial design phases and construction efforts.

3.2 A central counterparty should ensure that financial and other obligations imposed on participants under its risk management framework are proportional to the scale and nature of individual participants' activities.

3.2.1 A central counterparty should ensure that it has sufficient risk controls and other arrangements in place to comply with the CCP Standards, and address any other systemic risk implications of its activities. In accordance with a central counterparty's risk management framework, these arrangements may place financial and other obligations on participants, such as margin, contributions to prefunded default

9 A central counterparty should ensure that its information systems have the capacity to provide this information on a timely basis.

10 Internal audits should be performed by qualified and independent individuals who did not participate in the creation of the control mechanisms. The central counterparty should also subject aspects of its risk management processes to external independent review (see CCP Standard 2 on governance).

arrangements, *ex-ante* agreed arrangements for the provision of liquid resources and allocations of uncovered losses or liquidity shortfalls (see CCP Standard 4 on credit risk, CCP Standard 7 on liquidity risk and CCP Standard 12 on participant default rules and procedures), or minimum operational requirements (see CCP Standard 16 on operational risk). Such obligations should be proportional to the nature and magnitude of the risk that individual participants' activities pose to the safety of the central counterparty. In general, obligations placed on a participant with limited or conservative activities should differ from those placed on a participant with extensive or risky activities. For the purposes of this Standard, financial obligations do not include minimum capital requirements for participants, which are dealt with under CCP Standard 17 on access and participation requirements.

3.3 A central counterparty should provide incentives to participants and, where relevant, their customers to manage and contain the risks they pose to the central counterparty.

3.3.1 In establishing risk management policies, procedures and systems, a central counterparty should provide incentives to participants and, where relevant, their customers to manage and contain the risks they pose to the central counterparty. There are several ways in which a central counterparty may provide incentives. One example is the use of loss-sharing arrangements proportional to the exposures brought to the central counterparty. Provision of incentives can help reduce the moral hazard that may arise from formulas in which losses are shared equally among participants or other formulas where losses are not shared proportionally to risk.

3.4 A central counterparty should regularly review the material risks it bears from and poses to other entities (such as other FMIs, money settlement agents, liquidity providers and service providers) as a result of interdependencies, and develop appropriate risk management tools to address these risks.

3.4.1 A central counterparty should regularly review the material risks it bears from and poses to other entities (such as other FMIs, money settlement agents, liquidity providers and service providers) as a result of interdependencies and develop appropriate risk management tools to address these risks (see also CCP Standard 19 on FMI links). In particular, a central counterparty should have effective risk management tools to manage all relevant risks, including the legal, credit, liquidity, general business and operational risks that it bears from and poses to other entities, in order to limit the effects of disruptions from and to such entities as well as disruptions from and to the broader financial markets. These tools should include business continuity arrangements that allow for rapid recovery and resumption of critical operations and services in the event of operational disruptions (see CCP Standard 16 on operational risk), liquidity risk management techniques (see CCP Standard 7 on liquidity risk), and recovery or orderly wind-down plans should the central counterparty become non-viable. Because of the interdependencies between and among systems, a central counterparty should ensure that its crisis management arrangements allow for effective coordination among the affected entities, including cases in which its own viability or the viability of an interdependent entity is in question.

3.5 A central counterparty should identify scenarios that may potentially prevent it from being able to provide its critical operations and services as a going concern and assess the effectiveness of a full range of options for recovery or orderly wind-down. A central counterparty should prepare appropriate plans for its recovery or orderly wind-down based on the results of that assessment. Where applicable, a central counterparty should also provide relevant authorities with the information needed for purposes of resolution planning.

3.5.1 A central counterparty should identify scenarios that may potentially prevent it from being able to provide its critical operations and services as a going concern and assess the effectiveness of a full range of options for recovery or orderly wind-down. These scenarios should take into account the various independent and related risks to which the central counterparty is exposed. Using this analysis (and taking into account any constraints potentially imposed by domestic legislation), the central counterparty should prepare appropriate plans for its recovery or orderly wind-down. The plans should contain, among other elements, a substantive summary of the key recovery or orderly wind-down strategies, the identification of the central counterparty's critical operations and services, and a description of the measures needed to implement the key strategies. A central counterparty should have the capacity to identify and provide to related entities the information needed to implement its plans on a timely basis during stress scenarios. In addition, these plans should be reviewed and updated regularly. Where applicable, a central counterparty should provide relevant resolution authorities with the information, including strategy and scenario analysis, needed for purposes of resolution planning.

Standard 4: Credit risk

A central counterparty should effectively measure, monitor and manage its credit exposures to participants and those arising from its clearing processes. A central counterparty should maintain sufficient financial resources to cover its credit exposure to each participant fully with a high degree of confidence.

Guidance

Credit risk is broadly defined as the risk that a counterparty will be unable to meet fully its financial obligations when due or at any time in the future. The default of a participant (and its affiliates) has the potential to cause severe disruption to a central counterparty, its other participants and the financial markets more broadly. Therefore, a central counterparty should establish a robust framework to manage its credit exposures to its participants and the credit risks arising from its clearing processes (see also CCP Standard 3 on the framework for the comprehensive management of risks, CCP Standard 9 on money settlements and CCP Standard 15 on custody and investment risks). Credit exposures may arise in the form of current exposures, potential future exposures, or both. Current exposure, in this context, is defined as the loss that a central counterparty would face immediately if a participant were to default.[11] Potential future exposure is broadly defined as any potential credit exposure that a central counterparty could face at a future point in time.[12] The type and level of credit exposure faced by a central counterparty will vary based on its design and the credit risk of the counterparties concerned.[13]

4.1 A central counterparty should establish a robust framework to manage its credit exposures to its participants and the credit risks arising from its clearing processes. Credit exposures may arise from current exposures, potential future exposures, or both.

11 Current exposure is technically defined as the larger of zero or the market value (or replacement cost) of a transaction or portfolio of transactions within a netting set with a counterparty that would be lost upon the default of the counterparty.

12 Potential future exposure is technically defined as the maximum exposure estimated to occur at a future point in time at a high level of statistical confidence. Potential future exposure arises from potential fluctuations in the market value of a participant's open positions between the time they are incurred or reset to the current market price and the time they are liquidated or effectively hedged.

13 In considering any credit exposure to a central bank, on a case-by-case basis a central counterparty may take into account the special characteristics of the central bank.

4.1.1 A central counterparty typically faces both current and potential future exposures because it typically holds open positions with its participants. Current exposure arises from fluctuations in the market value of open positions between the central counterparty and its participants.[14] Potential future exposure arises from potential fluctuations in the market value of a defaulting participant's open positions until the positions are closed out, fully hedged or transferred by the central counterparty following an event of default.[15] For example, during the period in which a central counterparty neutralises or closes out a position following the default of a participant, the market value of the position or asset being cleared may change, which could increase the central counterparty's credit exposure, potentially significantly.[16] A central counterparty can also face potential future exposure due to the potential for collateral (initial margin) to decline significantly in value over the close out period.

4.2 A central counterparty should identify sources of credit risk, routinely measure and monitor credit exposures, and use appropriate risk management tools to control these risks. To assist in this process, a central counterparty should ensure it has the capacity to calculate exposures to participants on a timely basis as required, and to receive and review timely and accurate information on participants' credit standing.

4.2.1 A central counterparty should frequently and regularly measure and monitor its credit risks throughout the day using timely information. A central counterparty should ensure that it has access to adequate information to allow it to measure and monitor its current and potential future exposures, including to individual participants. Current exposure is relatively straightforward to measure and monitor when relevant market prices are readily available. Potential future exposure is typically more challenging to measure and monitor and usually requires modelling and estimation of possible future market price developments and other variables and conditions, as well as specifying an appropriate time horizon for the close out of defaulted positions. In order to estimate the potential future exposures that could result from participant defaults, a central counterparty should identify risk factors and monitor potential market developments and conditions that could affect the size and likelihood of its losses in the close out of a defaulting participant's positions. A central counterparty should regularly monitor the existence of large exposures to its participants and, where appropriate, their customers. A central counterparty's systems should be capable of calculating exposures to participants intraday and at short notice.

4.2.2 Additionally, a central counterparty should have the capacity to monitor any changes in the creditworthiness of its participants through the systematic review of timely information on financial standing, business activities and profile, and potential interdependencies. The central counterparty

14 For example, for a central counterparty that pays and collects variation margin (after marking positions to market and then, upon completion of the variation cycle, resetting the value of positions to zero daily), the current exposure is the difference between the current (that is, at the moment) value of open positions and the value of the positions when the central counterparty last marked them to market for the purpose of collecting variation margin.

15 For positions that are marked to market and settled daily, potential future exposure is typically related to price development in the interval between the last daily mark to market and the point the position is closed out fully hedged or transferred.

16 A central counterparty may close out a defaulting participant's positions by entering the market to buy or sell contracts identical but opposite to the net positions held by the defaulting participant at current market prices (see CCP Standard 12 on participant default rules and procedures). The central counterparty may alternatively auction the defaulting participant's positions to other participants whether in whole or in parts. During the liquidation period, market prices on the open positions can change, exposing the central counterparty to additional liquidation costs until the point of close out. To mitigate this risk, a central counterparty may also temporarily hedge the defaulter's positions by entering into positions with values that are negatively correlated with the values of the positions held by the defaulting participant. The central counterparty's liquidation cost therefore not only includes the uncovered current exposure that would exist at the time of default but also the potential future exposure associated with relevant changes in market prices during the liquidation period.

should use this capacity to conduct periodic reviews of its participants' credit standing, and to conduct ad hoc reviews where the central counterparty has reason to believe that a participant's credit standing may deteriorate.

4.2.3 A central counterparty should mitigate its credit risk to the extent possible. For example, to control the build-up of current exposures, a central counterparty should require that open positions be marked to market and that each participant pay funds, typically in the form of variation margin, to cover any loss in its positions' net value at least daily; such a requirement limits the accumulation of current exposures and therefore mitigates potential future exposures. In addition, a central counterparty should have the authority and operational capacity to make intraday margin calls, both scheduled and unscheduled, from participants. Further, a central counterparty may in some cases choose to place limits on credit exposures, even where these are collateralised. Limits on concentrations of positions or additional collateral requirements may also be warranted.

4.2.4 A central counterparty typically uses a sequence of prefunded financial resources, often referred to as a 'waterfall', to manage its losses caused by participant defaults. The waterfall may include a defaulter's initial margin, the defaulter's contribution to a prefunded default arrangement, a specified portion of the central counterparty's own funds, and other participants' contributions to a prefunded default arrangement.[17] A central counterparty should hold a combination of margin and pooled prefunded resources to control credit risks. Initial margin is used to cover a central counterparty's potential future exposures, as well as current exposures not covered by variation margin, to each participant with a high degree of confidence. However, a central counterparty generally remains exposed to residual risk (or tail risk) if a participant defaults and market conditions concurrently change more than is anticipated in the margin calculations. In such scenarios, a central counterparty's losses may exceed the defaulting participant's posted margin. Although it is not feasible to cover all such tail risks, given the unknown scope of potential losses due to price changes, a central counterparty should maintain additional pooled prefunded financial resources to cover a portion of the tail risk.

4.3 A central counterparty should have the authority to impose activity restrictions or additional credit risk controls on a participant in situations where the central counterparty determines that the participant's credit standing may be in doubt.

4.3.1 If a central counterparty determines that a participant's credit standing may be in doubt, it should have the authority, under its rules and procedures, to impose additional credit risk controls on the participant. These may include placing restrictions on the level or types of activities that the participant can undertake, or calling additional margin or collateral from the participant. In extreme cases, the central counterparty may need to consider suspending the participant (see CCP Standard 12 on participant default rules and procedures and CCP Standard 17 on access and participation requirements).

4.4 A central counterparty should cover its current and potential future exposures to each participant fully with a high degree of confidence using margin and other prefunded financial

17 Prefunded default arrangements for loss mutualisation and other pooling-of-resources arrangements involve trade-offs that a central counterparty should carefully assess and balance. For example, a central counterparty may be able to protect itself against defaults in extreme conditions more efficiently using pooled resources, as the costs are shared among participants. The lower cost provides an incentive to increase the available financial resources so that the central counterparty is more financially secure. The pooling of resources, however, also increases the interdependencies among participants. The proportion of assets used to absorb a default that is pooled across participants versus the proportion that is not, such as margins, should balance the safety and soundness of the central counterparty against the increased interdependencies among participants in order to minimise systemic risk.

resources (see CCP Standard 5 on collateral and CCP Standard 6 on margin). In addition, a central counterparty that is involved in activities with a more complex risk profile or that is systemically important in multiple jurisdictions should maintain additional financial resources to cover a wide range of potential stress scenarios that should include, but not be limited to, the default of the two participants and their affiliates that would potentially cause the largest aggregate credit exposure for the central counterparty in extreme but plausible market conditions. All other central counterparties should maintain additional financial resources sufficient to cover a wide range of potential stress scenarios that should include, but not be limited to, the default of the participant and its affiliates that would potentially cause the largest aggregate credit exposure for the central counterparty in extreme but plausible market conditions. In all cases, a central counterparty should document its supporting rationale for, and should have appropriate governance arrangements relating to, the amount of total financial resources it maintains.

4.4.1 A central counterparty should cover its current and potential future exposures to each participant fully with a high degree of confidence using margin and other prefunded financial resources. As discussed more fully in CCP Standard 6 on margin, a central counterparty should establish initial margin requirements that are commensurate with the risks of each product and portfolio. Initial margin should be designed to meet an established single-tailed confidence level of at least 99 per cent of the estimated distribution of future exposure.[18] For a central counterparty that calculates margin at the portfolio level, this Standard applies to the distribution of future exposure of each portfolio. For a central counterparty that calculates margin at more granular levels, such as at the sub-portfolio level or product level, the Standard should be met for the corresponding distributions of future exposure.

4.4.2 In addition to fully covering its current and potential future exposures, a central counterparty should maintain additional financial resources sufficient to cover a wide range of potential stress scenarios involving extreme but plausible market conditions. Specifically, a central counterparty that is involved in activities with a more complex risk profile (such as clearing financial instruments that are characterised by discrete jump-to-default price changes or that are highly correlated with potential participant defaults) or that is systemically important in multiple jurisdictions, should maintain additional financial resources sufficient to cover a wide range of potential stress scenarios that should include, but not be limited to, the default of the two participants and their affiliates that would potentially cause the largest aggregate credit exposure for the central counterparty in extreme but plausible market conditions. Determinations of whether a central counterparty is systemically important in multiple jurisdictions should include consideration of, among other factors: the location of the central counterparty's participants; the aggregate volume and value of transactions that originate in each jurisdiction in which it operates; the proportion of its total volume and value of transactions that originate in each jurisdiction in which it operates; the range of currencies in which the instruments it clears are cleared or settled; any links it has with FMIs located in other jurisdictions; and the extent to which it clears instruments that are subject to mandatory clearing obligations in multiple jurisdictions. All other central counterparties should maintain additional financial resources sufficient to cover a wide range of potential stress scenarios that should include, but not be limited to, the default of the participant and its affiliates that would potentially cause the largest aggregate credit exposure for the

18 This concept parallels the technical definition of potential future exposure as a risk measure.

central counterparty in extreme but plausible market conditions. In all cases, a central counterparty should document its supporting rationale for, and should have appropriate governance arrangements relating to (see CCP Standard 2 on governance), the amount of total financial resources it maintains.

4.5 A central counterparty should, through rigorous stress testing, determine the amount and regularly test the sufficiency of its total financial resources available in the event of a default or multiple defaults in extreme but plausible market conditions. Stress tests should be performed daily using standard and predetermined parameters and assumptions. On at least a monthly basis, a central counterparty should perform a comprehensive and thorough analysis of stress-testing scenarios, models and underlying parameters and assumptions used to ensure they are appropriate for determining the central counterparty's required level of default protection in light of current and evolving market conditions. A central counterparty should perform this analysis of stress testing more frequently when the products cleared or markets served display high volatility, become less liquid, or when the size or concentration of positions held by a central counterparty's participants increases significantly. A full validation of a central counterparty's risk management model should be performed at least annually.

4.5.1 A central counterparty should determine the amount and regularly test the sufficiency of its total financial resources available in the event of a default or multiple defaults in extreme but plausible market conditions through rigorous stress testing. A central counterparty should also conduct reverse stress tests, as appropriate, to test how severe stress conditions would be covered by its total financial resources. Because initial margin is a key component of a central counterparty's total financial resources, a central counterparty should also test the adequacy of its initial margin requirements and model, through backtesting and sensitivity analysis, respectively (see CCP Standard 6 for further discussion on the testing of initial margin requirements and model).

4.6 In conducting stress testing, a central counterparty should consider the effect of a wide range of relevant stress scenarios in terms of both defaulters' positions and possible price changes in liquidation periods. Scenarios should include relevant peak historic price volatilities, shifts in other market factors such as price determinants and yield curves, multiple defaults over various time horizons, simultaneous pressures in funding and asset markets, and a spectrum of forward-looking stress scenarios in a variety of extreme but plausible market conditions.

4.6.1 In constructing stress scenarios, extreme but plausible conditions should not be considered a fixed set of conditions, but rather, conditions that evolve. Stress tests should, on a timely basis, incorporate emerging risks and changes in market assumptions (for example, departures from usual patterns of co-movements in prices among the products a central counterparty clears).[19] A central counterparty proposing to clear new products should consider movements in prices of any relevant related products.

4.6.2 A central counterparty should also conduct, as appropriate, reverse stress tests aimed at identifying the extreme scenarios and market conditions in which its total financial resources would not provide sufficient coverage of tail risk. Reverse stress tests require a central counterparty to model hypothetical positions and extreme market conditions that may go beyond what are considered extreme but plausible market conditions in order to help understand margin calculations and the sufficiency of financial resources given the underlying assumptions modelled. Modelling very extreme market

19 Dependence among exposures as well as between participants and exposures should be considered. If a central counterparty calculates exposures on a portfolio basis, then the dependence of the instruments within participants' portfolios needs to be stressed.

conditions can help a central counterparty determine the limits of its current model and resources. However, it requires the central counterparty to exercise judgement when modelling different markets and products. A central counterparty should develop hypothetical very extreme scenarios and market conditions tailored to the specific risks of the markets and of the products it serves. Reverse stress testing should be considered a helpful management tool but need not, necessarily, drive the central counterparty's determination of the appropriate level of financial resources.

4.7 A central counterparty should have clearly documented and effective rules and procedures to report stress-test information to appropriate decision-makers and ensure that additional financial resources are obtained on a timely basis in the event that projected stress-test losses exceed available financial resources. Where projected stress-test losses of a single or only a few participants exceed available financial resources, it may be appropriate to increase non-pooled financial resources; otherwise, where projected stress-test losses are frequent and consistently widely dispersed across participants, clear processes should be in place to augment pooled financial resources.

4.7.1 In the event that projected stress-test losses exceed available financial resources, a central counterparty should obtain additional financial resources. The central counterparty should therefore ensure that its rules and procedures support timely action to increase financial resources in these circumstances. The nature of the additional financial resources called may depend on the distribution of projected stress-test losses. If projected stress-test losses exceed available financial resources for only a single, or few participants, then it may be appropriate to call for additional margin or other non-pooled financial resources from those participants. The central counterparty should clearly articulate the circumstances in which it will call for additional margin or non-pooled financial resources from participants, and both the form (that is, cash or eligible non-cash collateral – see CCP Standard 5) and the time frame in which calls must be satisfied. The central counterparty should periodically engage with participants to ensure that they understand their potential obligations and have taken appropriate steps to ensure that they would be able to meet them. Where projected stress-test losses are consistently widely dispersed across participants, then it may be appropriate for the central counterparty to augment pooled financial resources. The central counterparty should have documented and effective processes in place to achieve this. These processes should clearly specify the circumstances in which additional pooled financial resources may be called, including how any additional contributions from participants are to be determined and when these should be paid.

4.7.2 A central counterparty should have clear procedures to report the results of its stress tests to appropriate decision-makers at the central counterparty and to use these results to evaluate the adequacy of and adjust its total financial resources. Stress scenarios, models and underlying parameters and assumptions should be examined based on historical data of prices of cleared products and participants' positions and potential developments of these factors under extreme but plausible market conditions in the markets that the central counterparty serves.

4.8 A central counterparty should establish explicit rules and procedures that address fully any credit losses it may face as a result of any individual or combined default among its participants with respect to any of their obligations to the central counterparty. These rules and procedures should address how potentially uncovered credit losses would be allocated, including the repayment of any funds a central counterparty may borrow from liquidity providers. These

rules and procedures should also indicate the central counterparty's process to replenish any financial resources that the central counterparty may employ during a stress event, so that the central counterparty can continue to operate in a safe and sound manner.

Use of financial resources

4.8.1 The rules of a central counterparty should expressly set out the waterfall, including the circumstances in which specific resources of the central counterparty can be used in a participant default (see CCP Standard 12 on participant default rules and procedures and CCP Standard 20 on disclosure of rules, key policies and procedures, and market data). For the purposes of this Standard, a central counterparty should not include as 'available' to cover credit losses from participant defaults those resources that are needed to cover current operating expenses, potential general business losses, or other losses from ancillary activities in which the central counterparty is engaged (see CCP Standard 1 on legal basis and CCP Standard 14 on general business risk). In addition, if a central counterparty serves multiple markets (either in the same jurisdiction or multiple jurisdictions), its ability to use resources supplied by participants in one market to cover losses from a participant default in another market should have a sound legal basis, be clear to all participants, and avoid significant levels of contagion risk between markets and participants. The design of a central counterparty's stress tests should take into account the extent to which resources are pooled across markets in scenarios involving one or more participant defaults across several markets.

Contingency planning for uncovered credit losses

4.8.2 In certain extreme circumstances, the post-liquidation value of the collateral and other financial resources that secure a central counterparty's credit exposures may not be sufficient to cover fully credit losses resulting from those exposures. A central counterparty should analyse and plan for how it would address any uncovered credit losses. A central counterparty should establish explicit rules and procedures that address fully any credit losses it may face as a result of any individual or combined default among its participants with respect to any of their obligations to the central counterparty. These rules and procedures should address how potentially uncovered credit losses would be allocated, including the repayment of any funds a central counterparty may borrow from liquidity providers.[20] A central counterparty's rules and procedures should also indicate its process to replenish any financial resources it may employ during a stress event, so that it can continue to operate in a safe and sound manner.

Standard 5: Collateral

A central counterparty that requires collateral to manage its or its participants' credit exposures should accept collateral with low credit, liquidity and market risks. A central counterparty should also set and enforce appropriately conservative haircuts and concentration limits.

20 For instance, a central counterparty's rules and procedures might provide the possibility to allocate uncovered credit losses by writing down potentially unrealised gains by non-defaulting participants and the possibility of calling for additional contributions from participants based on the relative size and risk of their portfolios.

Guidance

Collateralising credit exposures protects a central counterparty and, where relevant, its participants against potential losses in the event of a participant default (see CCP Standard 4 on credit risk). Besides mitigating a central counterparty's own credit risk, the use of collateral can provide participants with incentives to manage the risks they pose to the central counterparty or other participants. A central counterparty should apply prudent haircuts to the value of the collateral to achieve a high degree of confidence that the liquidation value of the collateral will be greater than or equal to the obligation that the collateral secures in extreme but plausible market conditions. Additionally, a central counterparty should have the capacity to use the collateral promptly when needed.

5.1 A central counterparty should generally limit the assets it (routinely) accepts as collateral to those with low credit, liquidity and market risks.

5.1.1 A central counterparty should generally limit the assets it (routinely) accepts as collateral to those with low credit, liquidity and market risks. Collateral with low credit, liquidity and market risks comprises assets that may be reliably liquidated or repurchased in private markets, within a reasonable time frame and at a value within the haircut applied or, *in extremis* and where the collateral taker has access, sold to a central bank under a repurchase agreement or otherwise pledged to a central bank. Certain types of collateral that are not considered to have low credit, liquidity and market risks may nevertheless be acceptable collateral for credit purposes if an appropriate haircut is applied. A central counterparty must be confident of the collateral's value in the event of liquidation and of its capacity to use that collateral quickly, especially in stressed market conditions. Where a central counterparty accepts collateral that does not have low credit, liquidity and market risks, it should demonstrate that it sets and enforces appropriately conservative haircuts and concentration limits (see CCP Standard 5.3).

5.1.2 In general, bank guarantees are not acceptable collateral. However, the use of bank guarantees may be acceptable under certain specified circumstances and under certain conditions, subject to prior approval from the Reserve Bank or other relevant authorities. The Reserve Bank will consider the acceptability of bank guarantees as collateral on a case-by-case basis, taking into account factors including: the credit standing of the bank providing the guarantee; the legal certainty of the arrangement; and whether there is any collateral supporting the guarantee.

5.1.3 Further, a central counterparty should regularly review its requirements for acceptable collateral in accordance with changes in underlying risks. When evaluating types of collateral, a central counterparty should consider potential delays in accessing the collateral due to the settlement conventions for transfers of the asset. In addition, participants should not be permitted to post their own debt or equity securities, or debt or equity of companies closely linked to them, as collateral. More generally, a central counterparty should mitigate specific wrong-way risk by limiting the acceptance of collateral that would likely lose value in the event that the participant providing the collateral defaulted. The central counterparty should measure and monitor the correlation between a counterparty's creditworthiness and the collateral posted and take measures to mitigate the risks, for instance by setting more conservative haircuts.

5.1.4 If a central counterparty plans to use assets held as collateral to secure liquidity facilities in the event of a participant default, the central counterparty will also need to consider, in determining acceptable collateral, what will be acceptable as security to lenders offering liquidity facilities (see CCP Standard 7 on liquidity risk).

5.2 In determining its collateral policies, a central counterparty should take into consideration the broad effect of these policies on the market. As part of this, a central counterparty should consider allowing the use of collateral commonly accepted in the relevant jurisdictions in which it operates.

5.2.1 A central counterparty's collateral policies may have broader effects than their direct implications for the effectiveness of the central counterparty's risk controls. On the one hand, assets accepted as collateral by a central counterparty may be more likely to then be held by participants or used as collateral in other contexts, and may become more liquid as a result. On the other hand, use of a particular class of assets to meet collateral obligations at a central counterparty may, depending on its supply, restrict the availability of such assets for other uses, or significantly affect liquidity and pricing. A central counterparty should consider such broader effects when framing its collateral policies.

5.2.2 Participants that are required to source unfamiliar assets as collateral may face additional operational, legal or financial risks as a result. A central counterparty should therefore consider allowing the use of collateral that is commonly accepted in each jurisdiction in which it operates. In particular, a central counterparty with material Australian-based participation should consider accepting appropriate Australian dollar-denominated securities as collateral.

5.3 A central counterparty should establish prudent valuation practices and develop haircuts that are regularly tested and take into account stressed market conditions.

5.3.1 To provide adequate assurance of the value of collateral in the event of liquidation, a central counterparty should establish prudent valuation practices and develop haircuts that are regularly tested and take into account stressed market conditions. A central counterparty should, at a minimum, mark its collateral to market daily. Haircuts should reflect the potential for asset values and liquidity to decline over the interval between their last revaluation and the time by which a central counterparty can reasonably assume that the assets can be liquidated. Haircuts also should incorporate assumptions about collateral value during stressed market conditions and reflect regular stress testing that takes into account extreme price moves, as well as changes in market liquidity for the asset. If market prices do not fairly represent the true value of the assets, a central counterparty should have the authority to exercise discretion in valuing assets according to predefined and transparent methods. A central counterparty's haircut procedures should be independently validated at least annually.[21]

5.4 In order to reduce the need for procyclical adjustments, a central counterparty should establish stable and conservative haircuts that are calibrated to include periods of stressed market conditions, to the extent practicable and prudent.

5.4.1 A central counterparty should appropriately address procyclicality in its collateral arrangements. To the extent practicable and prudent, a central counterparty should establish stable and conservative haircuts that are calibrated to include periods of stressed market conditions in order to reduce the need for procyclical adjustments. In this context, procyclicality typically refers to changes in risk management practices that are positively correlated with market, business or credit cycle fluctuations and that may cause or exacerbate financial instability. While changes in collateral values tend to be procyclical, collateral arrangements can increase procyclicality if haircut levels fall during periods of

21 Validation of the central counterparty's haircut procedures should be performed by personnel of sufficient expertise who are independent of the personnel that created or apply the haircut procedures. These expert personnel could be drawn from within the central counterparty. However, a review by personnel external to the central counterparty may also be necessary at times.

low market stress and increase during periods of high market stress. For example, in a stressed market, a central counterparty may require the posting of additional collateral both because of the decline in asset prices and because of an increase in haircut levels. Such actions could exacerbate market stress and contribute to driving down asset prices further, resulting in additional collateral requirements. This cycle could exert further downward pressure on asset prices. Addressing issues of procyclicality may create additional costs for central counterparties and their participants in periods of low market stress because of higher collateral requirements, but result in additional protection and potentially less costly and less disruptive adjustments in periods of high market stress.

5.5 A central counterparty should avoid concentrated holdings of certain assets where this would significantly impair the ability to liquidate such assets quickly without significant adverse price effects.

5.5.1 A central counterparty should avoid concentrated holdings of certain assets where this would significantly impair the ability to liquidate such assets quickly without significant adverse price effects, including in stressed market conditions. High concentrations within holdings can be avoided by establishing concentration limits or imposing concentration charges. Concentration limits restrict participants' ability to provide certain collateral assets above a specified threshold as established by the central counterparty. Concentration charges penalise participants for maintaining holdings of certain assets beyond a specified threshold as established by the central counterparty. Further, concentration limits and charges should be constructed to prevent participants from covering a large share of their collateral requirements with the most risky assets acceptable. Concentration limits and charges should be periodically reviewed by the central counterparty to determine their adequacy.

5.6 A central counterparty that accepts cross-border collateral should mitigate the risks associated with its use and ensure that the collateral can be used in a timely manner.

5.6.1 If a central counterparty accepts cross-border collateral, it should identify and mitigate any additional risks associated with its use and ensure that it can be used in a timely manner.[22] A cross-border collateral arrangement can provide an efficient liquidity bridge across markets, help relax collateral constraints for some participants, and contribute to the efficiency of some asset markets. These linkages, however, can also create significant interdependencies between a central counterparty and other FMIs and risks to the central counterparty that need to be evaluated and managed (see also CCP Standard 16 on operational risk and CCP Standard 19 on FMI links). For example, a central counterparty should have appropriate legal and operational safeguards to ensure that it can use the cross-border collateral in a timely manner and should identify and address any significant liquidity effects. A central counterparty also should consider foreign exchange risk where collateral is denominated in a currency different from that in which the exposure arises, and set haircuts to address the additional risk to a high level of confidence. The central counterparty should have the capacity to address potential operational challenges of operating across borders, such as differences in time zones or operating hours of foreign central securities depositories or custodians.

5.7 A central counterparty should use a collateral management system that is well designed and operationally flexible.

22 Cross-border collateral has at least one of the following foreign attributes with respect to the country in which the central counterparty's operations are based: the currency of denomination; the jurisdiction in which the assets are located; or the jurisdiction in which the issuer is established.

Collateral management systems

5.7.1 A central counterparty should use a well-designed and operationally flexible collateral management system. Such a system should accommodate changes in the ongoing monitoring and management of collateral. Where appropriate, the system should allow for the timely calculation and execution of margin calls, the management of margin call disputes, and the accurate daily reporting of levels of initial and variation margin. Further, a collateral management system should track the extent of reuse of collateral (both cash and non-cash) and the rights of a central counterparty to the collateral provided to it by its counterparties. Where appropriate, a central counterparty's collateral management system should also have functionality to accommodate the timely deposit, withdrawal, substitution and liquidation of collateral in each jurisdiction in which it operates. In particular, where the scope of Australian participation in the central counterparty is material, and where market conventions dictate, a central counterparty's collateral management system should have the capacity to accommodate the timely deposit, withdrawal, substitution and liquidation of collateral during Australian market hours. A central counterparty should allocate sufficient resources to its collateral management system to ensure an appropriate level of operational performance, efficiency and effectiveness. Senior management should ensure that the central counterparty's collateral management function is adequately staffed to ensure smooth operations, especially during times of market stress, and that all activities are tracked and reported, as appropriate, to senior management.[23]

Reuse of collateral

5.7.2 Reuse of collateral refers to the central counterparty's subsequent use of collateral that has been provided by participants in the normal course of business. This differs from the central counterparty's use of collateral in a default scenario during which the defaulter's collateral, which has become the property of the central counterparty, can be used to access liquidity facilities or liquidated to cover losses (see CCP Standard 12 on participant default rules and procedures). A central counterparty should have clear and transparent rules regarding the reuse of collateral (see CCP Standard 20 on disclosure of rules, key policies and procedures, and market data). In particular, the rules should clearly specify when a central counterparty may reuse its participant collateral and the process for returning that collateral to participants. In general, a central counterparty should not rely on the reuse of collateral as an instrument for increasing or maintaining its profitability. However, a central counterparty may invest any cash collateral received from participants on their behalf (see CCP Standard 15 on custody and investment risks).

Standard 6: Margin

A central counterparty should cover its credit exposures to its participants for all products through an effective margin system that is risk based and regularly reviewed.

Guidance

An effective margining system is a key risk management tool for a central counterparty to manage the credit exposures associated with its participants' open positions (see also CCP Standard 4 on credit risk). A central

23 Summary reports should include information on the reuse of collateral and the terms of such reuse, including instrument, credit quality and maturity. These reports should also track concentration of individual collateral asset classes.

counterparty should collect margin, which is a deposit of collateral in the form of money, securities or other financial instruments, to mitigate its credit exposures for all products that it clears in the event of a participant default (see also CCP Standard 5 on collateral). Margin systems typically differentiate between initial margin and variation margin.[24] Initial margin is typically collected to cover potential changes in the value of each participant's position (that is, potential future exposure) over the appropriate close out period in the event the participant defaults. Calculating potential future exposure requires modelling potential price movements and other relevant factors, as well as specifying the target degree of confidence and length of the close out period. Variation margin is collected and paid out to reflect current exposures resulting from actual changes in market prices. To calculate variation margin, open positions are marked to current market prices and funds are typically collected from (or paid to) a counterparty to settle any losses (or gains) on those positions.

6.1 A central counterparty should have a margin system that establishes margin levels commensurate with the risks and particular attributes of each product, portfolio and market it serves.

6.1.1 When setting margin requirements, a central counterparty should have a margin system that establishes margin levels commensurate with the risks and particular attributes of each product, portfolio and market it serves. Product risk characteristics can include, but are not limited to, price volatility and correlation, non-linear price characteristics, jump-to-default risk, market liquidity, possible liquidation procedures (for example, tender by or commission to market-makers), and correlation between price and position such as wrong-way risk.[25] Margin requirements need to account for the complexity of the underlying instruments and the availability of timely, high-quality pricing data. For example, OTC derivatives may require more conservative margin models because of their complexity and the greater uncertainty of the reliability of price quotes. Furthermore, the appropriate close out period may vary among products and markets depending upon the product's liquidity, price and other characteristics. Additionally, a central counterparty for cash markets (or physically deliverable derivatives products) should take into account the risk of 'fails to deliver' of securities (or other relevant instruments) in its margin methodology. In a fails-to-deliver scenario, the central counterparty should continue to margin positions for which a participant fails to deliver the required security (or other relevant instrument) on the settlement date.

6.2 A central counterparty should have a reliable source of timely price data for its margin system. A central counterparty should also have procedures and sound valuation models for addressing circumstances in which pricing data are not readily available or reliable.

6.2.1 A central counterparty should have a reliable source of timely price data because such data are critical for a central counterparty's margin system to operate accurately and effectively. In most cases, a central counterparty should rely on market prices from continuous, transparent and liquid markets. If a central counterparty acquires pricing data from third-party pricing services, the central counterparty should continually evaluate the reliability and accuracy of the data. A central counterparty should also have procedures and sound valuation models for addressing circumstances in which pricing data from markets or third-party sources are not readily available or reliable. A central counterparty should have its valuation models validated under a variety of market scenarios at least annually by a

24 Variation margin may also be called mark-to-market margin or variation settlement.

25 Correlation should not be understood to be limited to linear correlation, but rather to encompass a broad range of co-dependence or co-movement in relevant economic variables.

qualified and independent party to ensure that its model accurately produces appropriate prices, and, where appropriate, the central counterparty should adjust its calculation of initial margin to reflect any identified model risk.[26] A central counterparty should address all pricing and market liquidity concerns on an ongoing basis to support the daily measurement of its risks.

6.2.2 For some markets, prices may not be reliable because of the lack of a continuous liquid market. Although independent third-party sources would be preferable, in some cases participants may be an appropriate source of price data, as long as the central counterparty has a system that ensures that prices submitted by participants are reliable and accurately reflect the value of cleared products. Moreover, even when quotes are available, bid-ask spreads may be volatile and widen, particularly during times of market stress, thereby constraining the central counterparty's ability to measure accurately and promptly its exposure. In cases where price data are not available or reliable, to determine appropriate prices a central counterparty should analyse historical information about actual trades submitted for clearing and indicative prices (such as bid-ask spreads), as well as the reliability of price data, especially in volatile and stressed markets. When prices are estimated, the systems and models used for this purpose must be subject to annual validation and testing. As a general rule, margin settings should, other things being equal, be higher where price data are relatively less timely or reliable.

6.3 A central counterparty should adopt initial margin models and parameters that are risk based and generate margin requirements sufficient to cover its potential future exposure to participants in the interval between the last margin collection and the close out of positions following a participant default. Initial margin should meet an established single-tailed confidence level of at least 99 per cent with respect to the estimated distribution of future exposure. For a central counterparty that calculates margin at the portfolio level, this requirement applies to each portfolio's distribution of future exposure. For a central counterparty that calculates margin at more granular levels, such as at the sub-portfolio level or by product, the requirement should be met for corresponding distributions of future exposure. The model should: use a conservative estimate of the time horizons for the effective hedging or close out of the particular types of products cleared by the central counterparty (including in stressed market conditions); have an appropriate method for measuring credit exposure that accounts for relevant product risk factors and portfolio effects across products; and to the extent practicable and prudent, limit the need for destabilising, procyclical changes.

6.3.1 The method selected by the central counterparty to estimate its potential future exposure should be capable of measuring and incorporating the effects of price volatility and other relevant product factors and portfolio effects over a close out period that reflects the market size and dynamics for each product cleared by the central counterparty.[27] The estimation may account for the central counterparty's ability to implement effectively the hedging of future exposure. The method selected by the central counterparty should take into account correlations across product prices, market

26 Validation of the central counterparty's valuation procedures should be performed by personnel with sufficient expertise who are independent of the personnel that created and use the valuation procedures. These expert personnel could be drawn from within the central counterparty. However, a review by personnel external to the central counterparty may also be necessary at times.

27 Central counterparties often calculate exposures for a shorter period, commonly one day, and, when necessary, scale up to cover the liquidation period. A central counterparty should be cautious when scaling because the standard square-root of time heuristic is not appropriate for prices that are serially correlated or exhibit non-linear dynamics.

liquidity for close out or hedging, and the potential for non-linear risk exposures posed by certain products, including jump-to-default risks. Where a central counterparty calculates margin at the sub-portfolio level or by product, initial margin requirements must be met for the corresponding distributions of future exposure at a stage prior to margining among sub-portfolios or products. A central counterparty should have the authority and operational capacity to make intraday initial margin calls, both scheduled and unscheduled, to its participants.

6.3.2 A central counterparty should select an appropriate close out period for each product that it clears and document the close out periods and related analysis for each product type. A central counterparty should base its determination of the close out periods for its initial margin model upon historical price and liquidity data, as well as reasonably foreseeable events in a default scenario. The close out period should account for the impact of a participant's default on prevailing market conditions. Inferences about the potential impact of a default on the close out period should be based on historical adverse events in the product cleared, such as significant reductions in trading or other market dislocations. The close out period should be based on anticipated close out times in stressed market conditions but may also take into account a central counterparty's ability to hedge effectively the defaulter's portfolio. Further, close out periods should be set on a product-specific basis because less liquid products might require significantly longer close out periods. As a general guide, a central counterparty should assume a close out period of at least two business days, or at least five business days for less liquid markets. A central counterparty should also consider and address position concentrations, which can lengthen close out time frames and add to price volatility during close outs.

6.3.3 A central counterparty should select an appropriate sample period for its margin model to calculate required initial margin for each product that it clears and should document the period and related analysis for each product type. The amount of margin may be very sensitive to the sample period and the margin model. Selection of the period should be carefully examined based on the theoretical properties of the margin model and empirical tests on these properties using historical data. In certain instances, a central counterparty may need to determine margin levels using a shorter historical period to reflect new or current volatility in the market more effectively. Conversely, a central counterparty may need to determine margin levels based on a longer historical period in order to reflect past volatility. A central counterparty should also consider simulated data projections that would capture plausible events outside of the historical data especially for new products without enough history to cover stressed market conditions.

6.3.4 A central counterparty should identify and mitigate any credit exposure that may give rise to specific wrong-way risk. For example, participants in a central counterparty clearing credit default swaps should not be allowed to clear single-name credit default swaps on their own names or on the names of their legal affiliates. A central counterparty is expected to review its portfolio regularly in order to identify, monitor and mitigate promptly any exposures that give rise to specific wrong-way risk.

6.3.5 A central counterparty should appropriately and where practicable address procyclicality in its margin arrangements (see CCP Standard 5.4). In this context, procyclicality typically refers to changes in risk management practices that are positively correlated with market, business or credit cycle fluctuations and that may cause or exacerbate financial instability. For example, in a period of rising price volatility or credit risk of participants, a central counterparty may require additional initial margin for a given portfolio beyond the amount required by the current margin model. This could exacerbate market

stress and volatility further, resulting in additional margin requirements. These adverse effects may occur without any arbitrary change in risk management practices. To the extent practicable and prudent, a central counterparty should adopt forward-looking and relatively stable and conservative margin requirements that are specifically designed to limit the need for potentially destabilising, procyclical changes. To support this objective, a central counterparty could consider increasing the size of its prefunded default arrangements to limit the need for and likelihood of large or unexpected margin calls in times of market stress. These procedures may create additional costs for central counterparties and their participants in periods of low market volatility due to higher margin or prefunded default arrangement contributions, but they may also result in additional protection and potentially less costly and less disruptive adjustments in periods of high market volatility. In addition, transparency regarding margin practices when market volatility increases may help mitigate the effects of procyclicality.

6.4 A central counterparty should mark participant positions to market and collect variation margin at least daily to limit the build-up of current exposures. A central counterparty should have the authority and operational capacity to make intraday margin calls and payments, both scheduled and unscheduled, to participants.

Variation margin

6.4.1 A central counterparty faces the risk that its exposure to its participants can change rapidly as a result of changes in prices, positions, or both. Adverse price movements, as well as participants building larger positions through new trading, can rapidly increase a central counterparty's exposures to its participants (although some markets may impose trading limits or position limits that reduce this risk). A central counterparty can ascertain its current exposure to each participant by marking each participant's outstanding positions to current market prices. To the extent permitted by a central counterparty's rules and supported by law, the central counterparty should net any gains against any losses and require frequent (at least daily) settlement of gains and losses. This settlement should involve the daily (and, when appropriate, intraday) collection of variation margin from participants whose positions have lost value and can include payments to participants whose positions have gained value. The regular collection of variation margin prevents current exposures from accumulating and mitigates the potential future exposures a central counterparty might face. A central counterparty should also have the authority and operational capacity to make intraday variation margin calls and payments, both scheduled and unscheduled, to its participants. A central counterparty should consider the potential impact of its intraday variation margin collections and payments on the liquidity position of its participants and should have the operational capacity to make intraday variation margin payments.

Timeliness and possession of margin payments

6.4.2 A central counterparty should establish and rigorously enforce timelines for margin collections and payments and set appropriate consequences for failure to pay on time. Margin should be held by the central counterparty until the associated exposure has been extinguished; that is, margin should not be returned before settlement or close out of an exposure is successfully concluded.

6.5 In calculating margin requirements, a central counterparty may allow offsets or reductions in required margin across products that it clears or between products that it and another central counterparty clear, if the risk of one product is significantly and reliably correlated with the risk

of the other product. Where a central counterparty enters into a cross-margining arrangement with one or more other central counterparties, appropriate safeguards should be put in place and steps should be taken to harmonise overall risk management systems. Prior to entering into such an arrangement, a central counterparty should consult with the Reserve Bank.

Portfolio margining

6.5.1 In calculating margin requirements, a central counterparty may allow offsets or reductions in required margin amounts between products for which it is the counterparty if the risk of one product is significantly and reliably correlated with the risk of another product.[28] A central counterparty should base such offsets on an economically meaningful methodology that reflects the degree of price dependence between the products. Often, price dependence is modelled through correlations, but more complete or robust measures of dependence should be considered, particularly for products with non-linear risks. In any case, the central counterparty should consider how price dependence can vary with overall market conditions, including stressed market conditions. Following the application of offsets, the central counterparty needs to ensure that the margin continues to meet or exceed the single-tailed confidence level of at least 99 per cent with respect to the estimated distribution of the future exposure of the portfolio. If a central counter party uses portfolio margining, it should continuously review and test offsets among products. It should test the robustness of its portfolio method on both actual and appropriate hypothetical portfolios. It is especially important to test how correlations perform during periods of actual and simulated market stress to assess whether the correlations break down or otherwise behave erratically. Prudent assumptions informed by these tests should be made about product offsets.

Cross-margining

6.5.2 A central counterparty may enter into a cross-margining arrangement, which is an agreement with one or more other central counterparties to consider positions and supporting collateral at their respective organisations as a common portfolio for participants that are members of two or more of the organisations (see also CCP Standard 19 on FMI links). A central counterparty may reduce the aggregate collateral requirements for positions held in cross-margined accounts if the value of the positions held at the parties to the cross-margining arrangement move inversely in a significant and reliable fashion.

6.5.3 A central counterparty that participates in a cross-margining arrangement must share information frequently with other central counterparties in the arrangement and ensure that it has appropriate safeguards, such as joint monitoring of positions, margin collections and price information. The central counterparty must thoroughly understand the other central counterparties' respective risk management practices and financial resources. The central counterparty should also take steps to harmonise its overall risk management systems with those of the other central counterparties, and should regularly monitor possible discrepancies in the calculation of exposures, especially with regard to monitoring how price correlations perform over time. This harmonisation is especially relevant in terms of selecting an initial margin methodology, setting margin parameters, segregating accounts and collateral, and establishing default management arrangements. All of the precautions with regard to portfolio margining discussed in paragraph 6.5.1 also apply to cross-margining regimes between or

28 Effects on the value of positions in the two products will also depend on whether these positions are long or short positions.

among central counterparties. A central counterparty that is party to a cross-margining arrangement should also analyse fully the impact of cross-margining on prefunded default arrangements and on the adequacy of its overall financial resources. Each participating central counterparty should have in place arrangements that are legally robust and operationally viable to govern the cross-margining arrangement.

6.5.4 A central counterparty should consult with the Reserve Bank prior to entering into a cross-margining arrangement with another central counterparty. The central counterparty should be able to demonstrate the safeguards it has in place and provide information regarding its risk management systems and those of the other central counterparties involved in the cross-margining arrangement. Prior to entering into the cross-margining arrangement, the central counterparty should ascertain that the Reserve Bank is satisfied that to do so would not weaken its compliance with the CCP Standards, and should implement any additional controls or mitigants identified in consultation with the Reserve Bank.

6.6 A central counterparty should analyse and monitor its model performance and overall margin coverage by conducting rigorous daily backtesting and at least monthly, and more frequent where appropriate, sensitivity analysis. A central counterparty should regularly conduct an assessment of the theoretical and empirical properties of its margin model for all products it clears. In conducting sensitivity analysis of the model's coverage, a central counterparty should take into account a wide range of parameters and assumptions that reflect possible market conditions, including the most volatile periods that have been experienced by the markets it serves and extreme changes in the correlations between prices.

6.6.1 In order to validate its margin models and parameters, a central counterparty should have a backtesting program that tests its initial margin models against identified targets. Backtesting is an *ex post* comparison of observed outcomes with the outputs of the margin models. A central counterparty should also conduct sensitivity analysis to assess the coverage of the margin methodology under various market conditions, using historical data from realised stressed market conditions and hypothetical data for unrealised stressed market conditions. Sensitivity analysis should also be used to determine the impact of varying important model parameters. Sensitivity analysis is an effective tool to explore hidden shortcomings that cannot be discovered through backtesting. The results of both the backtesting and sensitivity analyses should be disclosed to participants.

6.6.2 A central counterparty should backtest its margin coverage using participant positions from each day in order to evaluate whether there are any exceptions to its initial margin coverage. This assessment of margin coverage should be considered an integral part of the evaluation of the model's performance. Coverage should be evaluated across products and participants and take into account portfolio effects across asset classes within the central counterparty. The initial margin model's actual coverage, along with projected measures of its performance, should meet at least the established single-tailed confidence level of 99 per cent with respect to the estimated distribution of future exposure over an appropriate close out period.[29] In case backtesting indicates that the model did not perform as expected (that is, the model did not identify the appropriate amount of initial margin necessary to

29 This period should be appropriate to capture the risk characteristics of the specific instrument in order to allow the central counterparty to estimate the magnitude of the price changes expected to occur in the interval between the last margin collection and the time the central counterparty estimates it will be able to close out the relevant positions.

achieve the intended coverage), a central counterparty should have clear procedures for recalibrating its margining system, such as by making adjustments to parameters and sampling periods. In addition, a central counterparty should analyse the source of any exceptions to initial margin coverage identified through backtesting, to determine if a fundamental change to the margin methodology is warranted or if only the recalibration of current parameters is necessary. Backtesting procedures alone are not sufficient to evaluate the effectiveness of models and adequacy of financial resources against forward-looking risks.

6.6.3 A central counterparty should test the sensitivity of its margin model coverage using a wide range of parameters and assumptions that reflect possible market conditions in order to understand how the level of margin coverage might be affected by highly stressed market conditions. The central counterparty should ensure that the range of parameters and assumptions captures a variety of historical and hypothetical conditions, including the most volatile periods that have been experienced by the markets it serves and extreme changes in the correlations between prices. The central counterparty should conduct sensitivity analysis incorporating stressed market conditions on its margin model coverage at least monthly and conduct a thorough analysis of the potential losses it could suffer. A central counterparty should evaluate the potential losses in individual participants' positions and, where appropriate, their customers' positions. Furthermore, for a central counterparty clearing credit instruments, parameters reflective of the simultaneous default of both participants and issuers of the underlying credit instruments should be considered. Sensitivity analysis should be performed on both actual and simulated positions. Rigorous sensitivity analysis of margin requirements may take on increased importance when markets are illiquid or volatile. This analysis should be conducted more frequently when markets are unusually volatile or less liquid or when the size or concentration of positions held by its participants increases significantly.

6.7 A central counterparty should regularly review and validate its margin system.

6.7.1 A central counterparty's margin methodology should be reviewed and validated by a qualified and independent party at least annually, or more frequently if there are material market developments. Any material revisions or adjustments to the methodology or parameters should be subject to appropriate governance processes (see also CCP Standard 2 on governance) and validated prior to implementation. A central counterparty that is party to a cross-margining arrangement should also analyse the impact of cross-margining on prefunded default arrangements and evaluate the adequacy of its overall financial resources (see CCP Standard 6.5). Also, the margin methodology, including the initial margin models and parameters used by a central counterparty, should be made as transparent as possible. At a minimum, the basic assumptions of the analytical method selected and the key data inputs should be disclosed to participants. A central counterparty should make details of its margin methodology available to its participants for use in their individual risk management efforts.

6.8 In designing its margin system, a central counterparty should consider the operating hours of payment and settlement systems in the markets in which it operates.

6.8.1 A central counterparty with participants in a range of time zones may need to adjust its procedures for margining (including the times at which it makes margin calls) to take into account the liquidity of a participant's local funding market and the operating hours of relevant payment and settlement systems. The extent to which a central counterparty's margining procedures should take into account local operating hours in a particular jurisdiction will depend on the extent of local participation

and the relative costs of any adjustments required to its operations. A central counterparty with material Australian-based participation that clears Australian dollar-denominated products for which the greatest depth of liquidity is in Australian markets should consider making margin calls during Australian market hours and in Australian dollars.

Standard 7: Liquidity risk

A central counterparty should effectively measure, monitor and manage its liquidity risk. A central counterparty should maintain sufficient liquid resources in all relevant currencies to effect same-day and, where appropriate, intraday and multiday settlement of payment obligations with a high degree of confidence under a wide range of potential stress scenarios that should include, but not be limited to, the default of the participant and its affiliates that would generate the largest aggregate liquidity obligation for the central counterparty in extreme but plausible market conditions.

Guidance

Liquidity risk arises in a central counterparty when it, its participants, or other entities cannot settle their payment obligations when due as part of the clearing or settlement process. Depending on the design of a central counterparty, liquidity risk can arise between the central counterparty and its participants, or between the central counterparty and other entities (such as commercial bank money settlement agents, nostro agents, custodian banks and liquidity providers). It is particularly important for a central counterparty to manage carefully its liquidity risk if, as is typical in many systems, the central counterparty relies on incoming payments from participants or other entities during the settlement process in order to make payments to other participants. If a participant or another entity fails to pay the central counterparty, the central counterparty may not have sufficient funds to meet its payment obligations to other participants. In such an event, the central counterparty would need to rely on its own liquid resources (that is, liquid assets and prearranged funding arrangements, including any arrangements with its participants) to cover the funds shortfall and complete settlement. A central counterparty should have a robust framework to manage its liquidity risks from the full range of participants and other entities. In some cases, a participant may play other roles within the central counterparty, such as a settlement or custodian bank or liquidity provider. These other roles should be considered in determining a central counterparty's liquidity needs.

7.1 A central counterparty should have a robust framework to manage its liquidity risks from its participants, commercial bank money settlement agents, nostro agents, custodians, liquidity providers and other entities.

Sources of liquidity risk

7.1.1 A central counterparty should clearly identify its sources of liquidity risk and assess its current and potential future liquidity needs on a daily basis. A central counterparty can face liquidity risk from the default of a participant. For example, a central counterparty might not be able to convert a defaulting participant's collateral into cash at short notice. A central counterparty can also face liquidity risk from any commercial bank money settlement agents, nostro agents, custodians and liquidity providers, as well as linked FMIs and service providers, if they fail to perform as expected. Moreover, as noted above, a central counterparty may face additional risk from entities that have multiple roles within the central counterparty (for example, a participant that also serves as the central counterparty's money

settlement agent or liquidity provider). These interdependencies and the multiple roles that an entity may assume within a central counterparty should be taken into account by the central counterparty.

Managing liquidity risk

7.1.2 A central counterparty should regularly assess its design and operations to manage liquidity risk in the system. It could reduce the liquidity demands of its participants by providing participants with sufficient information or control systems to help them manage their liquidity needs and risks. Furthermore, a central counterparty should ensure that it is operationally ready to manage the liquidity risk caused by participants' or other entities' financial or operational problems. Among other things, a central counterparty that does not settle its funds obligations directly in central bank money (see CCP Standard 9 on money settlements) should have the operational capacity to reroute payments, where feasible, on a timely basis in case of problems with a correspondent bank.

7.1.3 A central counterparty may use other risk management tools to manage its liquidity risk. To mitigate and manage liquidity risk stemming from a participant default, a central counterparty could use, either individually or in combination, exposure limits, collateral requirements and prefunded default resources. To mitigate and manage liquidity risk stemming from a service provider or a linked FMI, a central counterparty could use, individually or in combination, selection criteria, concentration or exposure limits, and collateral requirements. For example, a central counterparty should seek to manage or diversify its liquid resources to avoid excessive intraday or overnight exposure to one entity. This, however, may involve trade-offs between the efficiency of relying on an entity and the risks of being overly dependent on that entity.

7.2 A central counterparty should have effective operational and analytical tools to identify, measure and monitor its settlement and funding flows on an ongoing and timely basis, including its use of intraday liquidity.

7.2.1 A central counterparty should have effective operational and analytical tools to identify, measure and monitor its settlement and funding flows on an ongoing and timely basis, including its use of intraday liquidity. In particular, a central counterparty should understand and assess the value and concentration of its daily settlement and funding flows through any commercial bank money settlement agents, nostro agents and other intermediaries. A central counterparty also should be able to monitor on a daily basis the level of liquid assets (such as cash, securities, other assets held in custody and investments) that it holds. A central counterparty should be able to determine the value of its available liquid assets, taking into account the appropriate haircuts on those assets (see CCP Standard 5 on collateral and CCP Standard 6 on margin).

7.2.2 If a central counterparty maintains prearranged funding arrangements, the central counterparty should also identify, measure and monitor its liquidity risk from the liquidity providers of those arrangements. A central counterparty should obtain a high degree of confidence through rigorous due diligence that each liquidity provider, whether or not it is a participant in the central counterparty, would have the capacity to perform as required under the liquidity arrangement and is subject to commensurate regulation, supervision or oversight of its liquidity risk management requirements. Where relevant to assessing a liquidity provider's performance reliability with respect to a particular currency, the liquidity provider's potential access to credit from the relevant central bank may be taken into account.

7.3 A central counterparty should maintain sufficient liquid resources in all relevant currencies to settle securities-related payments, make required variation margin payments and meet other payment obligations on time with a high degree of confidence under a wide range of potential stress scenarios that should include, but not be limited to, the default of the participant and its affiliates that would generate the largest aggregate payment obligation to the central counterparty in extreme but plausible market conditions. In addition, a central counterparty that is involved in activities with a more complex risk profile or that is systemically important in multiple jurisdictions should consider maintaining additional liquidity resources sufficient to cover a wider range of potential stress scenarios that should include, but not be limited to, the default of the two participants and their affiliates that would generate the largest aggregate payment obligation to the central counterparty in extreme but plausible market conditions.

7.3.1 A central counterparty should carefully analyse its projected liquidity needs under a range of stress scenarios, and subject this analysis to review by the Reserve Bank and other relevant authorities. In many cases, a central counterparty will need to maintain sufficient liquid resources to meet payments to settle required margin and other payment obligations over multiple days to accommodate multiday hedging and close out activities as directed by the central counterparty's participant default procedures (see CCP Standard 7.8 on liquidity stress testing).

7.4 For the purpose of meeting its minimum liquid resource requirement, a central counterparty's qualifying liquid resources in each currency include cash at the central bank of issue and at creditworthy commercial banks, committed lines of credit, committed foreign exchange swaps and committed repos, as well as highly marketable collateral held in custody and investments that are readily available and convertible into cash with prearranged and highly reliable funding arrangements, even in extreme but plausible market conditions. If a central counterparty has access to routine credit at the central bank of issue, the central counterparty may count such access as part of the minimum requirement to the extent it has collateral that is eligible for pledging to (or for conducting other appropriate forms of transactions with) the relevant central bank. All such resources should be available when needed.

7.4.1 A central counterparty's outright holdings of qualifying instruments, such as cash and assets eligible for pledging as collateral to (or for conducting other collateralised transactions with) the central bank of issue, are generally the most reliable source of liquidity and should form a substantial part of a central counterparty's qualifying liquid resources (see CCP Standard 7.7).

7.4.2 In addition to outright holdings of qualifying instruments, a central counterparty may negotiate committed lines of credit and repos on commercial terms with external third parties. A central counterparty may also conclude contractual agreements with its participants to provide additional qualifying liquid resources in specified circumstances. Such resources may, for example, be provided under committed lines of credit or committed repos. Any such arrangements should be highly reliable and explicitly included in the central counterparty's rules and procedures, ensuring that they have at least as robust a contractual basis as any equivalent commercial arrangement that might be reached with non-participant counterparties.

7.5 A central counterparty may supplement its qualifying liquid resources with other forms of liquid resources. If the central counterparty does so, these liquid resources should be in the form of assets that are likely to be saleable or acceptable as collateral for lines of credit, swaps or repos on an ad hoc basis following a default, even if this cannot be reliably prearranged or guaranteed in extreme market conditions. Even if a central counterparty does not have access to routine central bank credit, it should still take account of what collateral is typically accepted by the relevant central bank, as such assets may be more likely to be liquid in stressed circumstances. A central counterparty should not assume the availability of emergency central bank credit as part of its liquidity plan.

7.5.1 A central counterparty may consider using non-qualifying liquid resources within its liquidity risk management framework in advance of, or in addition to, using its qualifying liquid resources. This may be particularly beneficial where liquidity needs exceed qualifying liquid resources, where qualifying liquid resources can be preserved to cover a future default, or where using other liquid resources would cause less liquidity dislocation to the central counterparty's participants and the financial system as a whole.

7.6 A central counterparty should obtain a high degree of confidence, through rigorous due diligence, that each provider of its minimum required qualifying liquid resources, whether a participant of the central counterparty or an external party, has sufficient information to understand and to manage its associated liquidity risks, and that it has the capacity to perform as required under its commitment. Where relevant to assessing a liquidity provider's performance reliability with respect to a particular currency, a liquidity provider's potential access to credit from the central bank of issue may be taken into account. A central counterparty should regularly test its procedures for accessing its liquid resources at a liquidity provider.

7.6.1 A central counterparty should have detailed procedures for using its liquid resources to complete settlement during a liquidity shortfall. A central counterparty's procedures should clearly document the sequence in which each type of liquid resource would be expected to be used (for example, the use of certain assets before prearranged funding arrangements). These procedures may include instructions for accessing cash deposits or overnight investments of cash deposits, executing same-day market transactions, or drawing on prearranged liquidity lines, including any pre-committed liquidity allocation mechanisms involving participants established under the central counterparty's rules. In addition, a central counterparty should regularly test its procedures for accessing its liquid resources at a liquidity provider, including by activating and drawing down test amounts from committed credit facilities and by testing operational procedures for conducting same-day repos. A central counterparty should also adequately plan for the renewal of prearranged funding arrangements with liquidity providers in advance of their expiration.

7.7 A central counterparty with access to central bank accounts, payment services or securities services should use these services, where practical, to enhance its management of liquidity risk. A central counterparty that the Reserve Bank determines to be systemically important in Australia and has obligations in Australian dollars should operate its own Exchange Settlement Account, in its own name or that of a related body corporate acceptable to the Reserve Bank, to enhance its management of Australian dollar liquidity risk.

7.7.1 If a central counterparty has access to central bank accounts, payment services, securities services or collateral management services, it should use these services, where practical, to enhance its management of liquidity risk. Cash balances at the central bank of issue, for example, offer the highest liquidity (see CCP Standard 9 on money settlements).

7.7.2 A central counterparty that the Reserve Bank determines to be systemically important in Australia and has obligations in Australian dollars should operate its own Exchange Settlement Account at the Reserve Bank to enhance its management of Australian dollar liquidity risk.[30] This account may be held in the central counterparty's own name or, if approved by the Reserve Bank, in the name of a related body corporate. A holder of an Exchange Settlement Account may access the Reserve Bank's overnight and intraday liquidity facilities, provided it meets the Reserve Bank's other requirements for access to these facilities, including that it can deliver securities eligible as collateral to the Reserve Bank under a repo agreement. In assessing the systemic importance of a central counterparty, the Reserve Bank will consider factors such as:

- the size of the central counterparty in Australia (for example, the value of transactions processed by the central counterparty in Australian dollar-denominated products, or its market share; or the total amount of initial margin held in respect of Australian dollar-denominated products)
- the availability of substitutes for the central counterparty's services in Australia
- the nature and complexity of the products cleared by the central counterparty
- the degree of interconnectedness with other parts of the Australian financial system.

7.8 A central counterparty should determine the amount and regularly test the sufficiency of its liquid resources through rigorous stress testing. A central counterparty should have clear procedures to report the results of its stress tests to appropriate decision-makers at the central counterparty and to use these results to evaluate the adequacy of, and adjust, its liquidity risk management framework. In conducting stress testing, a central counterparty should consider a wide range of relevant scenarios. Scenarios should include relevant peak historic price volatilities, shifts in other market factors such as price determinants and yield curves, multiple defaults over various time horizons, simultaneous pressures in funding and asset markets, and a spectrum of forward-looking stress scenarios in a variety of extreme but plausible market conditions. Scenarios should also take into account the design and operation of the central counterparty, include all entities that might pose material liquidity risks to the central counterparty (such as commercial bank money settlement agents, nostro agents, custodians, liquidity providers and linked FMIs) and, where appropriate, cover a multiday period. In all cases, a central counterparty should document its supporting rationale for, and should have appropriate governance arrangements relating to, the amount and form of total liquid resources it maintains.

7.8.1 As part of a central counterparty's assessment of the sufficiency of its liquid resources through stress testing, it should consider any strong interlinkages or similar exposures between its participants, as well as the multiple roles that participants may play with respect to the risk management of the

30 The Reserve Bank has established a specific category of Exchange Settlement Account for central counterparties available at <http://www.rba.gov.au/media-releases/2012/mr-12-17.html>.

central counterparty, and assess the probability of multiple failures and the contagion effect among its participants that such failures may cause.

7.8.2 Liquidity stress testing should be performed on a daily basis using standard and predetermined parameters and assumptions. In addition, on at least a monthly basis, a central counterparty should perform a comprehensive and thorough analysis of stress-testing scenarios, models and underlying parameters and assumptions used to ensure they are appropriate for achieving the central counterparty's identified liquidity needs and resources in light of current and evolving market conditions. A central counterparty should perform stress testing more frequently when markets are unusually volatile, when they are less liquid, or when the size or concentration of positions held by its participants increases significantly. A full validation of a central counterparty's liquidity risk management model should be performed at least annually.

7.8.3 A central counterparty should conduct, as appropriate, reverse stress tests aimed at identifying the extreme default scenarios and extreme market conditions for which the central counterparty's liquid resources would be insufficient. In other words, these tests identify how severe stress conditions would be covered by the central counterparty's liquid resources. A central counterparty should judge whether it would be prudent to prepare for these severe conditions and various combinations of factors influencing these conditions. Reverse stress tests require a central counterparty to model extreme market conditions that may go beyond what are considered extreme but plausible market conditions in order to help understand the sufficiency of liquid resources given the underlying assumptions modelled. Modelling very extreme market conditions can help a central counterparty determine the limits of its current model and resources; however, it requires the central counterparty to exercise judgement when modelling different markets and products. A central counterparty should develop hypothetical very extreme scenarios and market conditions tailored to the specific risks of the markets and of the products it serves. Reverse stress tests should be considered a helpful risk management tool but they need not, necessarily, drive a central counterparty's determination of the appropriate level of liquid resources.

7.9 A central counterparty should establish explicit rules and procedures that enable the central counterparty to effect same-day and, where appropriate, intraday and multiday settlement of payment obligations on time following any individual or combined default among its participants. These rules and procedures should address unforeseen and potentially uncovered liquidity shortfalls and should aim to avoid unwinding, revoking or delaying the same-day settlement of payment obligations. These rules and procedures should also indicate the central counterparty's process to replenish any liquidity resources it may employ during a stress event, so that it can continue to operate in a safe and sound manner.

7.9.1 In certain extreme circumstances, the liquid resources of a central counterparty or its participants required under CCP Standard 7.3 may not be sufficient to meet the payment obligations of the central counterparty to its participants.[31] In a stressed environment, for example, normally liquid assets held by a central counterparty may prove not to be sufficiently liquid to obtain same-day funding, or the liquidation period may be longer than expected. A central counterparty should establish explicit rules and procedures that enable the central counterparty to effect same-day and, where appropriate, intraday and multiday settlement of payment obligations on time following any individual or

31 These exceptional circumstances could arise from unforeseen operational problems or unanticipated rapid changes in market conditions.

combined default among its participants. These rules and procedures should address unforeseen and potentially uncovered liquidity shortfalls and should aim to avoid unwinding, revoking or delaying the same-day settlement of payment obligations. These rules and procedures should also indicate the central counterparty's process to replenish any liquidity resources it may employ during a stress event, so that it can continue to operate in a safe and sound manner.

7.9.2 If a central counterparty allocates potentially uncovered liquidity shortfalls to its participants, the central counterparty should have clear and transparent rules and procedures for the allocation of shortfalls. These procedures could involve a funding arrangement between the central counterparty and its participants, the mutualisation of shortfalls among participants according to a clear and transparent formula, or the use of liquidity rationing (for example, reductions in payouts to participants). Any allocation rule or procedure must be discussed thoroughly with and communicated clearly to participants, as well as be consistent with participants' respective regulatory liquidity risk management requirements. Furthermore, a central counterparty should consider and validate, through simulations and other techniques and through discussions with each participant, the potential impact on each participant of any such same-day allocation of liquidity risk and each participant's ability to bear proposed liquidity allocations.

Standard 8: Settlement finality

A central counterparty should ensure clear and certain final settlement, at a minimum by the end of the value date. Where necessary or preferable, a central counterparty should facilitate final settlement intraday or in real time.

Guidance

A central counterparty should be designed to ensure clear and certain final settlement of payments, transfer instructions or other obligations. Final settlement is defined as the irrevocable and unconditional transfer of an asset or financial instrument, or the discharge of an obligation by the central counterparty or its participants in accordance with the terms of the underlying contract.[32] A payment, transfer instruction or other obligation that a central counterparty accepts for settlement in accordance with its rules and procedures should be settled with finality on the intended value date.[33] Completing final settlement by the end of the value date is important because deferring final settlement to the next business day can create both credit and liquidity pressures for a central counterparty's participants and other stakeholders, and potentially be a source of systemic risk. Where necessary or preferable, a central counterparty should ensure intraday or real-time settlement finality to reduce settlement risk. This will be necessary where transactions are settled through an intraday multilateral net batch or on a real-time basis.

Although some central counterparties guarantee settlement, this Standard does not require a central counterparty to provide such a guarantee. Instead, this Standard requires central counterparties to clearly define the point at which the settlement of a payment, transfer instruction or other obligation is final, and to ensure completion of the settlement process no later than the end of the value date, and preferably earlier

32 Final settlement (or settlement finality) is a legally defined moment. See also CCP Standard 1 on legal basis.

33 The value date of a central counterparty's settlement activity might not necessarily coincide with the exact calendar date if the central counterparty utilises night-time settlement.

on the value date. Similarly, this Standard is not intended to eliminate fails to deliver in securities trades.[34] The occurrence of non-systemic amounts of such failures, although potentially undesirable, should not by itself be interpreted as a failure to satisfy this Standard. However, a central counterparty should take steps to mitigate both the risks and the implications of such failures to deliver securities (see, in particular, CCP Standard 4 on credit risk and CCP Standard 7 on liquidity risk).

8.1 A central counterparty's rules and procedures should clearly define the point at which settlement is final.

8.1.1 A central counterparty's rules and procedures should clearly define the point at which settlement is final. A clear definition of when settlements are final also greatly assists in a resolution scenario such that the positions of the participant in resolution and other affected parties can be quickly ascertained.

8.1.2 A central counterparty's legal framework and rules generally determine finality. For a transaction to be considered final, the legal basis governing the central counterparty, including relevant insolvency law, must acknowledge the discharge of a payment, transfer instruction or other obligation between the central counterparty and system participants, or between or among participants (see CCP Standard 1.5). Where relevant, a central counterparty should take reasonable steps to confirm the effectiveness of cross-border recognition and protection of cross-system settlement finality, especially when it is developing plans for recovery or orderly wind-down or providing the Reserve Bank and other relevant authorities with information relating to its resolvability. Because of the complexity of legal frameworks and system rules, particularly in the context of cross-border settlement where legal frameworks are not harmonised, a well-reasoned legal opinion is generally necessary to establish the point at which finality takes place (see also CCP Standard 1 on legal basis).

8.2 A central counterparty should ensure final settlement no later than the end of the value date, and preferably intraday or in real time, to reduce settlement risk.

Same-day settlement

8.2.1 A central counterparty's arrangements should be designed to ensure final settlement, at a minimum no later than the end of the value date. This means that any payment, transfer instruction or other obligation that has been submitted to and accepted by a central counterparty in accordance with its risk management process and other relevant acceptance criteria should be settled on the intended value date. A central counterparty that is not designed to ensure final settlement on the value date (or same-day settlement) would not satisfy this Standard, even if the transaction's settlement date is adjusted back to the value date after settlement. This is because, in most such arrangements, there is no certainty that final settlement will occur on the value date as expected. Further, deferral of final settlement to the next business day can entail overnight risk exposures. For example, if a central counterparty conducts its money settlements using instruments or arrangements that involve next-day settlement, a participant's default on its settlement obligations between the initiation and finality of settlement could pose significant credit and liquidity risks to the central counterparty and its other participants.

34 These fails typically occur because of miscommunication between the counterparties, operational problems in the delivery of securities, or failure to acquire a specific security associated with the trade by a specific point in time.

Intraday settlement

8.2.2 Depending on the type of obligations that a central counterparty has, the use of intraday settlement, either in multiple batches or in real time, may be necessary or desirable to reduce settlement risk. Accordingly, a central counterparty should consider the use of real-time gross settlement (RTGS) or multiple batch settlement to complete final settlement intraday. A central counterparty should, for instance, settle margin intraday, preferably via RTGS. If a central counterparty does settle margin via batch settlement, the batch process should not include settlement of non-margin obligations or obligations associated with unrelated products. The timely settlement of margins is a critical component of a central counterparty's risk management process and should not be dependent on the settlement of other transactions. Any time lag between the acceptance and final settlement of instructions should also be minimised where batch settlement is used.

8.3 A central counterparty should clearly define the point after which unsettled payments, transfer instructions or other obligations may not be revoked by a participant.

8.3.1 A central counterparty should clearly define the point after which unsettled payments, transfer instructions or other obligations may not be revoked by a participant. In general, a central counterparty should prohibit the unilateral revocation of accepted and unsettled payments, transfer instructions or other obligations after a certain point or time in the settlement day, so as to avoid creating liquidity risks. In all cases, cut-off times and materiality rules for exceptions should be clearly defined. The rules should make clear that changes to operating hours are exceptional and require individual justifications. For example, a central counterparty may want to permit extensions for reasons connected with broader financial market disruption. If extensions are allowed for participants with operating problems to complete processing, the rules governing the approval and duration of such extensions should be clear to participants.

Standard 9: Money settlements

A central counterparty should conduct its money settlements in central bank money where practical and available. If central bank money is not used, a central counterparty should minimise and strictly control the credit and liquidity risk arising from the use of commercial bank money.

Guidance

A central counterparty typically needs to conduct money settlements with or between its participants for a variety of purposes, such as the settlement of individual payment obligations, funding and defunding activities, and the collection and distribution of margin payments. To conduct such money settlements, a central counterparty can use central bank money, commercial bank money or a combination of the two. Where individual payment obligations are settled in commercial bank money, exposures are typically created between commercial banks, which are ultimately settled in central bank money. A central counterparty may not specify how participants fund their obligations. However, the central counterparty, its participants, any commercial settlement banks and any commercial bank money settlement agents should take into account the risks associated with alternative money settlement arrangements.

Settlement in central bank money typically involves the central bank of issue assuming the role of money settlement agent, with final money settlement occurring across accounts held by participants or their

commercial settlement banks with the central bank. Typically, this sort of arrangement for the settlement of individual transactions minimises the accrual of exposures between commercial settlement banks.

Settlement in commercial bank money typically occurs on the books of a commercial bank money settlement agent. In this model, a central counterparty typically establishes an account with one or more commercial bank(s) and requires each of its participants to establish an account with one of them. In some cases, the central counterparty itself can serve as the money settlement agent, in which case money settlements are effected through accounts on the books of the central counterparty. A central counterparty may also use a combination of central bank and commercial bank monies to conduct settlements, for example, by using central bank money for funding accounts at commercial banks, prior to settlement of individual payment obligations in commercial bank money across those accounts.

A central counterparty and its participants may face credit and liquidity risks from money settlements. Credit risk may arise when participants use commercial settlement banks to effect money settlements, or when the central counterparty uses a commercial bank money settlement agent. Liquidity risk may arise in money settlements if, after a payment obligation has been settled, participants or the central counterparty itself are unable to transfer readily their assets at the commercial settlement bank, or money settlement agent, into other liquid assets, such as claims on a central bank.

9.1 A central counterparty should conduct its money settlements in central bank money, where practical and available, to avoid credit and liquidity risks. A central counterparty that the Reserve Bank determines to be systemically important in Australia and has Australian dollar obligations should settle its Australian dollar obligations across an Exchange Settlement Account held at the Reserve Bank, in its own name or that of a related body corporate acceptable to the Reserve Bank.

9.1.1 With the use of central bank money, a payment obligation is typically discharged by providing the central counterparty, its participants or its participants' commercial settlement banks with a direct claim on the central bank; that is, the relevant central bank is the money settlement agent, and the settlement asset is central bank money. Central banks have the lowest credit risk and are the source of liquidity with regard to their currency of issue. However, the use of central bank money may not always be practical or available. For example, a central counterparty or its participants may not have direct access to central bank accounts and payment services in all relevant jurisdictions.

9.1.2 In Australia, a central counterparty may apply to hold an Exchange Settlement Account at the Reserve Bank, in its own name or that of a related body corporate acceptable to the Reserve Bank, provided that it meets any associated financial, operational and legal requirements.[35] Further, a central counterparty that the Reserve Bank determines to be systemically important in Australia and has obligations in Australian dollars should operate its own Exchange Settlement Account, in its own name or that of a related body corporate acceptable to the Reserve Bank, to settle its Australian dollar obligations. In determining whether a central counterparty is systemically important in Australia the Reserve Bank will have regard to relevant factors, including those listed in paragraph 7.7.2.

9.2 If central bank money is not used, a central counterparty should conduct its money settlements using a settlement asset with little or no credit or liquidity risk.

35 See the Reserve Bank's policy on Exchange Settlement Accounts for central counterparties, available at <http://www.rba.gov.au/media-releases/2012/mr-12-17.html>.

9.2.1 An alternative to the use of central bank money is commercial bank money. When settling in commercial bank money, a payment obligation is typically discharged by providing the central counterparty or its participants with a direct claim on a commercial bank money settlement agent. To conduct settlements in commercial bank money, a central counterparty and its participants need to establish accounts with at least one commercial bank, and likely hold intraday or overnight balances, or both. The use of commercial bank money to settle payment obligations, however, can create additional credit and liquidity risks for the central counterparty and its participants. For example, if a commercial bank money settlement agent became insolvent, the central counterparty and its participants might not have immediate access to their settlement funds or ultimately receive the full value of their funds. It also creates operational dependencies on the relevant commercial bank(s).

9.3 If a central counterparty settles in commercial bank money or its participants effect settlements using commercial settlement banks, it should monitor, manage and limit credit and liquidity risks arising from the commercial bank money settlement agents and commercial settlement banks. In particular, a central counterparty should establish and monitor adherence to strict criteria for commercial banks appropriate to their role in the settlement process, taking account of matters such as their regulation and supervision, creditworthiness, capitalisation, access to liquidity and operational reliability. A central counterparty should also monitor and manage the concentration of its and its participants' credit and liquidity exposures to commercial bank money settlement agents and settlement banks.

9.3.1 If a central counterparty uses a commercial bank money settlement agent (or a non-bank deposit-taking institution) for its money settlements, it should monitor, manage and limit its credit and liquidity risks arising from this arrangement. For example, a central counterparty should limit both the probability of being exposed to the bank's failure and limit the potential losses and liquidity pressures to which it would be exposed in the event of such a failure. A central counterparty should establish and monitor adherence to strict criteria for its commercial bank money settlement agents that take into account, among other things, their regulation and supervision, creditworthiness, capitalisation, access to liquidity and operational reliability. Under these criteria, a commercial bank money settlement agent should be subject to effective banking regulation and supervision. It should also be creditworthy, be well capitalised and have ample liquidity from the marketplace or the central bank of issue. Where money settlements take place in Australian dollars, a central counterparty should only utilise an authorised deposit-taking institution (ADI) that holds an Exchange Settlement Account at the Reserve Bank and has been approved to act as an agent for RTGS payments by the Australian Prudential Regulation Authority.

9.3.2 Even where ultimate settlement occurs in central bank money, many participants in a central counterparty may not have direct access to accounts with the relevant central bank. They will therefore typically use the services of commercial settlement banks to effect money settlements or carry out funding and defunding activities. These commercial settlement banks play an important role in the settlement of payment obligations (including margin payments) and therefore the central counterparty should establish appropriate criteria around their financial and operational capacity to fulfil this role, which may include similar criteria to those described in paragraph 9.3.1 (see also CCP Standard 12 on participant default rules and procedures).

9.3.3 In addition, a central counterparty should monitor and manage the concentration of its and, to the extent reasonably practicable, its participants' credit and liquidity exposures to commercial bank money settlement agents and commercial settlement banks. The central counterparty should consider the diversification of its and its participants' exposures to commercial banks in the settlement process and assess its potential losses and liquidity pressures as well as those of its participants in the event of the failure of a commercial bank money settlement agent or commercial settlement bank (see also CCP Standard 18 on tiered participation arrangements).

9.4 If a central counterparty conducts money settlements on its own books, it should minimise and strictly control its credit and liquidity risks.

9.4.1 Where a central counterparty conducts money settlements on its own books, it offers cash accounts to its participants, and a payment or settlement obligation is discharged by providing the central counterparty's participants with a direct claim on the central counterparty itself. The credit and liquidity risks associated with a claim on a central counterparty are therefore directly related to the central counterparty's overall credit and liquidity risks. A central counterparty should look to minimise these risks by limiting its activities and operations to clearing and closely related processes (see CCP Standard 1.1). Further, to settle payment obligations, the central counterparty could be established as a supervised special purpose financial institution and limit the provision of cash accounts to participants. In some cases, a central counterparty can further mitigate risk by having participants fund and defund their cash accounts at the central counterparty using central bank money. In such an arrangement, a central counterparty is able to back the settlements conducted on its own books with balances that it holds in its account at the central bank.

9.5 A central counterparty's legal agreements with any commercial bank money settlement agents should state clearly when transfers on the books of the relevant commercial bank are expected to occur, that transfers are to be final when effected, and that funds received should be transferable as soon as possible, at a minimum by the end of the day and ideally intraday, in order to enable the central counterparty and its participants to manage credit and liquidity risks.

9.5.1 In settlements involving either central bank or commercial bank money, a critical issue is the timing of the finality of funds transfers. These transfers should be final when effected (see also CCP Standard 1 on legal basis and CCP Standard 8 on settlement finality). To this end, a central counterparty's legal agreements with any commercial bank money settlement agent should contain clear provisions regarding the finality of funds transfers. The central counterparty should communicate the effect of these provisions to participants. Participants' legal agreements with commercial settlement banks should similarly provide clarity in relation to these matters, although in some cases a central counterparty may not have access to these agreements. If a central counterparty conducts intraday money settlements (for example, to collect intraday margin), the arrangement should provide real-time finality or intraday finality at the times when a central counterparty wishes to effect money settlement.

Standard 10: Physical deliveries

A central counterparty should clearly state its obligations with respect to the delivery of physical instruments or commodities and should identify, monitor and manage the risks associated with such physical deliveries.

Guidance

A central counterparty may take on obligations involving the settlement of transactions using physical delivery, which is the delivery of an asset, such as an instrument or a commodity, in physical form.[36] For example, the settlement of futures contracts cleared by a central counterparty may allow or require the physical delivery of an underlying financial instrument or commodity. A central counterparty that provides physical settlement should have rules that clearly state its obligations with respect to the delivery of physical instruments or commodities.[37] In addition, a central counterparty should identify, monitor and manage the risks and costs associated with the storage and delivery of such physical instruments and commodities.

10.1 A central counterparty's rules should clearly state its obligations with respect to the delivery of physical instruments or commodities.

10.1.1 A central counterparty's rules should clearly state its obligations with respect to the delivery of physical instruments or commodities. The obligations that a central counterparty may assume with respect to physical deliveries vary based on the types of assets that the central counterparty settles. A central counterparty should clearly state which asset classes it accepts for physical delivery and the procedures surrounding the delivery of each. A central counterparty also should clearly state whether its obligation is to make or receive physical deliveries or to indemnify participants for losses incurred in the delivery process. Clear rules on physical deliveries enable the central counterparty and its participants to take the appropriate steps to mitigate the risks posed by such physical deliveries. A central counterparty should engage with its participants to ensure that they have an understanding of their obligations and the procedures for effecting physical delivery.

10.2 A central counterparty should identify, monitor and manage the risks and costs associated with the storage and delivery of physical instruments or commodities.

Risk of storage and delivery

10.2.1 A central counterparty should identify, monitor and manage the risks and costs associated with the storage and delivery of physical instruments or commodities. Issues relating to delivery may arise, for example, when a derivatives contract requires physical delivery of an underlying instrument or commodity. A central counterparty should plan for and manage physical deliveries by, for example, establishing: definitions for acceptable physical instruments or commodities; the appropriateness of alternative delivery locations or assets; rules for warehouse operations; and the timing of delivery, when relevant. If a central counterparty is responsible for the warehousing and transportation of a commodity, it should make arrangements that take into account the commodity's particular

36 Examples of physical instruments that may be covered under this Standard include securities, commercial paper and other debt instruments that are issued in paper form.

37 The term 'physical delivery' in the credit default swap market typically refers to the process by which the protection buyer of a credit default swap contract 'delivers' an instrument to the protection seller after a credit event, but does not necessarily involve the delivery of an instrument in paper form. This type of 'physical delivery' is outside the scope of this Standard.

characteristics (for example, storage under specific conditions, such as an appropriate temperature and humidity for perishables).

10.2.2 A central counterparty should have appropriate processes, procedures and controls to manage the risks of storing and delivering physical assets, such as the risk of theft, loss, counterfeiting or deterioration of assets. A central counterparty's policies and procedures should ensure that the central counterparty's record of physical assets accurately reflects its holdings of assets, for example, by separating duties between handling physical assets and maintaining records. A central counterparty also should have appropriate employment policies and procedures for personnel that handle physical assets and should include appropriate pre-employment checks and training. In addition, a central counterparty should consider other measures, such as insurance coverage and random storage facility audits, to mitigate its storage and delivery risks (other than principal risk).

Matching participants for delivery and receipt

10.2.3 In some instances, a central counterparty serving a commodity market can reduce its risks associated with the physical storage and delivery of commodities by matching participants that have delivery obligations with those due to receive the commodities, thereby removing itself from direct involvement in the storage and delivery process. In such instances, the legal obligations for delivery should be clearly expressed in the rules, including default rules, and any related agreements. In particular, a central counterparty should be clear whether the receiving participant should seek compensation from the central counterparty or the delivering participant in the event of a loss. Additionally, a central counterparty holding margin should not release the margin of the matched participants until it confirms that both have fulfilled their respective obligations. A central counterparty should also monitor its participants' performance and, to the extent practicable, ensure that its participants have the necessary systems and resources to be able to fulfil their physical delivery obligations.

Standard 11: Exchange-of-value settlements

If a central counterparty is involved in the settlement of transactions that comprise two linked obligations (for example, securities or foreign exchange transactions), it should eliminate principal risk by ensuring that the final settlement of one obligation is conditional upon the final settlement of the other.

Guidance

The settlement of a financial transaction may involve the settlement of two linked obligations, such as the delivery of securities against payment of cash or securities or the delivery of one currency against delivery of another currency.[38] In this context, principal risk may be created when one obligation is settled, but the other obligation is not (for example, the securities are delivered but no cash payment is received). Because this principal risk involves the full value of the transaction, substantial credit losses as well as substantial liquidity pressures may result from the default of a counterparty or, more generally, the failure to complete the settlement of both linked obligations. Further, a settlement default could result in high replacement costs (that

38 In some cases, the settlement of a transaction can be free of payment, for example, for the purposes of pledging collateral and repositioning securities. The settlement of a transaction may also involve more than two linked obligations, for example, for the purposes of some collateral substitutions where there are multiple securities or for premium payments related to securities lending in two currencies. These cases are not inconsistent with this Standard.

is, the unrealised gain on the unsettled contract or the cost of replacing the original contract at market prices that may be changing rapidly during periods of stress). A central counterparty should eliminate or mitigate these risks by ensuring that it uses an appropriate DvP, DvD or PvP settlement mechanism.[39]

11.1 A central counterparty should eliminate principal risk associated with the settlement of any obligations involving two linked obligations by ensuring that the payment system or securities settlement facility employed operates in such a way that the final settlement of one obligation occurs if and only if the final settlement of the linked obligation also occurs, regardless of whether the securities settlement facility settles on a gross or net basis and when finality occurs.

11.1.1 A central counterparty should ensure that it employs a DvP, DvD or PvP settlement mechanism, which eliminates principal risk by ensuring that the final settlement of one obligation occurs if and only if the final settlement of the linked obligation occurs (see also CCP Standard 4 on credit risk, CCP Standard 7 on liquidity risk and CCP Standard 8 on settlement finality). In the securities market, for example, a DvP settlement mechanism is a mechanism that links a securities transfer and a funds transfer in such a way as to ensure that delivery occurs if and only if the corresponding payment occurs. Similarly, a PvP settlement mechanism is a mechanism which ensures that the final transfer of a payment in one currency occurs if and only if the final transfer of a payment in another currency or currencies takes place, and a DvD settlement mechanism is a securities settlement mechanism which links two or more securities transfers in such a way as to ensure that delivery of one security occurs if and only if the corresponding delivery of the other security or securities occurs.

11.1.2 DvP (or PvP or DvD) should be achieved for all linked obligations cleared by a central counterparty. The settlement of two obligations can be achieved in several ways and varies by how trades or obligations are settled, either on a gross basis (trade-by-trade or line-by-line) or on a net basis, and the timing of when finality occurs.

11.2 A central counterparty should eliminate principal risk associated with the settlement of linked obligations by ensuring that it employs an appropriate delivery versus payment (DvP), delivery versus delivery (DvD) or payment versus payment (PvP) settlement mechanism.

11.2.1 In meeting the requirements of CCP Standard 11.1, the final settlement of two linked obligations can be achieved either on a gross basis or on a net basis. The choice of settlement model employed by a central counterparty will depend on the nature of obligations that it settles. Typically, exchange-of-value settlement can be achieved in one of three ways:

- where the final transfers of payment and/or securities between trade counterparties required to extinguish linked obligations occur contemporaneously and on a trade-by-trade (or line-by-line) basis in real time (i.e. DvP model 1)
- where final securities transfers are settled on a trade-by-trade (or line-by-line) basis in real time, with final payment transfers settled on a multilateral net basis at the end of the processing cycle (i.e. DvP model 2)[40]

39 While DvP, DvD and PvP settlement mechanisms eliminate principal risk, they do not eliminate the risk that the failure of a participant could result in systemic disruptions, including liquidity dislocations.

40 Given the separation of securities and funds transfers in such a system, intraday finality of securities settlement can only be achieved if securities transfers are collateralised or otherwise guaranteed.

- where both final securities transfers and/or final payment transfers required to extinguish linked obligations occur contemporaneously on a multilateral net basis at the end of the processing cycle (i.e. DvP model 3).

Regardless of whether a central counterparty employs a payment system or securities settlement facility that settles on a gross or net basis, the facility's legal, contractual, technical and risk management framework should ensure that the settlement of an obligation is final if and only if the settlement of the corresponding obligation is final.

11.2.2 The timing of exchange-of-value settlement of trades is important. Where the final contemporaneous transfers of securities and/or payment required to extinguish linked obligations occur either in real time throughout the day, or on a multilateral net basis at the end of the processing cycle, principal risk is eliminated. On the other hand, where final transfer of securities occurs in real time, but final payment is deferred until some later time, sellers of securities remain exposed to principal risk, which must therefore be managed.

11.2.3 Where settlement involves the exchange of a security for payment (a DvP transaction), the settlement of obligations requires up to three steps:

- the security (or title over the security) needs to be transferred from seller to buyer
- payment must be transferred from the buyer to the seller, either across accounts with the securities settlement facility's money settlement agent (which may be the central bank of issue), or using the services of a commercial settlement bank
- where the buyer and seller use a different commercial settlement bank, funds must be transferred from the account of the buyer's settlement bank to the account of the seller's settlement bank with the money settlement agent (see CCP Standard 9 on money settlements).

11.2.4 Contemporaneous performance of the three steps involved in a DvP transaction requires that:

- the transfer of money settlement assets is irrevocably linked with the settlement of securities and payment obligations, such that one cannot occur without the other
- where netting is used, securities blocked prior to transfer are not subject to claims by third parties
- final and irrevocable settlement of all obligations arising from a securities trade occurs either simultaneously or within such a very small period of time that the benefits of DvP are achieved.

11.2.5 Notwithstanding that contemporaneous multilateral net settlement of securities and/or final payment transfers eliminates principal risk, a participant default that triggered recalculation of obligations within the net settlement batch could, if obligations were sufficiently large, cause either, or both, the central counterparty and survivors to face significant liquidity pressures on a short horizon. Furthermore, even where a participant default did not give rise to sizeable swings in liquidity requirements for participants, the dependencies between participants in a net batch settlement model are such that problems with a single participant could nevertheless cause delays and uncertainty for all participants.

11.2.6 Where individual trade values are large, in the sense that dealing with a defaulting participant's obligations within a multilateral net batch could cause significant delays, uncertainty or liquidity pressures a central counterparty would be expected to settle linked obligations via a payment system or securities settlement facility that provides for trade-by-trade (or line-by-line) settlement on a real-time basis. Only where trade values are not large in this sense would it be acceptable for

the payment transfers and/or final securities transfers required to extinguish linked obligations to occur on a multilateral net basis. Even where trade values are small, linked settlements should occur contemporaneously unless this is precluded by operational requirements. Where netting is involved, the central counterparty should ensure that it has taken steps to ensure the certainty of netting arrangements (see CCP Standard 1 on legal basis). The central counterparty should, at a minimum, ensure that the final and irrevocable settlement of obligations is completed by the end of the settlement day.

11.2.7 Operational requirements that may necessitate non-contemporaneous settlement of linked obligations refer to practical matters arising out of the nature of the security and payment being exchanged that preclude contemporaneous settlement. This may occur, for example, where title must be exchanged by individual physical delivery and, as a practical matter, payment is by other than electronic transfer.

Standard 12: Participant default rules and procedures

A central counterparty should have effective and clearly defined rules and procedures to manage a participant default. These rules and procedures should be designed to ensure that the central counterparty can take timely action to contain losses and liquidity pressures and continue to meet its obligations.

Guidance

Participant default rules and procedures facilitate the continued functioning of a central counterparty in the event that a participant fails to meet its obligations. Such rules and procedures help limit the potential for the effects of a participant's failure to spread to other participants and possibly undermine the viability of the central counterparty. Key objectives of default rules and procedures should include: ensuring timely completion of settlement, even in extreme but plausible market conditions; minimising losses for the central counterparty and for non-defaulting participants; limiting disruptions to the market; providing a clear framework for accessing central counterparty liquidity facilities as needed; and managing and closing out a defaulting participant's positions and liquidating any applicable collateral in a prudent and orderly manner. In some instances, managing a participant default may involve hedging open positions, funding collateral so that the positions can be closed out over time, or both. A central counterparty may also decide to auction or allocate open positions to its participants.[41] To the extent consistent with these objectives, a central counterparty should allow non-defaulting participants to continue to manage their positions and transactions as normal.

12.1 A central counterparty should have default rules and procedures that enable the central counterparty to continue to meet its obligations in the event of a participant default and that address the replenishment of resources following a default. A central counterparty should ensure that financial and other obligations created for non-defaulting participants in the event of a participant default are proportional to the scale and nature of individual participants' activities.

41 For certain products, a central counterparty may need to consider requiring participants to agree in advance to bid on the defaulting participant's portfolio and, should the auction fail, accept an allocation of the portfolio.

Rules and procedures

12.1.1 A central counterparty should have default rules and procedures that enable the central counterparty to continue to meet its obligations to non-defaulting participants in the event of a participant default. A central counterparty should explain clearly in its rules and procedures what circumstances constitute a participant default, addressing both financial and operational defaults.[42] A central counterparty should describe the method for identifying a default. In particular, a central counterparty should specify whether a declaration of default is automatic or discretionary, and if discretionary, which person or group shall exercise that discretion. Key aspects to be considered in designing the rules and procedures include: the actions that a central counterparty can take when a default is declared; the extent to which such actions are automatic or discretionary; potential changes to the normal settlement practices, should these changes be necessary in extreme circumstances, to ensure timely settlement; the management of transactions at different stages of processing; the expected treatment of proprietary and customer transactions and accounts; the probable sequencing of actions; the roles, obligations and responsibilities of the various parties, including non-defaulting participants; and the existence of other mechanisms that may be activated to contain the impact of a default. A central counterparty should involve its participants, the Reserve Bank and other relevant authorities, and other relevant stakeholders in developing its default rules and procedures (see CCP Standard 2 on governance).

12.1.2 In the event of a participant default, financial and other obligations created for non-defaulting participants should be proportional to the scale and nature of participants' activities. Disproportionate obligations may place undue demands on participants at a time of wider market distress. Obligations placed on non-defaulting participants may include calls for additional default fund contributions, unfunded loss or liquidity allocations, or compulsory participation in auctions or allocations of the defaulting participant's open positions. In these cases, a central counterparty may consider making the size of participant contributions or allocation of positions dependent on the risk and scale of the participant's activities. Where compulsory participation in auctions or allocations of the defaulting participant's open positions is used, procedures should include consideration of the risk profile and portfolio of each receiving participant before allocating positions, so as to minimise additional risk for the non-defaulting participants. The scope of an individual participant's activities should also be considered. For example, where a central counterparty clears multiple products with distinct risk profiles, it should consider the potential impact on participants that are active in only a subset of these products when determining whether to operate a commingled default fund, or separate default funds based on product types. As another example, where a participant holds most of its positions in Australian dollar-denominated contracts, a central counterparty's loss allocation arrangements could be designed to avoid allocating positions in other currencies to that participant.

Use and sequencing of financial resources

12.1.3 A central counterparty's default rules and procedures should enable the central counterparty to take timely action to contain losses and liquidity pressures, before, at and after the point of participant default (see also CCP Standard 4 on credit risk and CCP Standard 7 on liquidity risk). Specifically, a central counterparty's rules and procedures should allow the central counterparty to use promptly any financial resources that it maintains for covering losses and containing liquidity pressures arising from

42 An operational default occurs when a participant is not able to meet its obligations due to an operational problem, such as a failure in information technology systems.

default, including liquidity facilities. The rules of the central counterparty should specify the order in which different types of resources will be used. This information would enable participants to assess their potential future exposures from using the central counterparty's services. Typically, a central counterparty should first use assets provided by the defaulting participant, such as margin or other collateral, to provide incentives for participants to manage prudently the risks, particularly credit risk, they pose to a central counterparty.[43] The application of previously provided collateral should not be subject to prevention, stay or reversal under applicable law and the rules of the central counterparty. A central counterparty should also have a credible and explicit plan for replenishing its resources over an appropriate time horizon following a participant default so that it can continue to operate in a safe and sound manner. In particular, the central counterparty's rules and procedures should define any obligations of the non-defaulting participants to replenish the financial resources depleted during a default so that the time horizon of such replenishment is anticipated by non-defaulting participants.

Close out or transfer of positions

12.1.4 A central counterparty should have rules and procedures to facilitate the prompt close out or transfer of a defaulting participant's proprietary and customer positions. Typically, the longer these positions remain open on the books of the central counterparty, the larger the central counterparty's potential credit exposures resulting from changes in market prices or other factors. A central counterparty should have the ability to apply the proceeds of liquidation, along with other funds and assets of the defaulting participant, to meet the defaulting participant's obligations. It is critical that a central counterparty has the authority to act promptly to contain its exposure, while having regard to overall market effects, such as potential sharp declines in market prices.

12.2 A central counterparty should be well prepared to implement its default rules and procedures, including any appropriate discretionary procedures provided for in its rules. This requires that the central counterparty should:

(a) require its participants to inform it immediately if they:

(i) become subject to, or aware of the likelihood of external administration, or have reasonable grounds for suspecting that they will become subject to external administration; or

(ii) have breached, or are likely to breach, a risk control requirement of the central counterparty; and

(b) have the ability to close out, hedge or transfer, a participant's open contracts in order to appropriately control risk of a participant that:

(i) becomes subject to external administration; or

(ii) breaches a risk control requirement of the central counterparty.

12.2.1 This Standard is aimed at avoiding any systemic disturbance that may arise from the default of a participant. The central counterparty should have a legally binding requirement for participants to notify it should they be in default or reasonably suspect that this is the case. Similar notification

43 The defaulting participant's assets do not include segregated customer collateral; such segregated collateral should not be used to cover losses resulting from a participant default, except in the case of a potential close out of segregated customer positions. See CCP Standard 13 on segregation and portability.

should be made in the event of a breach or likely breach of any risk control requirement of the central counterparty. Any communication should be at an appropriately high level both within the participant organisation and the central counterparty. There is a difference between external administration and cases where a participant may have sufficient assets to meet its obligations, yet be unable to complete settlement of its obligations due to operational failure or liquidity pressures. This distinction should be recognised in the rules of the central counterparty. The central counterparty should have the ability to suspend or cancel the participation of a participant in default, thus preventing that participant from continuing to take on trade obligations.

12.2.2 A central counterparty should be well prepared to implement its default rules and procedures, including any appropriate discretionary procedures provided for in the rules. Management should ensure that the central counterparty has the operational capacity, including sufficient well-trained personnel, to implement its procedures in a timely manner. A central counterparty's rules and procedures should outline examples of when management discretion may be appropriate and should include arrangements to minimise any potential conflicts of interests. Management should also have internal plans that clearly delineate the roles and responsibilities for addressing a default and provide training and guidance to its personnel on how the procedures should be implemented. These plans should address documentation, information needs and coordination when more than one central counterparty or authority is involved. In addition, timely communication with stakeholders, in particular with the Reserve Bank and other relevant authorities, is of critical importance (see also CCP Standard 21 on regulatory reporting). The central counterparty, to the extent permitted, should clearly convey to affected stakeholders information that would help them to manage their own risks. The internal plan should be reviewed by management and the relevant board committees at least annually or after any significant changes to the central counterparty's arrangements.

12.2.3 A central counterparty should have the information, resources and tools to close out positions promptly. In circumstances where prompt close out is not practicable, a central counterparty should have the tools to hedge positions as an interim risk management technique. In some cases, a central counterparty may use seconded personnel from non-defaulting participants to assist in the close out or hedging process. The central counterparty's rules and procedures should clearly state the anticipated scope of duties and term of service of seconded personnel. In other cases, the central counterparty may elect to auction positions or portfolios to the market. The central counterparty's rules and procedures should clearly state the scope for such action, and any participant obligations with regard to such auctions should be clearly set out. The close out of positions should not be subject to prevention, stay or reversal under applicable law and the rules of the central counterparty.

12.3 A central counterparty should publicly disclose key aspects of its default rules and procedures.

12.3.1 To provide certainty and predictability regarding the measures that a central counterparty may take in a default event, a central counterparty should publicly disclose key aspects of its default rules and procedures, including: the circumstances in which action may be taken; who may take those actions; the scope of the actions which may be taken, including the treatment of both proprietary and customer positions, funds and other assets; the mechanisms to address a central counterparty's obligations to non-defaulting participants; and, where direct relationships exist with participants' customers, the mechanisms to help address the defaulting participant's obligations to its customers. Such transparency should facilitate the orderly handling of defaults, enable participants to understand

their obligations to the central counterparty and to their customers, and provide for informed decisions by market participants about their activities in the market. A central counterparty should ensure that its participants and their customers, as well as the public, have appropriate access to the central counterparty's default rules and procedures and should promote their understanding of those procedures in order to foster confidence in the market in the event of a participant default.

12.4 A central counterparty should involve its participants and other stakeholders in the testing and review of the central counterparty's default procedures, including any close out procedures. Such testing and review should be conducted at least annually and following material changes to the rules and procedures to ensure that they are practical and effective.

12.4.1 A central counterparty should involve relevant participants and other stakeholders in the testing and review of its default procedures, including any close out procedures. Such testing and review should be conducted at least annually and following material changes to the rules and procedures to ensure that they are practical and effective. The periodic testing and review of default procedures is important to help the central counterparty and its participants understand fully the procedures and to identify any lack of clarity in, or discretion allowed by, the rules and procedures. Such tests should include all relevant parties, or an appropriate subset, that would likely be involved in the default procedures, such as members of the appropriate board committees, participants, linked or interdependent FMIs, the Reserve Bank and other relevant authorities, and any related service providers. This is particularly important where a central counterparty relies on non-defaulting participants or third parties to assist in the close out process and where the default procedures have never been tested by an actual default. The results of these tests and reviews should be shared with the central counterparty's board of directors, risk committee, and the Reserve Bank and other relevant authorities.

12.4.2 Furthermore, part of a central counterparty's participant default testing should include the implementation of the resolution regime for a central counterparty's participants, as relevant. A central counterparty should be able to take all appropriate steps to address the resolution of a participant. Specifically, the central counterparty, or if applicable a resolution authority, should be able to transfer a defaulting participant's open positions and customer accounts to a receiver, third party or bridge financial company.

12.5 A central counterparty should demonstrate that its default management procedures take appropriate account of interests in relevant jurisdictions and, in particular, any implications for pricing, liquidity and stability in relevant financial markets.

12.5.1 A central counterparty should ensure that its default management procedures take appropriate account of the interests of all relevant stakeholders across the jurisdictions in which it operates, including those of its direct and indirect participants. A central counterparty's governance arrangements should ensure that these interests are taken into account (see CCP Standard 2 on governance). The actions that a central counterparty takes in the event of a default, such as closing out a defaulter's positions or auctioning or allocating open positions to surviving participants, could potentially impact on pricing, liquidity and stability in relevant financial markets. A central counterparty should consider these wider market impacts of its default management actions, and take mitigating action to minimise market impacts as appropriate.

Standard 13: Segregation and portability

A central counterparty should have rules and procedures that enable the segregation of positions of a participant's customers and the collateral provided to the central counterparty with respect to those positions.

Guidance

Segregation of customers' positions and collateral plays an important part in the safe and effective holding and transfer of customers' positions and collateral, especially in the event of a participant's default or insolvency. Customers' positions and collateral should be segregated from those of the participant through which the customers clear. In addition, individual customers' positions and collateral may be held separately from the positions and collateral of other customers of the same participant to protect customers from each other's default. Where such segregation is offered by the central counterparty, positions and collateral should be protected effectively from the concurrent default or insolvency of the participant and a fellow customer.

Effective segregation arrangements can reduce the impact of a participant's insolvency on its customers by providing for clear and reliable identification of a participant's customers' positions and related collateral. Segregation also protects customers' collateral from becoming lost to a participant's other creditors. In addition, segregation facilitates the transfer of customers' positions and collateral. Even if no transfers take place, segregation can improve a customer's ability to identify and recover its collateral (or the value thereof), which, at least to some extent, contributes to retaining customers' confidence in their clearing participants and may reduce the potential for 'counterparty runs' on a deteriorating clearing participant.

By facilitating transfers from one participant to another, effective portability arrangements lessen the need for closing out positions, including during times of market stress. Portability thus minimises the costs and potential market disruption associated with closing out positions and reduces the possible impact on customers' ability to continue to obtain access to central clearing.

The effectiveness of segregation and portability measures taken by a central counterparty depends in part on applicable legal frameworks, including those in foreign jurisdictions in the case of remote participants, and on measures taken by other parties, for example, where customers post excess collateral to the participant.

13.1 A central counterparty should, at a minimum, have segregation and portability arrangements that effectively protect a participant's customers' positions and related collateral from the default or insolvency of that participant. If the central counterparty additionally offers protection of such customer positions and collateral against the concurrent default of the participant and a fellow customer, the central counterparty should take steps to ensure that such protection is effective.

13.1.1 In order to achieve fully the benefits of segregation and portability, the central counterparty's arrangements to protect and transfer the positions and collateral of a participant's customers should be supported by the legal framework applicable to the central counterparty.[44] The legal framework will influence how the segregation and portability arrangements are designed and what benefits can be achieved. The relevant legal framework will vary depending upon many factors, including the participant's legal form of organisation, the manner in which collateral is provided (for example, security

44 For example, portability arrangements could be undermined if applicable insolvency laws did not protect the transfer of customer positions and collateral from avoidance ('clawback') by the participant's insolvency practitioner. Also, in some jurisdictions, it may not be possible to segregate cash.

interest, title transfer or full ownership right), and the types of assets (for example, cash or securities) provided as collateral. The appropriate model may therefore vary for central counterparties across relevant jurisdictions. However, a central counterparty should structure its segregation and portability arrangements (including applicable rules) in a manner that protects the interests of its participant's customers and achieves a high degree of legal certainty under applicable law. A central counterparty should also consider potential conflicts of law when designing its arrangements. In particular, the central counterparty's rules and procedures that set out its segregation and portability arrangements should avoid any potential conflict with applicable legal or regulatory requirements.

13.2 A central counterparty should employ an account structure that enables it readily to identify positions of a participant's customers and to segregate related collateral. A central counterparty should maintain customer positions and collateral in individual customer accounts or in omnibus customer accounts, or equivalent.

13.2.1 In considering the appropriate account structure, including the level of segregation and the basis for margin collection (that is, gross or net), a central counterparty should take into account stakeholders' views and assess the important benefits of individual customer protection alongside all relevant legal and operational factors. Such factors might include applicable insolvency regimes, costs of implementation and operational implications (for example, operational challenges associated with maintaining and managing individual customer accounts).

Customer account structures

13.2.2 This Standard is particularly relevant for central counterparties that clear positions and hold collateral belonging to customers of a participant. This clearing structure allows customers (such as buy-side firms) that are not direct participants of a central counterparty to obtain access to central clearing where direct access is either not possible (for example, due to an inability to meet membership criteria) or not considered commercially appropriate (for example, due to the cost of establishing and maintaining the infrastructure necessary to perform as a clearing member or contributing to a central counterparty's default resources). A central counterparty should employ an account structure that enables it readily to identify positions belonging to a participant's customers and to segregate related collateral. Segregation of customer collateral by a central counterparty can be achieved in different ways, including through individual or omnibus accounts.

13.2.3 The degree of protection achievable for customer collateral will depend on whether customers are protected on an individual or omnibus basis and the way initial margin is collected (gross or net basis) by the central counterparty. Collecting margin on a gross basis means that the amount of margin a participant must post to the central counterparty on behalf of its customers is the sum of the amounts of margin required for each such customer. Collecting margin on a net basis means that the participant may, in calculating the amount of margin it must post to the central counterparty on behalf of its customers, offset the amounts of margin associated with the portfolios of different customers. Each of these decisions will have implications for the risks the central counterparty faces from its participants and, in some cases, their customers. The central counterparty should understand, monitor and manage these risks. (See also CCP Standard 18 on tiered participation arrangements.)

Individual account structure

13.2.4 Similarly, there are advantages and disadvantages to each type of account structure that the central counterparty should consider when designing its segregation regime .The individual account structure provides a high degree of protection to the clearing level collateral of customers of participants in a central counterparty, even in the case where the losses associated with another customer's default exceed the resources of the participant. Under this approach, each customer's collateral is held in a separate, segregated individual account at the central counterparty, and depending on the legal framework applicable to the central counterparty, a customer's collateral may only be used to cover losses associated with the default of that customer (that is, customer collateral is protected on an individual basis). This account structure facilitates the clear and reliable identification of a customer's collateral, which supports full portability of an individual customer's positions and collateral or, alternatively, can expedite the return of collateral to the customer. Since all collateral maintained in the individual customer's account is used to margin that customer's positions only, the central counterparty should be able to transfer these positions from the customer account of a defaulting participant to that of another participant with sufficient collateral to cover the exposures. The use of individual accounts and the collection of margin on a gross basis provide flexibility in how a customer's portfolio may be ported to another participant or group of participants. Maintaining individual accounts, however, can be operationally and resource intensive for the central counterparty in settling transactions and ensuring accurate bookkeeping. Finally, effectively achieving the advantages of maintaining individual accounts may depend upon the legal framework applicable to the insolvency of the participant.

Omnibus account structure

13.2.5 Another approach is to use an omnibus account structure where all collateral belonging to all customers of a particular participant is commingled and held in a single account segregated from that of the participant. This approach can be less operationally intensive, while continuing to protect customers' collateral from being used to cover a default by the direct participant.

13.2.6 However, depending on the legal framework and the central counterparty's rules, omnibus accounts may expose a customer to 'fellow customer risk' – the risk that another customer of the same participant will default and create a loss that exceeds both the amount of available collateral supporting the defaulting customer's positions and the available resources of the participant. As a result, the remaining commingled collateral of the participant's non-defaulting customers is exposed to the loss. Fellow customer risk is of particular concern because customers have limited, if any, ability to monitor or to manage the risk of their fellow customers.

13.2.7 One potential solution is for omnibus account structures to be designed in a manner that operationally commingles collateral related to customer positions while protecting customers legally on an individual basis – that is, protecting them from fellow customer risk. Such individual protection does require the central counterparty to maintain accurate books sufficient to promptly ascertain an individual customer's interest in a portion of the collateral. A failure to do so can lead to delays or even losses in returning margin and other collateral that has been provided to the central counterparty to individual customers in the event that a participant becomes insolvent.[45]

45 Ascertaining each customer's interest in the omnibus account may require reliance on the participant's records containing the sub-accounting for individual customers.

13.2.8 The degree to which portability is fostered for a customer whose assets are held in an omnibus account also varies depending on whether the central counterparty collects margin on a gross or net basis. As with account structure, there are advantages and disadvantages to the alternative ways in which margin may be collected by the central counterparty that employs an omnibus account structure. Margin calculated on a gross basis to support individual customer portfolios results in less netting efficiency at the participant level; however, it is likely to mitigate the risk of under-margined customer positions when ported. As a result, central counterparties can port a participant's customers' positions and related margin in bulk or piecemeal. Gross margining enhances the feasibility of portability, which is desirable since porting avoids the transaction costs, including bid-offer spreads, associated with terminating and replacing a participant's customers' positions. When margin is collected on a gross basis, it is more likely that there will be sufficient collateral in the omnibus account to cover all positions of a participant's customers.

13.2.9 When margin is collected by the central counterparty on a net basis but held in an omnibus account structure, there is a risk that full portability cannot be achieved. Since the collateral maintained in the omnibus account covers the net positions across all customers of a particular participant, upon a participant default, any excess collateral maintained by the defaulting participant may not be readily available for porting to another participant to adequately collateralise a customer's positions.[46] Moreover, other than a bulk transfer of all customer positions of the defaulting participant, along with the aggregate of the customer collateral held at the central counterparty and at the participant, any transfer of a customer's positions to another participant would depend on the ability and willingness of customers to provide additional collateral. Otherwise, porting individual customer portfolios, with their pro rata share of net margin, to multiple transferee clearing members is likely to result in under-margined customer positions. Transferee clearing members are unlikely to accept such positions unless the margin shortfall is remedied by the customer.

Alternative arrangements for cash markets

13.2.10 Under certain circumstances, central counterparties clearing cash markets may be able to achieve materially equivalent protection of customer assets by alternative means. Such alternative arrangements should ensure that: customer positions can be identified in a timely manner; customers will be protected by an alternative mechanism (for example, an investor protection scheme) designed to move customer accounts from the failed or failing participant to another participant in a timely manner; and customer assets can be restored. In these cases, the central counterparty should consult with the Reserve Bank and other relevant authorities to demonstrate that the applicable legal or regulatory framework achieves materially equivalent protection for customers to that which would otherwise be achieved by the segregation and portability arrangements described elsewhere in this Standard.

13.3 To the extent reasonably practicable under prevailing law, a central counterparty should structure its portability arrangements in a way that makes it highly likely that the positions and collateral of a defaulting participant's customers will be transferred to one or more other participants.

46 Collateral exceeding the amount required by the central counterparty to cover the net positions is often maintained by the participant.

13.3.1 Efficient and complete portability of a participant's customers' positions and related collateral is important in both pre-default and post-default scenarios but is particularly critical when a participant defaults or is undergoing insolvency proceedings.[47] A central counterparty's ability to transfer customers' positions and related collateral in a timely manner may depend on such factors as market conditions, sufficiency of information on the individual constituents, and the complexity or sheer size of the portfolio. To the extent reasonably practicable under prevailing law, a central counterparty should therefore structure its portability arrangements in a way that makes it highly likely that the positions and collateral of a defaulting participant's customers will be effectively transferred to one or more other participants, taking into account all relevant circumstances. In order to achieve a high likelihood of portability, a central counterparty will need to: have the ability to identify positions that belong to customers; identify and assert its rights to related collateral held by or through the central counterparty; transfer positions and related collateral to one or more other participants; identify potential participants to accept the positions; and disclose relevant information to such participants so that they can evaluate the counterparty credit and market risk associated with the customers and positions, respectively. A central counterparty's rules and procedures should require participants to facilitate the transfer of a participant's customers' positions and collateral upon the customer's request, subject to any notice or other contractual requirements. The central counterparty should obtain the consent of the direct participant to which positions and collateral are ported. If there are circumstances where this would not be the case, they should be set out in the central counterparty's rules, policies or procedures. A central counterparty's policies and procedures also should provide for the proper handling of positions and collateral of customers of a defaulting participant. (See also CCP Standard 12 on participant default rules and procedures.)

13.4 A central counterparty should disclose its rules, policies and procedures relating to the segregation of a participant's customers' positions and related collateral. In particular, the central counterparty should disclose whether customer collateral is segregated on an individual or omnibus basis. In addition, a central counterparty should disclose any constraints, such as legal or operational constraints, that may impair its ability to segregate or port a participant's customers' positions and related collateral.

13.4.1 A central counterparty should state its segregation and portability arrangements, including the method for determining the value at which customer positions will be transferred, in its rules, policies and procedures. (See CCP Standard 20 on disclosure of rules, key policies and procedures, and market data.) A central counterparty's disclosure should be adequate such that customers can understand how much customer protection is provided, how segregation and portability are achieved, and any risks or uncertainties associated with such arrangements. Disclosure helps customers to assess and manage the related risks and conduct due diligence when entering into transactions that are cleared or settled through a direct participant in the central counterparty, reducing the risk of financial spillover via customers in the event of a participant default. Customers should have sufficient information about which of their positions and collateral held at or through a central counterparty are segregated from positions and collateral of the participant and the central counterparty. Disclosure regarding segregation should include: whether the segregated assets are reflected on the books and records at the central

47 A customer should also be able to transfer its positions and collateral to another participant in the normal course of business (for example, in the case of a relationship with a new clearing firm or merger of entities), subject to applicable laws and contractual terms. In addition, portability arrangements can also facilitate an orderly wind-down of a participant.

counterparty or unaffiliated third-party custodians that hold assets for the central counterparty; who holds the customer collateral (for example, the central counterparty or a third-party custodian); and under what circumstances customer collateral may be used by the central counterparty. In particular, the central counterparty should disclose whether customer collateral is protected on an individual or omnibus basis.

Standard 14: General business risk

A central counterparty should identify, monitor and manage its general business risk and hold, or demonstrate that it has legally certain access to, sufficient liquid net assets funded by equity to cover potential general business losses so that it can continue operations and services as a going concern if those losses materialise. Further, liquid net assets should at all times be sufficient to ensure a recovery or orderly wind-down of critical operations and services.

Guidance

A central counterparty should have robust management and control systems to identify, monitor and manage general business risk. General business risk refers to the risks and potential losses arising from a central counterparty's administration and operation as a business enterprise that are neither related to participant default nor separately covered by financial resources under CCP Standard 4 on credit risk or CCP Standard 7 on liquidity risk. General business risk includes any potential impairment of the central counterparty's financial position (as a business concern) as a consequence of a decline in its revenues or an increase in its expenses, such that expenses exceed revenues and result in a loss that must be charged against capital. Such impairment can be caused by a variety of business factors, including poor execution of business strategy, negative cash flows or unexpected and excessively large operating expenses. Business-related losses also may arise from risks covered by other standards, for example, legal risk (in the case of legal actions challenging the central counterparty's custody arrangements), investment risk affecting the central counterparty's resources, and operational risk (in the case of fraud, theft or loss).[48] In these cases, general business risk may cause a central counterparty to experience an extraordinary one-time loss as opposed to recurring losses.

14.1 A central counterparty should have robust management and control systems to identify, monitor and manage general business risks, including losses from poor execution of business strategy, negative cash flows or unexpected and excessively large operating expenses.

Identifying business risk

14.1.1 A central counterparty should identify and assess the sources of business risk and their potential impact on its operations and services, taking into account past loss events and financial projections. A central counterparty should assess and thoroughly understand its business risk and the potential effect that this risk could have on its cash flows, liquidity and capital positions. In doing so, a central counterparty should consider a combination of tools, such as risk management and internal control assessments, scenario analysis and sensitivity analysis. Internal control assessments should identify key risks and controls and assess the impact and probability of the risks and the effectiveness of the controls. Scenario analysis should examine how specific scenarios would affect the central counterparty. Sensitivity analysis should test how changes in one risk affect the central counterparty's

48 See also CCP Standard 1 on legal basis, CCP Standard 15 on custody and investment risks, and CCP Standard 16 on operational risk.

financial standing; for example, how the loss of a key customer or service provider might impact the central counterparty's existing business activities. In some cases, a central counterparty may wish to consider an independent assessment of specific business risks.

14.1.2 A central counterparty should clearly understand its general business risk profile so that it is able to assess its ability to either avoid, reduce or transfer specific business risks, or accept and manage those risks. This requires the ongoing identification of risk mitigation options that the central counterparty may use in response to changes in its business environment. When planning an expansion of activity, a central counterparty should conduct a comprehensive enterprise risk assessment. In particular, when considering any major new product, service or project, the central counterparty should forecast potential revenues and expenses as well as identify and plan how it will cover any additional capital requirements. Further, a central counterparty may eliminate or mitigate some risks by instituting appropriate internal controls or by obtaining insurance or indemnity from a third party.

Measuring and monitoring business risk

14.1.3 Once a central counterparty has identified and assessed its business risk, it should measure and monitor these risks on an ongoing basis and develop appropriate information systems as part of a robust enterprise-wide risk management program. Key components of a robust enterprise-wide risk management program include establishing strong financial and internal control systems, so that the central counterparty can monitor, manage and control its cash flows and operating expenses and mitigate any business-related losses (see CCP Standard 3 on the framework for the comprehensive management of risks). In particular, a central counterparty should minimise and mitigate the probability of business-related losses and their impact on its operations across a range of adverse business and market conditions, including the scenario that its viability as a going concern is questioned. A central counterparty should also ensure that it has rigorous and appropriate investment guidelines and monitoring procedures (see CCP Standard 15 on custody and investment risks).

14.2 A central counterparty should hold, or demonstrate that it has legally certain access to, liquid net assets funded by equity (such as common stock, disclosed reserves or other retained earnings) so that it can continue operations and services as a going concern if it incurs general business losses. The amount of liquid net assets funded by equity a central counterparty should hold, or have access to, should be determined by its general business risk profile and the length of time required to achieve a recovery or orderly wind-down, as appropriate, of its critical operations and services if such action is taken.

14.2.1 A central counterparty should hold, or demonstrate that it has legally certain access to, liquid net assets funded by equity (such as common stock, disclosed reserves or other retained earnings) so that it can continue operations and services as a going concern if it incurs general business losses.[49] Equity allows a central counterparty to absorb losses on an ongoing basis and should be permanently available for this purpose. The amount of liquid net assets funded by equity a central counterparty should hold, or have access to, should be determined by its general business risk profile and the length of time required to achieve a recovery or orderly wind-down, as appropriate, of its critical operations and services if such

49 If the central counterparty's corporate structure is such that it cannot legally or institutionally raise equity (for example, under certain structures of mutual ownership), it should ensure an equal amount of equivalent loss-absorbing financial resources is available.

action is taken.[50] If these assets are not held by the central counterparty itself, the central counterparty must have legally certain arrangements in place that guarantee it can access liquid net assets held by an affiliated entity, including in circumstances where its own or the affiliated entity's financial standing was in doubt. Any such arrangement should be subject to approval by the Reserve Bank and other relevant authorities.

14.2.2 In order to estimate the amount of liquid net assets funded by equity that a particular central counterparty would need, the central counterparty should regularly analyse and understand how its revenue and operating expenses may change under a variety of adverse business scenarios as well as how it might be affected by extraordinary one-time losses. This analysis should also be performed when a material change to the assumptions underlying the model occurs, either because of changes to the central counterparty's business model or because of external changes. A central counterparty needs to consider not only possible decreases in revenues but also possible increases in operating expenses, as well as the possibility of extraordinary one-time losses, when deciding on the amount of liquid net assets to hold or make accessible to cover general business risk.

14.3 A central counterparty should maintain a viable recovery or orderly wind-down plan and should hold, or have legally certain access to, sufficient liquid net assets funded by equity to implement this plan. At a minimum, a central counterparty should hold, or have legally certain access to, liquid net assets funded by equity equal to at least six months of current operating expenses. These assets are in addition to resources held to cover participant defaults or other risks covered under CCP Standard 4 on credit risk and CCP Standard 7 on liquidity risk. However, equity held under international risk-based capital standards can be included where relevant and appropriate to avoid duplicate capital requirements.

14.3.1 A central counterparty should maintain a viable plan to achieve recovery and orderly wind-down and should hold, or have access to, sufficient liquid net assets funded by equity to implement this plan.[51] The appropriate amount of liquid net assets funded by equity will depend on the content of the plan and, specifically, on the size of the central counterparty, the scope of its activities, the types of actions included in the plan and the length of time needed to implement them. A central counterparty should also take into consideration the operational, technological and legal requirements for participants to establish and move to an alternative arrangement in the event of an orderly wind-down. At a minimum, however, a central counterparty should hold, or have access to, liquid net assets funded by equity equal to at least six months of current operating expenses.[52]

14.3.2 Assets held by a central counterparty to cover risks or losses other than business risk (for example, the financial resources required under CCP Standard 4 on credit risk and CCP Standard 7 on liquidity risk) should not be included when accounting for liquid net assets available to cover business risk.[53]

50 Recovery could include recapitalising, replacing management, merging with another central counterparty, revising business strategies (including cost or fee structures), or restructuring services provided.

51 The requirement for liquid net assets funded by equity ensures that the assets held for the purposes of this Standard are sufficiently liquid to be available to mitigate any potential business risks in a timely manner, can only be used for business risk purposes, and are funded by equity rather than long term liabilities.

52 Operating expenses may exclude depreciation and amortisation expenses for the purposes of this calculation.

53 Depending on the rules of the particular central counterparty and the insolvency law of the jurisdiction in which it is established, the equity of a central counterparty may ultimately be used if the resources that form the default backing are insufficient to cover the losses generated in the event of a participant default.

However, any equity held under international risk-based capital standards should be included where relevant and appropriate to avoid duplicate capital requirements.

14.4 Assets held to cover general business risk should be of high quality and sufficiently liquid in order to allow the central counterparty to meet its current and projected operating expenses under a range of scenarios, including in adverse market conditions.

14.4.1 To ensure the adequacy of its own resources, a central counterparty should regularly assess and report its liquid net assets funded by equity relative to its potential business risks to the Reserve Bank and other relevant authorities (see also CCP Standard 21 on regulatory reporting).

14.5 A central counterparty should maintain a viable plan for raising additional equity should its equity fall close to or below the amount needed. This plan should be approved by the board of directors and updated regularly.

14.5.1 A central counterparty should provide a viable capital plan for maintaining an appropriate level of equity. The capital plan should specify how a central counterparty would raise new capital if its equity capital were to fall close to or below the amount needed. This plan should be approved by the board of directors (or an appropriate board committee), reviewed at least annually and updated as appropriate. A central counterparty may also need to consult its participants and others during the development of its plan.

14.5.2 In developing a capital plan, a central counterparty should consider a number of factors, including its ownership structure and any insured business risks. For example, a central counterparty should determine if and to what extent specific business risks are covered by explicit insurance from a third party, or explicit indemnity agreements from a parent, owners or participants (for example, general loss-allocation provisions and parent guarantees), which would be realisable within the recovery or orderly wind-down time frame. Given the contingent nature of these resources, a central counterparty should use conservative assumptions when taking them into account for its capital plan. Furthermore, these resources should not be taken into account when assessing the central counterparty's capital adequacy.

Standard 15: Custody and investment risks

A central counterparty should safeguard its own and its participants' assets and minimise the risk of loss on and delay in access to these assets. A central counterparty's investments should be in instruments with minimal credit, market and liquidity risks.

Guidance

A central counterparty has the responsibility to safeguard its assets, such as cash and securities, as well as the assets that its participants have provided to the central counterparty. Assets that are used by a central counterparty to support its operating funds or capital funds or that have been provided by participants to secure their obligations to the central counterparty should be held at supervised or regulated entities that have strong processes, systems and credit profiles, including other FMIs (for example, central securities depositories). In addition, assets should generally be held in a manner that assures the central counterparty of prompt access to those assets in the event that the central counterparty needs to draw on them.

A central counterparty should ensure that its investment strategy is consistent with its overall risk management strategy. Resources held by a central counterparty to cover credit, liquidity or general business risks should not be exposed to credit, market or liquidity risks (including through concentrated exposures to investment counterparties) that may compromise the ability of the central counterparty to use these resources when needed.

15.1 A central counterparty should hold its own and its participants' assets at supervised and regulated entities that have robust accounting practices, safekeeping procedures and internal controls that fully protect these assets.

15.1.1 A central counterparty should mitigate its custody risk by using only supervised and regulated entities with robust accounting practices, safekeeping procedures, and internal controls that fully protect its own and its participants' assets. It is particularly important that assets held in custody are protected against claims of a custodian's creditors. The custodian should have a sound legal basis supporting its activities, including the segregation of assets (see also CCP Standard 1 on legal basis). The custodian also should have a strong financial position to be able to sustain losses from operational problems or ancillary non-custodial activities.

15.2 A central counterparty should have prompt access to its assets and the assets provided by participants, when required.

15.2.1 A central counterparty should confirm that its interest or ownership rights in the assets can be enforced and that it can have prompt access to its assets and the assets provided by participants, when required. Timely availability and access should be ensured even if these securities are held in another time zone or jurisdiction. Furthermore, the central counterparty should confirm it has prompt access to the assets in the event of the default of a participant.

15.3 A central counterparty should evaluate and understand its exposures to its custodians, taking into account the full scope of its relationships with each.

15.3.1 A central counterparty should evaluate and understand its exposures to its custodians, taking into account the full scope of its relationships with each custodian. For example, a financial institution may serve as a custodian to a central counterparty as well as a money settlement agent or liquidity provider to the central counterparty. The custodian also may be a participant in the central counterparty and offer clearing services to other participants. A central counterparty should carefully consider all of its relationships with a particular custodian to ensure that its overall risk exposure to an individual custodian remains within acceptable limits. Where feasible, a central counterparty could consider using multiple custodians for the safekeeping of its assets to diversify its exposure to any single custodian. For example, a central counterparty may use one custodian for its margin assets and another custodian for its prefunded default resources. Such a central counterparty, however, may need to balance the benefits of risk diversification against the benefits of pooling resources at one or a small number of custodians. In any event, a central counterparty should monitor the concentration of risk exposures to, and financial condition of, its custodians on an ongoing basis.

15.4 A central counterparty's investment strategy should be consistent with its overall risk management strategy and fully disclosed to its participants, and investments should be secured by, or be claims on, high-quality obligors. These investments should allow for quick liquidation with little, if any, adverse price effect.

15.4.1 A central counterparty's strategy for investing its own and its participants' assets should be consistent with its overall risk management strategy and fully disclosed to its participants. When making its investment choices, the central counterparty should not allow pursuit of profit to compromise its financial soundness and liquidity risk management. Investments should be secured by, or be claims on, high-quality obligors to mitigate the credit risk to which the central counterparty is exposed. Within these parameters, a central counterparty should, to the extent reasonably practicable, have a high degree of confidence that its own capital would be sufficient to withstand losses associated with the failure of any individual non-government investment counterparty. This implies the imposition of conservative limits on the size and concentration of counterparty exposures. In considering its overall credit risk exposures to individual obligors, a central counterparty should also take into account other relationships with the obligor that create additional exposures, such as where an obligor is also a participant or an affiliate of a participant in the central counterparty. In addition, a central counterparty should ensure that any investment of participant assets in the securities of participants or their affiliates is subject to appropriate controls for specific wrong-way risk.

15.4.2 Because the value of a central counterparty's investments may need to be realised quickly, investments should allow for quick liquidation with little, if any, adverse price effect. For example, a central counterparty could invest in overnight reverse repo agreements backed by liquid securities with low credit risk. In allowing for quick liquidation with minimal adverse price effect, a central counterparty should also impose limits on the concentration of certain assets in its investment portfolio.

Standard 16: Operational risk

A central counterparty should identify the plausible sources of operational risk, both internal and external, and mitigate their impact through the use of appropriate systems, policies, procedures and controls. Systems should be designed to ensure a high degree of security and operational reliability and should have adequate, scalable capacity. Business continuity management should aim for timely recovery of operations and fulfilment of the central counterparty's obligations, including in the event of a wide-scale or major disruption.

Guidance

Operational risk is the risk that deficiencies in information systems, internal processes and personnel, or disruptions from external events, will result in the reduction, deterioration or breakdown of services provided by a central counterparty. Operational failures can damage a central counterparty's reputation or perceived reliability, lead to legal consequences, and result in financial losses incurred by the central counterparty, participants and other parties. In certain cases, operational failures can also be a source of systemic risk. A central counterparty should: establish a robust framework to manage its operational risks, which should identify the plausible sources of operational risk; deploy appropriate systems; establish appropriate policies, procedures and controls; set operational reliability objectives; and develop a business continuity plan. A central counterparty should take a holistic approach when establishing its operational risk management framework.

Identifying and managing operational risk

16.1 A central counterparty should establish a robust operational risk management framework with appropriate systems, policies, procedures and controls to identify, monitor and manage operational risks.

16.1.1 A central counterparty should actively identify, monitor and manage the plausible sources of operational risk and establish clear policies and procedures to address them. Operational risk can stem from both internal and external sources. Internal sources of operational risk include inadequate identification or understanding of risks and the controls and procedures needed to limit and manage them, inadequate control of systems and processes, inadequate screening of personnel, and, more generally, inadequate management. External sources of operational risk include the failure of critical service providers or utilities or events affecting a wide metropolitan area such as natural disasters, terrorism and pandemics. Both internal and external sources of operational risk can lead to a variety of operational failures that include: errors or delays in message handling; miscommunication; service degradation or interruption; fraudulent activities by staff; and disclosure of confidential information to unauthorised entities. If a central counterparty provides services in multiple time zones, it may face increased operational risk due to longer operational hours and less downtime for maintenance. A central counterparty should identify all potential single points of failure in its operations.[54] Additionally, a central counterparty should assess the evolving nature of the operational risk it faces on an ongoing basis (for example, pandemics and cyber-attacks), so that it can analyse its potential vulnerabilities and implement appropriate defence mechanisms.

16.2 A central counterparty's board of directors should clearly define the roles and responsibilities for addressing operational risk and should endorse the central counterparty's operational risk management framework. Systems, operational policies, procedures and controls should be reviewed, audited and tested periodically and after significant changes.

16.2.1 A central counterparty should establish clear policies, procedures and controls that mitigate and manage its sources of operational risk. Overall, operational risk management is a continuous process encompassing risk assessment, defining an acceptable tolerance for risk and implementing risk controls. This process results in a central counterparty accepting, mitigating or avoiding risks consistent with its operational reliability objectives. A central counterparty's governance arrangements are pertinent to its operational risk management framework (see also CCP Standard 2 on governance). In particular, a central counterparty's board should explicitly define the roles and responsibilities for addressing operational risk and endorse the central counterparty's operational risk management framework.

16.2.2 To ensure the proper functioning of its risk controls, a central counterparty should have sound internal controls. For example, a central counterparty should have adequate management processes for setting operational standards, measuring and reviewing performance, and correcting deficiencies. A central counterparty may draw on relevant international, national and industry level standards, guidelines or recommendations in designing its operational risk management framework. Conformity with commercial standards can help a central counterparty meet its operational objectives. For example, commercial standards exist for information security, business continuity and project management. A central counterparty should regularly assess the need to integrate the applicable commercial standards into its operational risk management framework. In addition, a central counterparty should seek to comply with relevant commercial standards in a manner commensurate with the central counterparty's importance and level of interconnectedness.

54 A single point of failure is any point in a system, whether a service, activity or process, which, if it failed to work correctly, would lead to the failure of the entire system.

16.2.3 A central counterparty's arrangements with participants, operational policies and operational procedures should be periodically, and whenever necessary, tested and reviewed, especially after significant changes occur to the system or a major incident occurs. In order to minimise any effects of the testing on operations, tests should be carried out in a 'testing environment'. This testing environment should, to the extent possible, replicate the production environment (including the implemented security provisions, in particular, those regarding data confidentiality). Additionally, key elements of a central counterparty's operational risk management framework should be audited periodically and whenever necessary. In addition to periodic internal audits, external independent reviews may be necessary, depending on the central counterparty's importance and level of interconnectedness. Consistent with the evolving nature of operational risk management, a central counterparty's operational objectives should be periodically reviewed to incorporate new technological and business developments.

16.2.4 The central counterparty's operational risk management framework should include formal change management and project management processes to mitigate operational risk arising from modifications to operations, policies, procedures and controls. Change management processes should provide mechanisms for preparing, approving, tracking, testing and implementing all changes to the system. Project management processes, in the form of policies and procedures, should mitigate the risk of any inadvertent effects on a central counterparty's current or future activities due to an upgrade, expansion or alteration to its service offerings, especially for major projects. In particular, these policies and procedures should guide the management, documentation, governance, communication and testing of projects, regardless of whether projects are outsourced or executed internally.

16.3 A central counterparty should have clearly defined operational reliability objectives and should have policies in place that are designed to achieve those objectives. These policies include, but are not limited to, having: exacting targets for system availability; scalable capacity adequate to handle increasing stress volumes; and comprehensive physical and information security policies that address all potential vulnerabilities and threats.

Operational reliability

16.3.1 A central counterparty should have clearly defined operational reliability objectives and should have policies in place that are designed to achieve those objectives. These objectives serve as benchmarks for a central counterparty to evaluate its efficiency and effectiveness and evaluate its performance against expectations. These objectives should be designed to promote confidence among the central counterparty's participants. Operational reliability objectives should include the central counterparty's operational performance objectives and committed service level targets. Operational performance objectives and service level targets should define both qualitative and quantitative measures of operational performance and should explicitly state the performance standards the central counterparty is intending to meet. The central counterparty should monitor and assess regularly whether the system is meeting its established objectives and service level targets. The system's performance should be reported regularly to senior management, relevant board committees, participants, the Reserve Bank and other relevant authorities. In addition, a central counterparty's operational objectives should be periodically reviewed to incorporate new technological and business developments.

System availability

16.3.2 A central counterparty should set explicit and exacting benchmarks for the availability of key systems, commensurate with the criticality of the services it provides. Measures of system availability should be reported regularly to senior management, relevant board committees, participants, the Reserve Bank and other relevant authorities. A central counterparty should have procedures to investigate a failure to meet system availability benchmarks, including external review where appropriate, and should implement any recommended changes to operations on a timely basis.

Operational capacity

16.3.3 A central counterparty should ensure that it has scalable capacity adequate to handle increasing stress volumes and to achieve its service level objectives, such as the required processing speed. Capacity management requires that the central counterparty monitor, review and test (including stress test) the actual capacity and performance of the system on an ongoing basis. The central counterparty should carefully forecast demand and make appropriate plans to adapt to any plausible change in the volume of business or technical requirements. These plans should be based on a sound, comprehensive methodology so that the required service levels and performance can be achieved and maintained. As part of its capacity planning, a central counterparty should determine a required level of redundant capacity, taking into account the central counterparty's level of importance and interconnectedness, so that if an operational outage occurs, the system is able to resume operations and process all remaining transactions before the end of the day (see CCP Standard 16.7).

Physical and information security

16.3.4 A central counterparty should have comprehensive physical and information security policies that address all potential vulnerabilities and threats. In particular, a central counterparty should have policies effective in assessing and mitigating vulnerabilities in its physical sites from attacks, intrusions and natural disasters. A central counterparty also should have sound and robust information security policies, standards, practices and controls to ensure an appropriate level of confidence and trust in the central counterparty by all stakeholders. These policies, standards, practices and controls should include the identification, assessment, mitigation and management of current and potential future security threats and vulnerabilities for the purpose of implementing appropriate safeguards into its systems. These safeguards should both defend against the intrusion of external threats and limit the vulnerability of systems to threats that breach perimeter safeguards. System security should be subject to regular review and testing, and systems should be periodically updated as appropriate. Data should be protected from loss and leakage, unauthorised access, and other processing risks, such as negligence, fraud, poor administration and inadequate recordkeeping. A central counterparty's information security objectives and policies should conform to commercially reasonable standards for confidentiality, integrity, authentication, authorisation, non-repudiation, availability and auditability (or accountability).

16.4 A central counterparty should ensure that it can reliably access and utilise well-trained and competent personnel, as well as technical and other resources. These arrangements should be designed to ensure that all key systems are operated securely and reliably in all circumstances, including where a related body becomes subject to external administration.

Access to resources

16.4.1 Because the proper performance of a central counterparty's employees is a core aspect of any operational risk management framework, a central counterparty should be able to access and utilise sufficient well-qualified personnel. These personnel should be able to operate the system safely and consistently follow operational and risk management procedures during normal and abnormal circumstances. A central counterparty should implement appropriate human resources policies to hire, train and retain qualified personnel, thereby mitigating the effects of high rates of personnel turnover or key person risk. Additionally, a central counterparty should have appropriate human resources and risk management policies to address fraud prevention. Where appropriate, a central counterparty should also have reliable access to technical expertise and other resources external to the central counterparty as necessary to ensure the security and reliability of key systems.

Resources shared with a related body

16.4.2 In some cases a central counterparty may utilise personnel and other resources that are employed or owned by a related body. Agreements between a central counterparty and any related bodies governing such arrangements should ensure, to the extent permissible by law, that the central counterparty can continue to access key resources in all circumstances, including in the event of the related body's insolvency or external administration.

16.5 A central counterparty should identify, monitor and manage the risks that key participants, other FMIs and service and utility providers might pose to its operations. A central counterparty should inform the Reserve Bank of any critical dependencies on utilities or service providers. In addition, a central counterparty should identify, monitor and manage the risks its operations might pose to its participants and other FMIs. Where a central counterparty operates in multiple jurisdictions, managing these risks may require it to provide adequate operational support to participants during the market hours of each relevant jurisdiction.

16.5.1 A central counterparty is connected directly and indirectly to its participants, other FMIs, and its service and utility providers. Accordingly, the central counterparty should identify both direct and indirect effects on its ability to process and settle transactions in the normal course of business and manage risks that would stem from the external operational failure of a connected entity. Such effects may include those transmitted through its participants, which may participate in multiple FMIs. Likewise, a central counterparty should identify, monitor and manage the risks it poses to its participants and that it faces from and poses to other FMIs (see CCP Standard 19 on FMI links). To the extent possible, a central counterparty should coordinate business continuity arrangements with interdependent FMIs. A central counterparty also should consider the risks associated with its service and utility providers and the operational effect on the central counterparty if a service or utility provider failed to perform as expected. A central counterparty should provide reliable service, not only for the benefit of its direct participants, but also for all entities that would be affected by its ability to process transactions.

Dependencies on service providers

16.5.2 A central counterparty should have a formal policy that sets out the process for entering into, maintaining and exiting key outsourcing or service provision arrangements. Before an outsourcing or service provision arrangement is established, senior management should identify the business,

operational and other risks involved and ensure that these risks can be adequately monitored and controlled by the facility, and that the Reserve Bank and other relevant authorities are able to access sufficient information and effectively perform crisis management actions (see CCP Standards 16.9, 16.10 and 16.11). The board should approve the establishment of any outsourcing or service provision arrangement for a key business activity and be informed on a regular basis of the performance of the service provider.

16.5.3 A central counterparty that outsources operations to or is otherwise dependent on critical service providers should also disclose the nature and scope of this dependency to its participants. In addition to these service providers (such as financial messaging providers), a central counterparty is also typically dependent on the adequate functioning of utilities (such as power and telecommunication companies). As a result, a central counterparty should identify the risks from its critical service providers and utilities and take appropriate actions to manage these dependencies through appropriate contractual and organisational arrangements. A central counterparty should inform the Reserve Bank of any critical dependencies on utilities or service providers and ensure that both it and the Reserve Bank are able to access sufficient information on the performance of these utilities or service providers. To that end, the central counterparty may contractually provide for direct contacts between the critical service provider and the Reserve Bank, or contractually ensure that the Reserve Bank is able to obtain specific reports from the critical service provider. Alternatively, the central counterparty may provide the Reserve Bank with relevant information that it receives from the critical service provider.

16.5.4 A central counterparty's contractual arrangements with critical service providers should also ensure that the central counterparty's approval is mandatory before a critical service provider can itself outsource material elements of the service provided to the central counterparty, and that in the event of such an arrangement, full access to necessary information is preserved. Clear lines of communication should be established between the dependent central counterparty and the critical service provider to facilitate the flow of information between parties in both ordinary and exceptional circumstances (see CCP Standard 16.9). Additional controls may be required where outsourcing or service provision arrangements involve critical functions of the central counterparty or where relevant to crisis management (see CCP Standards 16.10 and 16.11).

16.5.5 Where a central counterparty operates in multiple jurisdictions, managing the risks that it poses to its participants may require it to provide adequate operational support to participants during the market hours of each relevant jurisdiction. In particular, where it has material Australian-based participation, the central counterparty should provide an appropriate degree of operational support to its Australian-based participants during Australian market hours. The degree of operational support should be sufficient to allow participants to resolve operational issues on a timely basis during Australian market hours (or within a reasonable extension of these hours, where necessary).

16.6 A participant of a central counterparty should have complementary operational and business continuity arrangements that are appropriate to the nature and size of the business undertaken by that participant. The central counterparty's rules and procedures should clearly specify operational requirements for participants.

16.6.1 To manage the operational risks associated with its participants, a central counterparty should establish minimum operational requirements for its participants (see also CCP Standard 17 on access and participation requirements). A central counterparty should define operational and business continuity

requirements for participants in accordance with the participant's role and importance to the system, taking into consideration the nature and scale of the business undertaken by each participant. These requirements should complement the central counterparty's own operational and business continuity arrangements. Rules and procedures should clearly and fairly specify the requirements of participants in this regard. In some cases, a central counterparty may wish to identify critical participants based on consideration of transaction volumes and values, services provided to the central counterparty and other interdependent systems, and, more generally, the potential impact on other participants and the system as a whole in the event of a significant operational problem. Critical participants may need to meet some of the same operational risk management requirements as the central counterparty itself. A central counterparty should have clear and transparent criteria, methodologies or standards for critical participants to ensure that their operational risks are managed appropriately.

Business continuity arrangements

16.7 A central counterparty should have a business continuity plan that addresses events posing a significant risk of disrupting operations, including events that could cause a wide-scale or major disruption. The plan should incorporate the use of a secondary site and should be designed to ensure that critical information technology systems can resume operations within two hours following disruptive events. Business continuity arrangements should provide appropriate redundancy of critical systems and appropriate mitigants for data loss. The business continuity plan should be designed to enable the central counterparty to facilitate settlement by the end of the day of the disruption, even in case of extreme circumstances. The central counterparty should regularly test these arrangements.

Business continuity management

16.7.1 Business continuity management is a key component of a central counterparty's operational risk management framework. A business continuity plan should have clearly stated objectives and should include policies and procedures that allow for the rapid recovery and timely resumption of critical operations following a disruption to a service, including in the event of a wide-scale or major disruption. A central counterparty should explicitly assign responsibility for business continuity planning and devote adequate resources to this planning. The plan should identify and address events that pose a significant risk of disrupting operations, including events that could cause a wide-scale or major disruption, and should focus on the impact on the operation of critical infrastructures and services. A central counterparty's business continuity plan should ensure that the central counterparty can continue to meet agreed upon service levels in such events. Both internal and external threats should be considered in the business continuity plan, and the impact of each threat should be identified and assessed. In addition to reactive measures, a central counterparty's business continuity plan may need to include measures that prevent disruptions of critical operations. All aspects of the business continuity plan should be clearly and fully documented and details of relevant procedures made available to participants.

16.7.2 The objectives of a central counterparty's business continuity plan should include the system's recovery time and recovery point. A central counterparty should aim to be able to resume operations within two hours following disruptive events; however, backup systems ideally should commence processing immediately. This may imply maintenance of dual redundancy for critical systems at its

primary site. The plan should be designed to enable the central counterparty to facilitate settlement by the end of the day even in case of extreme circumstances. Systems, including backup and data recovery procedures, should be designed to resume operations with a high degree of confidence that data will not be lost. This should include regular, and ideally real-time, replication of data across primary and secondary sites, and robust and timely procedures to recover data and transactions submitted in the interval between the last data replication and successful failover to a secondary site. Should data loss nevertheless occur, contingency plans for all central counterparties should ensure that the status of all transactions at the time of the disruption can be identified with certainty in a timely manner.

16.7.3 A central counterparty should set up a secondary site with sufficient resources, capabilities, and functionalities and appropriate staffing arrangements that would not be affected by a wide-scale disruption and would allow the secondary site to take over operations if needed.[55] The secondary site should provide the level of critical services necessary to perform the functions consistent with the recovery time objective and should be located at a sufficient geographical distance from the primary site that it has a distinct risk profile.[56] Depending on the central counterparty's importance and level of interconnectedness, the need and possibilities for a third site could be considered, in particular to provide sufficient confidence that the central counterparty's business continuity objectives will be met in all scenarios. A central counterparty should also consider alternative arrangements (for example, manual paper-based procedures) to allow for the processing of time-critical transactions in extreme circumstances. Both primary and secondary (and any additional) sites should have sufficient capacity to process volumes that are at least double projected stress volumes. This redundant capacity should be sufficient to ensure that each site is able to operate continuously and independently even in extreme circumstances.

16.7.4 A central counterparty's business continuity plan should also include clearly defined procedures for crisis and event management. The plan, for example, should address the need for rapid deployment of a multiskilled crisis and event management team as well as procedures to consult and inform participants, interdependent FMIs, the Reserve Bank and other relevant authorities, and others (such as service providers and, where relevant, the media) on a timely basis. Communication with the Reserve Bank and other relevant authorities is critical in case of a major disruption to a central counterparty's operations or wider market distress that affects the central counterparty, particularly where data held by the central counterparty may be critical for crisis management. Depending on the nature of the problem, communication channels with local civil authorities (for physical attacks or natural disasters) or computer experts (for software malfunctions or cyber-attacks) may also need to be activated. If a central counterparty has global importance or critical linkages to one or more interdependent FMIs, it should set up, test and review appropriate cross-system or cross-border crisis management arrangements.

16.7.5 A central counterparty's business continuity plan and its associated arrangements should be subject to periodic review and testing. Tests should address various scenarios that simulate wide-scale disasters

55 A particular site may be primary for certain functions and secondary for others. It is not intended that a central counterparty would be required to have numerous separate secondary sites for each of its essential functions.

56 A central counterparty should conduct a comparative risk analysis of the secondary site. The secondary site should in principle not be affected by an event that affects the primary site, with the exception of some very specific threats, such as a coordinated attack. Each site should have robust resilience based on the duplication of software and hardware, and the technology in place to replicate data between the various sites should be consistent with the chosen recovery point objectives.

and inter-site switchovers. A central counterparty's employees should be thoroughly trained to execute the business continuity plan, and participants, critical service providers and linked FMIs should be regularly involved in the testing and be provided with a general summary of the testing results. The degree of participant involvement in the testing should be appropriate to the nature and size of the business undertaken by individual participants (see CCP Standard 16.8). The central counterparty should also consider the need to participate in industry-wide tests. A central counterparty should make appropriate adjustments to its business continuity plans and associated arrangements based on the results of the testing exercises.

Incident management

16.7.6 A central counterparty should have comprehensive and well-documented procedures in place to record, report, analyse and resolve all operational incidents. After every significant disruption, a central counterparty should undertake a 'post-incident' review to identify the causes and any required improvement to the normal operations or business continuity arrangements. Such reviews should, where relevant, include the central counterparty's participants. The details of the incident and conclusions of the review should be provided to the Reserve Bank on a timely basis (see CCP Standard 21.1(h)).

16.8 A central counterparty should consider making contingency testing compulsory for the largest participants to ensure they are operationally reliable and have in place tested contingency arrangements to deal with a range of operational stress scenarios that may include impaired access to the central counterparty.

16.8.1 An operational disruption to the largest participants of a central counterparty may pose significant risks to the central counterparty's own operational performance, either directly or through interdependencies with other participants or FMIs. A central counterparty should therefore consider requiring its largest participants to perform contingency tests for their own operations with a particular focus on reliability of access to the central counterparty, and to participate in the central counterparty's own contingency testing. Where interdependencies between the central counterparty and its largest participants are significant, there will be a strong case for these participants to be involved in the central counterparty's contingency tests. Large participants' contingency tests should address the operational reliability of the participants and should cover a range of stress scenarios, including impaired access to the central counterparty.

Outsourcing and other dependencies

16.9 A central counterparty that relies upon, outsources some of its operations to, or has other dependencies with a related body, another FMI or a third-party service provider (for example, data processing and information systems management) should ensure that those operations meet the resilience, security and operational performance requirements of these CCP Standards and equivalent requirements of any other jurisdictions in which it operates.

16.9.1 A central counterparty that relies upon, outsources some of its operations to, or has other dependencies with a related body, another FMI, or a third-party service provider (for example, data processing and information systems management) should ensure that those operations meet relevant resilience, security and operational requirements of the CCP Standards and equivalent requirements of any

other jurisdiction in which it operates. Requirements placed on such service providers should be proportional to the nature of the services that they provide. Further, even when systems and processes are outsourced or provided externally, the central counterparty remains responsible for those systems and processes. The central counterparty should have robust arrangements for the selection and substitution of such providers, timely access to all necessary information, and appropriate controls and monitoring tools (see CCP Standard 16.5).

16.9.2 Where a central counterparty outsources or is otherwise dependent on a provider of a critical function – a function that is integral to the safe and effective provision of its core services as a central counterparty – a greater degree of scrutiny of arrangements may be appropriate. In scrutinising service providers in accordance with this Standard, a central counterparty that outsources or relies upon external providers of critical functions should, consistent with the expectations set out in Annex F to the Principles, ensure that each provider of these critical services:

- identifies and manages relevant operational and financial risks to its critical services and ensures that its risk management processes are effective
- implements and maintains appropriate policies and procedures, and devotes sufficient resources to ensure the confidentiality and integrity of information and the availability of its critical services in order to fulfil the terms of its relationship with the central counterparty
- implements appropriate policies and procedures to ensure that its critical services are available, reliable and resilient. Its business continuity management and disaster recovery plans should therefore support the timely resumption of its critical services in the event of an outage so that the service provided fulfils the terms of its agreement with the central counterparty
- has in place robust methods to plan for the entire lifecycle of the use of its technologies and the selection of technological standards
- provides users, including the central counterparty and, where appropriate, its participants, with sufficient information to enable them to understand clearly their roles and responsibilities in managing risks related to their use of a critical service provider.

Where a critical service provider is a regulated entity, it may be more likely to achieve these criteria. However, the central counterparty must still form its own judgement as to whether the criteria have been met. The central counterparty should inform the Reserve Bank of the arrangements it has in place to ensure that critical service providers meet these requirements (see CCP Standard 16.10).

16.10 All of a central counterparty's outsourcing or critical service provision arrangements should provide rights of access to the Reserve Bank to obtain sufficient information regarding the service provider's operation of any critical functions provided. A central counterparty should consult with the Reserve Bank prior to entering into an outsourcing or service provision arrangement for critical functions.

16.10.1 All of a central counterparty's outsourcing or critical service provision arrangements should incorporate contractual rights of access for the Reserve Bank, allowing the Reserve Bank to seek information directly from the service provider in order to assess its operational performance and reliability with regard to any critical functions provided (see CCP Standard 16.5). Notwithstanding any assessment that the Reserve Bank may make regarding such service providers, a central counterparty should independently monitor the adherence of outsourcing or critical service providers to the resilience,

security and operational performance requirements of the CCP Standards and other relevant standards (see CCP Standard 16.9).

16.10.2 Prior to entering into an outsourcing or service provision arrangement for a critical function, a central counterparty should consult with the Reserve Bank (see also CCP Standard 21 on regulatory reporting). As part of this consultation process, the central counterparty should provide the Reserve Bank with details of the arrangement, including provisions that satisfy the requirements of CCP Standards such as 16.5, 16.9, 16.10 and 16.11, and any other provisions necessary to comply with the operational requirements under the CCP Standards.

16.11 A central counterparty should organise its operations, including any outsourcing or critical service provision arrangements, in such a way as to ensure continuity of service in a crisis and to facilitate effective crisis management actions by the Reserve Bank or other relevant authorities. These arrangements should be commensurate with the nature and scale of the central counterparty's operations.

16.11.1 A central counterparty should ensure that its operations, including any outsourcing or critical service provision arrangements, are organised in such a way that it is able to provide continuous and reliable service in a crisis, and that the Reserve Bank or other relevant authorities are able to take effective action to manage or resolve a crisis. A central counterparty may need to consider contractual arrangements with outsourcing providers or other service providers that contain explicit provisions safeguarding continuity of service in crisis scenarios, including financial distress to the central counterparty.

16.11.2 A systemically important central counterparty should have robust arrangements to ensure continuity of service and facilitate effective crisis management actions by the Reserve Bank or other relevant authorities.[57] A systemically important central counterparty that also has a strong connection to the Australian real economy and financial system should also organise its operations so as to facilitate resolution actions taken by the Reserve Bank or other relevant authorities. This may require that the central counterparty directly operate critical functions, or, for outsourced or externally provided functions and to the extent supported by law, provide for contractual rights of access to any appointed statutory manager in a resolution scenario. These rights of access would need to survive termination of the outsourcing or service provision agreement. In determining whether a systemically important central counterparty has a strong connection to the Australian real economy and financial system, the following factors are likely to be relevant:

- whether the central counterparty offers services in a domestic or international market
- the mix of domestic and international participants in the central counterparty
- the potential for disruption to the central counterparty to affect the real economy
- whether the market serviced by the central counterparty is retail or wholesale
- whether the central counterparty clears a domestic securities market
- links that the central counterparty has with other Australian FMIs.

57 See guidance to CCP Standard 7.7 for factors the Reserve Bank will consider in assessing the systemic importance of a central counterparty.

Standard 17: Access and participation requirements

A central counterparty should have objective, risk-based and publicly disclosed criteria for participation, which permit fair and open access.

Guidance

Access refers to the ability to use a central counterparty's services and includes the direct use of the central counterparty's services by participants, including other market infrastructures (for example, trading platforms) and, where relevant, service providers (for example, matching and portfolio compression service providers). In some cases, this includes the rules governing indirect participation. A central counterparty should allow for fair and open access to its services. It should control the risks to which it is exposed by its participants by setting reasonable risk-related requirements for participation in its services. A central counterparty should ensure that its participants and any linked FMIs have the requisite operational capacity, financial resources, legal powers and risk management expertise to prevent unacceptable risk exposure for the central counterparty and other participants. A central counterparty's participation requirements should be clearly stated and publicly disclosed so as to eliminate ambiguity and promote transparency.

17.1 A central counterparty should allow for fair and open access to its services, including by direct and, where relevant, indirect participants and other FMIs, based on reasonable risk-related participation requirements.

17.1.1 Restrictions on access can result in highly tiered clearing arrangements and potentially give rise to concentration risks (see CCP Standard 18 on tiered participation arrangements). Further, direct access to one or more central counterparties may play an important role in meeting other public policy objectives around the depth, efficiency and liquidity of markets, and support any market-wide plan for the safe and efficient clearing of certain classes of financial instruments (for example, any mandatory clearing of certain classes of derivatives). Care should therefore be taken that participation requirements do not arbitrarily limit access to a central counterparty's services.

17.1.2 While pursuing the benefits of fair and open access, however, a central counterparty's participation requirements should not compromise its risk-based controls or conflict with directors' statutory duties. Indeed, a central counterparty should always consider the risks that an actual or prospective participant may pose, both to the central counterparty and to other participants. This will typically entail risk-related participation requirements adequate to ensure that its participants meet appropriate operational, financial and legal standards consistent with timely fulfilment of their obligations to the central counterparty.

17.2 A central counterparty's participation requirements should be justified in terms of the safety of the central counterparty and the markets it serves, be tailored to and commensurate with the central counterparty's specific risks, and be publicly disclosed. Subject to maintaining acceptable risk control standards, a central counterparty should endeavour to set requirements that have the least restrictive impact on access that circumstances permit.

17.2.1 A central counterparty's participation requirements should be justified in terms of the safety of the central counterparty and the markets it serves, be tailored to the central counterparty's specific risks,

be imposed in a manner commensurate with such risks, and be set out in the central counterparty's rules and publicly disclosed. The requirements should be objective and should not unnecessarily discriminate against particular classes of participants or introduce competitive distortions.[58] Operational requirements may include reasonable criteria relating to the participant's ability and readiness (for example, its information technology capabilities) to use a central counterparty's services. Financial requirements may include reasonable risk-related capital requirements, other evidence of financial strength and creditworthiness, and contributions to prefunded default arrangements. Legal requirements may include appropriate licences and authorisations to conduct relevant activities as well as legal opinions or other arrangements that demonstrate that possible conflicts of law would not impede the ability of an applicant (for example, a foreign entity) to meet its obligations to the central counterparty. A central counterparty also may require participants to have appropriate risk management expertise. If a central counterparty admits non-regulated entities, it should take into account any additional risks that may arise from their participation and design its participation requirements and risk management controls accordingly.

17.2.2 To help address the balance between open access and risk, a central counterparty should set participation requirements and manage its participant-related risks through the use of real-time binding risk management controls and other operational arrangements that have the least restrictive impact on access that circumstances permit. One way a central counterparty can manage participant-related risks is to use real-time binding credit limits or collateral requirements. The permitted level of participation may be different for participants maintaining different levels of capital. Where other factors are equal, participants holding higher levels of capital may be permitted less restrictive risk limits or be able to participate in more functions within the central counterparty. Such risk management controls may mitigate the need for a central counterparty to impose onerous participation requirements that limit access. A central counterparty could also differentiate its services to provide different levels of access at varying levels of cost and complexity. For example, a central counterparty may wish to limit full direct participation to certain types of entities, and to apply limits to the activities of, or provide indirect access to, others. Participation requirements (and other risk controls) can be tailored to each class or tier of participants based on the risks each class or tier poses to the central counterparty and its participants.

17.2.3 When clearing on behalf of other market participants, a clearing participant assumes responsibility for the risks those market participants bring to the central counterparty. It is therefore important that the clearing participant has appropriate financial and operational resources and risk management arrangements to fulfil its obligations to the central counterparty arising from this activity. In some markets, there may be relatively few clearing participants with the financial and operational resources to fulfil this role, and therefore the potential concentration of exposures in a small number of direct clearing participants may argue for closer monitoring and perhaps more stringent participation requirements for clearing participants that provide clearing services to other market participants (see also CCP Standard 18 on tiered participation arrangements). Where tiering exists, each class of participation should be clearly defined and the participation requirements should be the same for all applicants of the same class.

58 A similar principle is set out in the guidance to CCP Standard 12.1, in relation to the proportionality of obligations placed on non-defaulting participants in the event of a default.

17.2.4 Notwithstanding that participation requirements based solely on a participant's size or capital may be insufficiently related to risk, and therefore deserve careful scrutiny, some objective threshold metric such as minimum capital is likely to be necessary, perhaps as a backstop to other more risk sensitive requirements. Requirements such as customised collateralisation of exposures beyond certain limits are typically dependent on real-time monitoring of both a participant's credit standing and the exposures it brings to the central counterparty. Both may be subject to rapid and perhaps unexpected changes. A minimum capital requirement may therefore help to guard against unexpected shocks, which could in some circumstances deliver losses that were not directly related to the magnitude of normal course risks run by the participant. A minimum capital requirement also ensures that a participant is of sufficient scale to justify investment in more comprehensive operational and compliance frameworks. This might be expected to reduce the potential for such shocks. Moreover, a minimum capital requirement may help to ensure that participants commit significant financial resources to the clearing business and assume the responsibility that direct participation entails. Indeed, to the extent that participants have capital allocated to this specific function, they have an incentive to monitor and control the risks they bring to the central counterparty. Nevertheless, an assessment of the appropriate level of minimum capital can only be made in the context of the whole suite of a central counterparty's risk control measures.

17.3 A central counterparty should monitor compliance with its participation requirements on an ongoing basis and have clearly defined and publicly disclosed procedures for facilitating the suspension and orderly exit of a participant that breaches, or no longer meets, the participation requirements.

17.3.1 A central counterparty should monitor compliance with its participation requirements on an ongoing basis through the receipt of timely and accurate information. Participants should be obliged to report any developments that may affect their ability to comply with a central counterparty's participation requirements. A central counterparty should have the authority to impose additional risk controls on a participant in situations where the central counterparty determines the participant poses heightened risk to the central counterparty. For example, if a participant's credit standing comes into doubt, the central counterparty may require the participant to provide additional margin or collateral or may place restrictions on the level or types of activities that the participant can undertake (see CCP Standard 4 on credit risk). A central counterparty should consider additional reporting requirements for non-regulated institutions. A central counterparty should also have clearly defined and publicly disclosed procedures for, in extreme cases, facilitating the suspension and orderly exit of a participant that breaches, or no longer meets, the participation requirements of the central counterparty (see CCP Standard 4 on credit risk and CCP Standard 12 on participant default rules and procedures).

17.3.2 If a central counterparty has an appeals process for suspending or cancelling participation in the central counterparty, the appeals process should not detract from the central counterparty's ability to suspend or cancel participation. For serious breaches, the preferable approach would be for the suspension or cancellation to persist during an appeal, with reinstatement upon a successful appeal, rather than the suspension or cancellation being put on hold until an appeal is heard.

Standard 18: Tiered participation arrangements

A central counterparty should identify, monitor and manage the material risks to the central counterparty arising from tiered participation arrangements.

Guidance

Tiered participation arrangements occur when some firms (indirect participants) rely on the services provided by other firms (direct participants) to use the central counterparty's clearing facilities.[59]

The dependencies and risk exposures (including credit, liquidity and operational risks) inherent in these tiered arrangements can present risks to the central counterparty and its smooth functioning, as well as to the participants themselves and the broader financial markets. For example, if a central counterparty has few direct participants but many indirect participants with large values or volumes of transactions, it is likely that a large proportion of the transactions processed by the central counterparty depend on a few direct participants. This will increase the severity of the effect on the central counterparty of a default of a direct participant or an operational disruption at a direct participant. The credit exposures in tiered relationships can also affect the central counterparty. If the value of an indirect participant's transactions is large relative to the direct participant's capacity to manage the risks, this may increase the direct participant's default risk. In some cases, for example, central counterparties offering indirect clearing will face credit exposures to indirect participants (or arising from indirect participants' positions) if a direct participant defaults. There may also be legal or operational risk to the central counterparty if there is uncertainty about the liability for indirect participant transactions and how these transactions will be handled in the event of a default (see CCP Standard 1 on legal basis).

The nature of these risks is such that they are most likely to be material where there are indirect participants whose business through the central counterparty is a significant proportion of the central counterparty's overall business or is large relative to that of the direct participant(s) through which they access the central counterparty's services. Typically, the identification, monitoring and management of risks from tiered participation will therefore be focused on financial institutions that are the immediate customers of direct participants and depend on the direct participant for access to a central counterparty's services. In exceptional cases, however, tiered participation arrangements may require the central counterparty to look beyond the direct participant and its immediate customer.

There are limits on the extent to which a central counterparty can, in practice, observe or influence direct participants' commercial relationships with their customers. However, a central counterparty will often have access to information on transactions undertaken on behalf of indirect participants and can set direct participation requirements that may include criteria relating to how direct participants manage relationships with their customers insofar as these criteria are relevant for the safe operation of the central counterparty. At a minimum, a central counterparty should identify the types of risk that could arise from tiered participation and should monitor concentrations of such risk. If a central counterparty or its smooth operation is exposed

59 This Standard considers tiered participation arrangements that arise from the different relationships that participants may have with the central counterparty. One type of relationship is with participants in the central counterparty that are bound by the central counterparty's rules and agreements. Such 'direct participants' and the management of the risks they present should be fully covered by the rules and agreements of the central counterparty and are generally dealt with in other CCP Standards. A second type of relationship is with entities that are not bound by the rules of the central counterparty, but whose transactions are cleared by or through the central counterparty. In this Standard, these entities are defined as 'indirect participants' in the central counterparty.

to material risk from tiered participation arrangements, the central counterparty should seek to manage and limit such risk.

18.1 A central counterparty should ensure that its rules, procedures and agreements allow it to gather basic information about indirect participation in order to identify, monitor and manage any material risks to the central counterparty arising from such tiered participation arrangements.

18.1.1 A central counterparty may be able to obtain information relating to tiered participation through its own systems or by collecting it from direct participants. A central counterparty should ensure that its procedures, rules and agreements with direct participants allow it to gather basic information about indirect participants in order to identify, monitor and manage any material risks to the central counterparty arising from such tiered participation arrangements. This information should enable the central counterparty, at a minimum, to identify: the proportion of activity that direct participants conduct on behalf of indirect participants; direct participants that act on behalf of a material number of indirect participants; indirect participants with significant volumes or values of transactions in the system; and indirect participants whose transaction volumes or values are large relative to those of the direct participants through which they access the central counterparty.[60]

18.2 A central counterparty should identify material dependencies between direct and indirect participants that might affect the central counterparty.

18.2.1 A central counterparty should identify material dependencies between direct and indirect participants that can affect the central counterparty. Indirect participants will often have some degree of dependence on the direct participant through which they access the central counterparty. In the case of a central counterparty with few direct participants but many indirect participants, it is likely that a large proportion of the transactions processed by the central counterparty would depend on the operational performance of those few direct participants. Disruption to the services provided by the direct participants – whether for operational reasons or because of a participant's default – could therefore present a risk to the smooth functioning of the system as a whole. The central counterparty should identify and monitor material dependencies of indirect participants on direct participants so that the central counterparty has readily available information on which significant indirect participants may be affected by problems at a particular direct participant.

18.2.2 In some cases, issues at an indirect participant could affect the central counterparty. This is most likely to occur where a large indirect participant accesses a central counterparty's facilities through a relatively small direct participant (see CCP Standard 18.3). Failure of this significant indirect participant to perform as expected, such as by failing to meet its payment obligations, or stress at the indirect participant, such as that which causes others to delay payments to the indirect participant, may affect the direct participant's ability to meet its obligations to the central counterparty. Central counterparties should therefore identify and monitor the material dependencies of direct participants on indirect participants so that the central counterparty has readily available information on how the central counterparty may be affected by problems at an indirect participant, including which direct participants may be affected.

60 If satisfying this Standard requires the collection of sensitive information that may advantage one party over another, the central counterparty should ensure that the sensitive information is appropriately protected and used only for risk purposes rather than commercial purposes.

18.3 A central counterparty should identify indirect participants responsible for a significant proportion of transactions processed by the central counterparty and indirect participants whose transaction volumes or values are large relative to the capacity of the direct participants through which they access the central counterparty in order to manage the risks arising from these transactions.

Credit and liquidity risks in tiered participation arrangements

18.3.1 Tiered participation arrangements typically create credit and liquidity exposures between direct and indirect participants. The management of these exposures is the responsibility of the participants and, where appropriate, subject to supervision by their regulators. A central counterparty is not expected to manage the credit and liquidity exposures between direct and indirect participants, although the central counterparty may have a role in applying credit or position limits in agreement with the direct participant. A central counterparty should, however, have access to information on concentrations of risk arising from tiered participation arrangements that may affect the central counterparty, allowing it to identify indirect participants responsible for a significant proportion of the central counterparty's transactions or whose transaction volumes or values are large relative to those of the direct participants through which they access the central counterparty. A central counterparty should identify and monitor such risk concentrations.

18.3.2 In a central counterparty, direct participants are responsible for the performance of their customers' financial obligations to the central counterparty. The central counterparty may, however, face an exposure to indirect participants (or arising from indirect participants' positions) if a direct participant defaults, at least until such time as the defaulting participant's customers' positions are ported to another participant or closed out. If a participant default would leave the central counterparty with a potential credit exposure related to an indirect participant's positions, the central counterparty should ensure it understands and manages the exposure it would face. For example, the central counterparty may set participation requirements that require the direct participant, on the central counterparty's request, to demonstrate that it is adequately managing relationships with its customers to the extent that they may affect the central counterparty. A central counterparty should also consider establishing concentration limits on exposures to indirect participants, where appropriate.

Indirect participation and default scenarios

18.3.3 Default scenarios can create uncertainty about the status of indirect participants' positions and exposures. Default scenarios can also raise legal and operational risks for the central counterparty if there is uncertainty about whether the indirect or direct participant is liable for outstanding obligations to the central counterparty. A central counterparty should ensure that its rules and procedures are clear regarding the status of indirect participants' positions and exposures (including the point at which they become subject to the rules of the system and the point after which the rules of the system no longer apply). A central counterparty should also ensure that it adequately understands its direct participants' processes and procedures for managing an indirect participant's default.

Encouraging direct participation

18.3.4 Direct participation in a central counterparty usually provides a number of benefits, some of which may not be available to indirect participants. Moreover, indirect participants are vulnerable to the

risk that their access to a central counterparty is withdrawn or disrupted. If these indirect participants have large values or volumes of business through the central counterparty, this may affect the smooth functioning of the central counterparty. For these reasons, where an indirect participant accounts for a material proportion of the transactions processed by a central counterparty, it may be appropriate to encourage direct participation. For example, a central counterparty may in some cases establish objective thresholds above which direct participation would normally be encouraged (provided that the firm satisfies the central counterparty's access criteria). Setting such thresholds and encouraging direct participation should be based on risk considerations rather than commercial advantage.

18.4 A central counterparty should regularly review risks arising from tiered participation arrangements and should take mitigating action when appropriate.

18.4.1 A central counterparty should regularly review risks to which it may be exposed as a result of tiered participation arrangements. If material risks exist, the central counterparty should take mitigating action as appropriate. The results of the review process should be reported to the board of directors and updated periodically and after substantial amendments to a central counterparty's rules.

Standard 19: FMI links

A central counterparty that establishes a link with one or more FMIs should identify, monitor and manage link-related risks.

Guidance

A link is a set of contractual and operational arrangements between two or more FMIs that connect the FMIs directly or through an intermediary. A central counterparty may establish a link with another central counterparty for the primary purpose of expanding its services to additional financial instruments, markets or institutions. For example, a central counterparty may establish a link with another central counterparty to enable a participant in the first central counterparty to clear trades with a participant in the second central counterparty without having to maintain two central counterparty relationships. A central counterparty may also establish a link with a different type of FMI. For example, a central counterparty for securities markets must establish and use a link to a central securities depository to receive and deliver securities. This Standard covers links between central counterparties as well as links between a central counterparty and other types of FMI, such as securities settlement facilities, central securities depositories and trade repositories.[61] If a central counterparty establishes a link, it should identify, monitor and manage its link-related risks, including legal, operational, credit and liquidity risks.[62] Further, a central counterparty that establishes multiple links should ensure that the risks generated by one link do not affect the soundness of the other links and linked FMIs. Mitigation of such spillover effects requires the use of effective risk management controls, including additional financial resources or the harmonisation of risk management frameworks across linked FMIs.

19.1 Before entering into a link arrangement, and on an ongoing basis once the link is established, a central counterparty should identify, monitor and manage all potential sources of risk arising from the link arrangement. Link arrangements should be designed such that the central counterparty is able to comply with these CCP Standards.

61 Links to payment systems are not addressed by this Standard because these links are addressed in CCP Standard 9 on money settlements.

62 Prior to entering into a link arrangement, a central counterparty should inform its participants of the expected effects on the central counterparty's risk profile. See also CCP Standard 20 on disclosure of rules, key policies and procedures, and market data.

Identifying link-related risks

19.1.1 Before entering into a link arrangement, and on an ongoing basis once the link is established, a central counterparty should identify and assess all potential sources of risk arising from the link arrangement. The type and degree of risk varies according to the design and complexity of the central counterparty and linked FMIs and the nature of the relationship between them. In a simple case of a vertical link, for example, a central counterparty may provide basic services to another FMI, or vice versa. Such links typically pose only operational and custody risks. Other links, such as an arrangement in which a central counterparty provides clearing services to another central counterparty may be more complex and may pose additional risks to the central counterparty, such as credit and liquidity risks. Cross-margining by two or more central counterparties may also pose additional risk because the central counterparties may rely on each other's risk management systems to measure, monitor and manage credit and liquidity risks (see CCP Standard 6 on margin). In addition, links between a central counterparty and other FMIs may pose specific risks to the central counterparty or other FMIs in the link arrangement. In all cases, link arrangements should be designed such that the central counterparty is able to observe the CCP Standards.

Managing operational risk

19.1.2 A central counterparty should obtain an appropriate level of information about each linked FMI's operations in order for the central counterparty to perform effective periodic assessments of the operational risk associated with the link. In particular, central counterparties should ensure that risk management arrangements and processing capacity are sufficiently scalable and reliable to operate the link safely for both the current and projected peak volumes of activity processed over the link (see CCP Standard 16 on operational risk). Systems and communication arrangements between the central counterparty and linked FMIs also should be reliable and secure so that the link does not pose significant operational risk to the central counterparty and the linked FMIs. Any reliance by a central counterparty on a critical service provider should be disclosed as appropriate to the linked FMI and the central counterparty should require reciprocal disclosure from the linked FMI. In addition, a linked central counterparty should identify, monitor and manage operational risks due to complexities or inefficiencies associated with differences in time zones, particularly as these affect staff availability. Governance arrangements and change management processes should ensure that changes in the central counterparty or a linked FMI will not inhibit the smooth functioning of the link, related risk management arrangements, or non-discriminatory access to the link (see CCP Standard 2 on governance and CCP Standard 17 on access and participation requirements).

Managing financial risk

19.1.3 A central counterparty in a link arrangement should effectively measure, monitor and manage its financial risk, including custody risk, arising from the link arrangement. A central counterparty should ensure that it and its participants have adequate protection of assets in the event of the insolvency of a linked FMI or a participant default in a linked FMI.

19.2 A link should have a well-founded legal basis, in all relevant jurisdictions, that supports its design and provides adequate protection to the central counterparty and other FMIs involved in the link.

19.2.1 A link involving a central counterparty should have a well-founded legal basis, in all relevant jurisdictions, that supports its design and provides adequate protection to the central counterparty. Cross-border links may present legal risk arising from differences between the laws and contractual rules governing the linked FMIs and their participants, including those relating to rights and interests, collateral arrangements, settlement finality and netting arrangements (see CCP Standard 1 on legal basis). For example, differences in law and rules governing settlement finality could lead to a scenario in which a transfer is regarded as final in the central counterparty but not final in the linked FMI, or vice versa. In some jurisdictions, differences in laws may create uncertainties regarding the enforceability of central counterparty obligations assumed by novation, open offer or other similar legal device. For instance, in the case of a link between two central counterparties, differences in insolvency laws may unintentionally give a participant in one central counterparty a claim on the assets or other resources of the linked central counterparty in the event of the first central counterparty's default. To limit such uncertainties, the respective rights and obligations of the linked FMIs and, where necessary, their participants should be clearly defined in the link agreement. In a cross-jurisdictional context, the terms of the link agreement should also set out an unambiguous choice of law that will govern each aspect of the link.

19.3 Where relevant to its operations in Australia, a central counterparty should consult with the Reserve Bank prior to entering into a link arrangement with another FMI.

19.3.1 Prior to entering into a link arrangement with another FMI that is relevant to its operations in Australia, a central counterparty should consult with the Reserve Bank. As part of this consultation, the central counterparty should provide the Reserve Bank with a comprehensive description of the link arrangement. This description should include details of the legal basis of the link, and any financial obligations or operational interdependencies created by the link, including obligations created for both the central counterparty and the linked FMI. A central counterparty should provide sufficient detail to demonstrate that the link arrangement will not adversely affect its compliance with the CCP Standards. Where the Reserve Bank identifies aspects of the proposal that may create unacceptable risks for the central counterparty, the central counterparty should make any necessary changes to the proposal to control or mitigate these risks prior to implementation. These changes may be necessary to ensure that the central counterparty continues to comply with the CCP Standards and equivalent standards in other relevant jurisdictions.

19.3.2 Where a linked FMI's principal place of business is not in Australia, the Reserve Bank may also consult with the regulator of the linked FMI in its principal place of business, in order to understand the overseas regulator's assessment of the link arrangement and to ensure that all relevant legal, regulatory, operational and financial risk issues have been considered and addressed.

19.4 Before entering into a link with another central counterparty, a central counterparty should identify and manage the potential spillover effects from the default of the linked central counterparty. If a link has three or more central counterparties, a central counterparty should identify, assess and manage the risks of the collective link arrangement.

19.4.1 A central counterparty may establish links with one or more other central counterparties. Although the details of individual link arrangements among central counterparties differ significantly because of the varied designs of central counterparties and the markets they serve, there are two basic types of central counterparty links: peer-to-peer links and participant links.

19.4.2 In a peer-to-peer link, a central counterparty maintains special arrangements with another central counterparty and is not subject to normal participant rules. Typically, however, the central counterparties exchange margin and other financial resources on a reciprocal basis. The linked central counterparties face current and potential future exposures to each other as a result of the process whereby they each net the trades cleared between their participants so as to create novated (net) positions between the central counterparties. Risk management between the central counterparties is based on a bilaterally approved framework, which is different from that applied to a normal participant.

19.4.3 In a participant link, one central counterparty (the participant central counterparty) is a participant in another central counterparty (the host central counterparty) and is subject to the host central counterparty's normal participant rules. In such cases, the host central counterparty maintains an account for the participant central counterparty and would typically require the participant central counterparty to provide margin, as would be the case for a participant that is not a central counterparty. A participant central counterparty should mitigate and manage its risk from the link separately from the risks in its core clearing and settlement activities. For example, if the host central counterparty were to default, the participant central counterparty may not have adequate protection because the participant central counterparty does not hold collateral from the host central counterparty to mitigate the counterparty risk posed to it by the host central counterparty. Risk protection in a participant link is one-way, unlike in a peer-to-peer link. A participant central counterparty that provides margin but does not collect margin from another linked central counterparty should therefore hold additional financial resources to protect itself against the default of the host central counterparty.

19.4.4 Both types of links – peer-to-peer and participant links – may present new or increased risks that should be measured, monitored and managed by the central counterparties involved in the link, particularly with respect to the risk management of the financial exposures that potentially arise from the link arrangement. Before entering into a link with another central counterparty, a central counterparty should identify and assess the potential spillover effects from the default of the linked central counterparty. If a link has three or more central counterparties, a central counterparty should identify and assess the risks of the collective link arrangement. A network of links between central counterparties that does not properly acknowledge and address the inherent complexity of multi-central counterparty links could have significant implications for systemic risk.

19.4.5 Because of the different possible types of link arrangements, different types of central counterparties, and differences in the legal and regulatory frameworks in which central counterparties may operate, different combinations of risk management tools may be used by the central counterparty. When linked central counterparties have materially different risk management frameworks, the risks stemming from the link are more complex. In this case, a central counterparty should carefully assess the effectiveness of its risk management models and methodologies, including its default procedures, in order to determine whether and to what extent the inter-central counterparty risk management frameworks should be harmonised or whether additional risk mitigation measures would be sufficient to mitigate risks arising from the link.

19.4.6 A central counterparty linked to one or more other central counterparties should maintain arrangements that are effective in managing the risks arising from the link; such arrangements often involve a separate default fund to cover that risk. In principle, the risk management measures related to the link should not reduce the resources that a central counterparty holds to address other risks.

The most direct way to achieve this outcome is for a central counterparty not to participate in another central counterparty's default fund, which may in turn mean that the central counterparty will need to provide additional margin. However, in arrangements in which central counterparties have agreed, consistent with their regulatory framework, to contribute to each other's default funds, the central counterparty should assess and mitigate the risks of making such contributions via specific conditions. In particular, funds used by a central counterparty to contribute to another central counterparty's default fund must represent prefunded additional financial resources and must not include resources used by the central counterparty to satisfy its regulatory requirements to hold sufficient capital or participant margin funds (or any other funds, including independent default fund resources) held by the central counterparty to mitigate the counterparty risk presented by its participants. Nor should it include funds held by the central counterparty to fund its plans for recovery or orderly wind-down (see CCP Standard 14 on general business risk). The contributing central counterparty should further ensure that any consequent exposure of its own participants to the risk of a participant default in the linked central counterparty is fully transparent to and understood by its participants. The contributing central counterparty may, for example, consider it appropriate that the default fund contribution is made only by those of its participants that use the link, if applicable. Moreover, the resources provided by one central counterparty to another should be held in such a way that they are ring fenced from other resources provided to that central counterparty. For example, securities could be held in a separate account at a custodian. Cash would need to be held in segregated accounts to be considered acceptable collateral in this case. Finally, in case of a participant default in the first central counterparty, the use of the linked central counterparty's contribution to the default fund of the first central counterparty could be restricted or limited. For example, the linked central counterparty's contribution to the default fund could be put at the bottom of the first central counterparty's default waterfall.

19.4.7 Link arrangements between central counterparties will expose each central counterparty to sharing in potentially uncovered credit losses if the linked central counterparty's default waterfall has been exhausted. For example, a central counterparty may be exposed to loss mutualisation from defaults of a linked central counterparty's participants. This risk will be greater to the extent that the first central counterparty is unable directly to monitor or control the other central counterparty's participants. Such contagion risks can be even more serious in cases where more than two central counterparties are linked, directly or indirectly, and a central counterparty considering such a link should satisfy itself that it can manage such risks adequately. A central counterparty should ensure that the consequent exposure of its own participants to a share in these uncovered losses is fully understood and disclosed to its participants. A central counterparty may consider it appropriate to devise arrangements to avoid sharing in losses that occur in products other than those cleared through the link and to confine any loss sharing to only participants that clear products through the link. Depending on how losses would be shared, a central counterparty may need to increase financial resources to address this risk.

19.4.8 A central counterparty should ensure that default fund contributions or allocation of uncovered losses are structured so that: the central counterparty is not treated less favourably than the participants of the other central counterparty; and the central counterparty's contribution to the loss sharing arrangements of the other central counterparty is proportional to the risk that the first central counterparty poses to the linked central counterparty.

19.5 A central counterparty in a central counterparty link arrangement should be able to cover, at least on a daily basis, its current and potential future exposures to the linked central

counterparty and its participants, if any, fully with a high degree of confidence without reducing the central counterparty's ability to fulfil its obligations to its own participants at any time.

19.5.1 Exposures faced by a central counterparty from a linked central counterparty should be identified, monitored and managed with the same rigour as exposures from a central counterparty's participants to prevent a default at one central counterparty from triggering a default at a linked central counterparty. Such exposures should be covered fully, primarily through the use of margin or other equivalent financial resources. In particular, each central counterparty in a central counterparty link arrangement should be able to cover, at least on a daily basis, its current and potential future exposures to the linked central counterparty and its participants, if any, fully with a high degree of confidence without reducing the central counterparty's ability to fulfil its obligations to its own participants at any time (see CCP Standard 6 on margin). Financial resources used to cover inter-central counterparty current exposures should be prefunded with highly liquid assets that exhibit low credit risk. Best practice is for a central counterparty to have near real-time inter-central counterparty risk management. However, at a minimum, financial exposures among linked central counterparties should be marked to market and covered on a daily basis. A central counterparty also needs to consider and address the risks arising from links in designing its stress tests and calibrating its prefunded default arrangements. A central counterparty should also take into account the potential effects on its risk management framework of contributions to other central counterparties' prefunded default arrangements, exchange of margin, common participants, major differences in risk management tools, and other relevant features, especially in relation to legal, credit, liquidity and operational risks.

Standard 20: Disclosure of rules, key policies and procedures, and market data

A central counterparty should have clear and comprehensive rules, policies and procedures and should provide sufficient information and data to enable participants to have an accurate understanding of the risks they incur by participating in the central counterparty. All relevant rules and key policies and procedures should be publicly disclosed.

Guidance

A central counterparty should provide sufficient information to its participants and prospective participants to enable them to identify clearly and understand fully the risks and responsibilities of participating in the system. To achieve this objective, a central counterparty should adopt and disclose written rules, policies and procedures that are clear and comprehensive and that include explanatory material written in plain language so that participants can fully understand the system's design and operations, their rights and obligations, and the risks of participating in the system. A central counterparty's rules, policies, procedures and explanatory material need to be accurate, up to date and readily available to all current and prospective participants. Moreover, a central counterparty should disclose to participants and the public basic operational information and responses to the CPSS-IOSCO *Disclosure Framework for Financial Market Infrastructures*.

20.1 A central counterparty should adopt clear and comprehensive rules, policies and procedures that are fully disclosed to participants. Relevant rules and key policies and procedures should

also be publicly disclosed (including specific requirements relating to CCP Standards 1.4, 2.2, 12.3, 13.4, 15.4, 17.2 and 17.3).

20.1.1 A central counterparty should adopt clear and comprehensive rules, policies and procedures that are fully disclosed to participants. Relevant rules and key policies and procedures should also be publicly disclosed. A central counterparty's rules, policies and procedures are typically the foundation of the central counterparty and provide the basis for participants' understanding of the risks they incur by participating in the central counterparty.

20.2 A central counterparty's rules, policies and procedures should clearly identify the nature and scope of the risk exposure assumed by the central counterparty, such as by novation, open offer or other similar legal devices. A central counterparty's rules, policies and procedures should clearly identify the point in the clearing process at which the central counterparty assumes the risk exposure.

20.2.1 A central counterparty should clearly communicate to all its participants the nature and scope of its assumption of risk exposure through novation, open offer or other similar legal devices. This should be clearly set out in the central counterparty's rules, policies and procedures, including identification of the point in the clearing process at which the central counterparty assumes the risk exposure. Clear disclosure of the legal device through which the central counterparty assumes risk exposure will assist participants in identifying and managing their own risks arising from the trading, clearing and settlement process (see CCP Standard 1 on legal basis).

20.3 A central counterparty should disclose clear descriptions of the system's design and operations, as well as the central counterparty's and participants' rights and obligations, so that participants can assess the risks they would incur by participating in the central counterparty (see CCP Standards 2.8 and 9.5).

20.3.1 Relevant rules, policies and procedures should include clear descriptions of the system's design and operations, as well as the rights and obligations of the central counterparty and its participants, so that participants can assess the risk they would incur by participating in the central counterparty.[63] They should clearly outline the respective roles of participants and the central counterparty as well as the rules, policies and procedures that will be followed in routine operations and non-routine, though foreseeable, events, such as a participant default (see CCP Standard 12 on participant default rules and procedures). In particular, a central counterparty should have clear and comprehensive rules, policies and procedures for addressing financial and operational problems within the system. For example, rules, policies and procedures should identify which parties are to be notified of specific events and the timetables for decision-making and notification. They should make clear the degree of discretion parties are able to exercise in taking decisions that can have a direct effect on the operation of the system.

20.3.2 In addition to disclosing all relevant rules and key policies and procedures, a central counterparty should have a clear and fully disclosed process for proposing and implementing changes to its rules, policies and procedures and for informing participants, and the Reserve Bank and other relevant authorities, of these changes. Similarly, the rules, policies and procedures should clearly disclose the degree of discretion that a central counterparty can exercise over key decisions that directly affect the

63 Information should be disclosed to the extent it would not risk prejudicing the security and integrity of the central counterparty or divulging commercially sensitive information, such as trade secrets or other intellectual property.

operation of the system, including in crises and emergencies (see also CCP Standard 1 on legal basis and CCP Standard 2 on governance). For example, a central counterparty's procedures may provide for discretion regarding the extension of operating hours to accommodate unforeseen market or operational problems. A central counterparty also should have appropriate procedures to minimise any conflict of interest issues that may arise when authorised to exercise its discretion.

20.4 A central counterparty should provide all necessary and appropriate documentation and training to facilitate participants' understanding of the central counterparty's rules, policies and procedures and the risks they face from participating in the central counterparty.

20.4.1 Participants bear primary responsibility for understanding the rules, policies, procedures and risks of participating in a central counterparty as well as the risks they may incur when the central counterparty has links with other FMIs. A central counterparty, however, should provide all documentation, training and information necessary to facilitate participants' understanding of the central counterparty's rules, policies and procedures and the risks they face from participation. New participants should receive training, before using the system, and existing participants should receive, as needed, additional periodic training. A central counterparty should disclose to each individual participant stress test scenarios used, individual results of stress tests, and other data to help each participant understand and manage the potential financial risks stemming from participation in the central counterparty.[64] Other relevant information that should be disclosed to participants, but typically not to the public, includes relevant aspects of the central counterparty's business continuity arrangements.[65]

20.4.2 A central counterparty is well placed to observe the performance of its participants and should promptly identify those participants whose behaviour demonstrates a lack of understanding of, or compliance with, applicable rules, policies, procedures and risks of participation. In such cases, a central counterparty should take steps to rectify any perceived lack of understanding by the participant and take other remedial action necessary to protect the central counterparty and its participants. This may include notifying senior management within the participant institution. In cases in which the participant's actions present significant risk or present cause for the participant's suspension, the central counterparty should notify the Reserve Bank and other relevant authorities.

20.5 A central counterparty should complete regularly and disclose publicly responses to the CPSS-IOSCO *Disclosure Framework for Financial Market Infrastructures*. A central counterparty also should, at a minimum, disclose basic risk and activity data, as directed by the Reserve Bank from time to time.

Disclosure framework and other information

20.5.1 A central counterparty should complete regularly, and disclose publicly, responses to the CPSS-IOSCO *Disclosure Framework for Financial Market Infrastructures*. The central counterparty should provide comprehensive and appropriately detailed disclosures to support the overall transparency of the central counterparty, its governance, operations and risk management framework. In order for the disclosures to reflect correctly the central counterparty's current rules, policies, procedures and

64 In disclosing stress-test information to individual participants, central counterparties should avoid revealing information regarding the positions of other individual participants.

65 Information on business continuity that can undermine a central counterparty's safety and soundness should not be disclosed to the public. However, this information should be disclosed to the Reserve Bank and other relevant authorities.

operations, the central counterparty should update its responses following material changes to the system or its environment. At a minimum, a central counterparty should review its responses to the CPSS-IOSCO *Disclosure Framework for Financial Market Infrastructures* each year to ensure continued accuracy and usefulness.

20.5.2 Other relevant information for participants and, more generally, the public could include general information on the central counterparty's full range of activities and operations, such as the names of direct participants in the central counterparty, key times and dates in its operations, and its overall risk management framework (including its margin methodology and assumptions).[66] A central counterparty should also disclose its financial condition, financial resources to withstand potential losses, timeliness of settlements, and other performance statistics. With respect to data, a central counterparty should, at a minimum, disclose basic data on transaction volumes and values, margin and collateral holdings, prefunded default resources, and liquid resources. The central counterparty should also disclose any additional data that the Reserve Bank may direct it to disclose from time to time.

Forms of disclosure

20.5.3 A central counterparty should make the relevant information and data it discloses as set forth in these CCP Standards readily available through generally accessible media, such as the internet, in English in addition to any other language(s) relevant to the scope of its operations. The data should be accompanied by robust explanatory documentation that enables users to understand and interpret the data correctly.

Standard 21: Regulatory reporting

A central counterparty should inform the Reserve Bank in a timely manner of any events or changes to its operations or circumstances that may materially impact its management of risks or ability to continue operations. A central counterparty should also regularly provide information to the Reserve Bank regarding its financial position and risk controls on a timely basis.

Guidance

The *Corporations Act 2001* and the CCP Standards impose requirements for notification to the Reserve Bank in certain circumstances. This Standard sets out some of these requirements and imposes additional reporting requirements.

Oral notification to the Reserve Bank may be appropriate, particularly in circumstances where timely communication is needed. In practice, this should be followed by notification in writing.

To assist in meeting this Standard, formal points of liaison will be agreed upon between the central counterparty and the Reserve Bank.

21.1 A central counterparty should inform the Reserve Bank as soon as reasonably practicable if:

(a) it breaches, or has reason to believe that it will breach:

(i) a CCP Standard; or

66 A clear description of the typical life cycle of the transaction clearing and settlement process under normal circumstances may also be useful for participants and the public. This information would highlight how the central counterparty processes a transaction, including the timeline of events, the validation and checks to which a transaction is subject, and the responsibilities of the parties involved.

(ii) its broader legislative obligation to do, to the extent that it is reasonably practicable to do so, all things necessary to reduce systemic risk;

(b) it becomes subject to external administration, or has reasonable grounds for suspecting that it will become subject to external administration;

(c) a related body to the central counterparty becomes subject to external administration, or if the central counterparty has reasonable grounds for suspecting that a related body will become subject to external administration;

(d) a participant becomes subject to external administration, or if the central counterparty has reasonable grounds for suspecting that a participant will become subject to external administration;

(e) a participant fails to meet its obligations under the central counterparty's risk control requirements or has its participation suspended or cancelled because of a failure to meet the central counterparty's risk control requirements;

(f) it fails to enforce any of its own risk control requirements;

(g) it plans to make significant changes to its risk control requirements or its rules, policies and procedures;

(h) it or a service it relies on from a third party or outsourced provider experiences a significant operational disruption, including providing the conclusions of its post-incident review;

(i) any internal audits or independent external expert reviews are undertaken of its operations, risk management processes or internal control mechanisms, including providing the conclusions of such audits or reviews;

(j) its operations or risk controls are affected, or are likely to be affected, by distress in financial markets;

(k) it has critical dependencies on utilities or service providers, including providing a description of the dependency and an update if the nature of this relationship changes;

(l) it proposes to grant a security interest over its assets (other than a lien, right of retention or statutory charge that arises in the ordinary course of business);

(m) it proposes to incur or permit to subsist any loans from participants or members unless such loans are subordinated to the claims of all other creditors of the central counterparty; or

(n) any other matter arises which has or is likely to have a significant impact on its risk control arrangements (see also CCP Standards 1.6, 16.10 and 19.3).

21.2 A central counterparty should also provide to the Reserve Bank, on a timely basis:

(a) audited annual accounts;

(b) management accounts on a regular basis, and at least quarterly;

(c) risk management reports, including detailed information on margining and stress testing, on a regular basis, and at least quarterly;

(d) periodic activity, risk and operational data, as agreed with the Reserve Bank; and

(e) any other information as specified by the Reserve Bank from time to time.

Glossary

Unless the contrary intention appears, the terms in the guidance to the *Financial Stability Standards for Central Counterparties* (CCP Standards) have the meanings provided for in this Glossary. Wordings or terms used in this Glossary importing the singular shall include the plural and vice versa where the context requires.

Note: This Glossary is based largely on the glossary to the Principles, and the CPSS Glossary of Terms Used in Payments and Settlement Systems*, added to and amended by the Reserve Bank as appropriate.* [67]

Term	Definition
affiliate	This term means 'associated entity' as defined in section 50AAA of the *Corporations Act 2001*.
backtesting	A comparison of previously observed outcomes with expected outcomes derived from the use of margin models.
batch settlement	The settlement of groups of payments, transfer instructions or other obligations together at one or more discrete, often pre-specified times during the processing day.
business continuity	A state of uninterrupted business operations. This term also refers to all of the organisational, technical and staffing measures used to ensure the continuation of operations following a disruption to a service, including in the event of a wide-scale or major disruption.
central bank money	A liability of a central bank, in this case in the form of deposits held at the central bank, which can be used for settlement purposes.
central counterparty	An entity that interposes itself between counterparties to contracts traded in one or more financial markets, becoming the buyer to every seller and the seller to every buyer, and thereby ensuring the performance of open contracts.
central securities depository	An entity that provides securities accounts, central safekeeping services, and asset services, which may include the administration of corporate actions and redemptions, and plays an important role in helping to ensure the integrity of securities issues (i.e. ensure that securities are not accidentally or fraudulently created or destroyed or their details changed).
choice of law	A contractual provision by which parties choose the law that will govern their contract or relationship. Choice of law may also refer to the question of what law should govern in the case of a conflict of laws.
clearing	The process of transmitting, reconciling, and, in some cases, confirming transactions prior to settlement, potentially including the netting of transactions and the establishment of final positions for settlement. For the clearing of futures and options, this term also refers to the daily balancing of profits and losses and the daily calculation of collateral requirements.
close out	The process of offsetting an existing contract by entering into a new contract of an equal and opposite position.
collateral	An asset or third-party commitment that is used by a collateral provider to secure an obligation vis-à-vis a collateral taker.

67 *A Glossary of Terms Used in Payments and Settlement Systems* is available at <http://www.bis.org/publ/cpss00b.pdf>.

Term	Definition
commercial bank money	A liability of a commercial bank, in the form of deposits held at the commercial bank, which can be used for settlement purposes.
conflict of laws	An inconsistency or difference in the laws of jurisdictions that have a potential interest in a transaction.
counterparty	A party to a trade.
credit risk	The risk that a counterparty, whether a participant or other entity, will be unable to meet fully its financial obligations when due, or at any time in the future.
critical-service provider	A related entity or third party that provides services to a central counterparty that are integral to the safe and effective provision of its core services as a central counterparty.
cross-margining arrangement	An agreement among central counterparties to consider positions and supporting collateral at their respective organisations as a common portfolio for participants that are members of two or more of the organisations.
current exposure	The loss that a central counterparty (or in some cases, its participants) would face immediately if a participant were to default. Current exposure is technically defined as the larger of zero or the market value (or replacement cost) of a transaction or portfolio of transactions within a netting set with a counterparty that would be lost upon the default of the counterparty.
custody risk	The risk of loss on assets held in custody in the event of a custodian's (or sub-custodian's) insolvency, negligence, fraud, poor administration or inadequate recordkeeping.
default	An event stipulated in an agreement as constituting a breach or default. Generally, such events relate to a failure to complete a transfer of funds or securities in accordance with the terms and rules of the system in question.
delivery versus delivery (DvD)	A securities settlement mechanism that links two securities transfers in such a way as to ensure that delivery of one security occurs if and only if the corresponding delivery of the other security occurs.
delivery versus payment (DvP)	A securities settlement mechanism that links a securities transfer and a funds transfer in such a way as to ensure that delivery occurs if and only if the corresponding payment occurs.
derivative	A financial contract whose value depends on the value of one or more underlying reference assets, rates or indices, on a measure of economic value or on factual events.
Exchange Settlement Account	An account held at the Reserve Bank which is used for the final settlement of obligations between Exchange Settlement Account holders.
external administration	This term has the meaning given by section 5 of the *Payment Systems and Netting Act 1998*.
failover	The process of switching over to a standby system in the event of an operational disruption.

Term	Definition
final settlement	The irrevocable and unconditional transfer of an asset or financial instrument, or the discharge of an obligation by a central counterparty or its participants in accordance with the terms of the underlying contract. Final settlement is a legally defined moment.
financial market infrastructure (FMI)	A multilateral system among participating institutions, including the operator of the system, used for the purposes of clearing, settling or recording payments, securities, derivatives or other financial transactions. Examples of FMIs include central counterparties, securities settlement facilities, securities settlement systems, central securities depositories, payments systems and trade repositories.
general business risk	Any potential impairment of the central counterparty's financial position (as a business concern) as a consequence of a decline in its revenues or an increase in its expenses, such that expenses exceed revenues and result in a loss that must be charged against capital.
governance	The set of relationships between a central counterparty's owners, board of directors (or equivalent), management and other relevant parties, including participants, authorities and other stakeholders (such as participants' customers, other interdependent FMIs and the broader market).
haircut	A risk control measure applied to underlying assets whereby the value of those underlying assets is calculated as the market value of the assets reduced by a certain percentage (the 'haircut'). Haircuts are applied by a collateral taker in order to protect itself from losses resulting from declines in the market value of a security in the event that it needs to liquidate that collateral.
initial margin	Collateral that is collected to cover potential changes in the value of each participant's position (i.e. potential future exposure) over the appropriate close out period in the event that the participant defaults.
investment risk	The risk of loss faced by a central counterparty when it invests its own or its participants' resources, such as collateral.
legal risk	The risk of the unexpected application of a law or regulation, usually resulting in a loss.
linked FMI	An FMI that is connected with one or more other FMIs, either directly or through an intermediary, according to a set of contractual and operational arrangements between the FMIs involved in the link.
liquidity risk	The risk that a counterparty, whether a participant or other entity, will have insufficient funds to meet its financial obligations as and when expected, although it may be able to do so in the future.
mark to market	The practice of revaluing securities and financial instruments using current market prices.
money settlement agent	The entity whose assets are used to settle the ultimate payment obligations arising from securities transfers within a securities settlement facility or other clearing and settlement activities. Accounts with the money settlement agent are held by settlement banks, which may act on their own behalf and/or offer payment services to participants that do not have accounts with the money settlement agent.

Term	Definition
money settlement asset	An asset which carries little or no credit or liquidity risk and is used to settle payment obligations arising from trades in financial products.
multilateral net batch	The settlement of groups of payments, transfer instructions or other obligations together at a discrete, often pre-specified time, where these obligations have been offset among multiple participants.
netting	The offsetting of obligations between or among participants in the netting arrangement, thereby reducing the number and value of payments or deliveries needed to settle a set of transactions.
novation	A process through which the original obligation between a buyer and a seller is discharged through the substitution of a central counterparty as seller to the buyer and buyer to the seller, creating two new contracts.
omnibus	An account structure where securities or collateral belonging to some or all customers of a particular participant are commingled and held in a single account segregated from those of the participant.
open offer	A process through which a central counterparty extends an 'open offer' to act as counterparty to market participants and thereby is interposed between participants at the time a trade is executed.
operational risk	The risk that deficiencies in information systems or internal processes, human errors, management failures or disruptions from external events will result in the reduction, deterioration or breakdown of services provided by a central counterparty.
over-the-counter (OTC)	A method of trading that does not involve an exchange. In over-the-counter markets participants trade directly with each other, typically through telephone or computer links.
payment system	A set of instruments, procedures and rules for the transfer of funds between or among participants; the system includes the participants and the entity operating the arrangement.
payment versus payment (PvP)	A settlement mechanism that ensures that the final transfer of a payment in one currency occurs if and only if the final transfer of a payment in another currency or currencies takes place.
physical delivery	The delivery of an asset, such as an instrument or commodity, in physical form.
pooled resources	Financial resources of a central counterparty that are available in the event of a participant default, and are not restricted in their use to a particular participant. Pooled resources may be provided on a mutualised basis by participants, may be provided on a commercial basis by an external provider (such as a commercial lender, investor, insurer or liquidity provider), or may be backed by the central counterparty's own capital or that of a related body.
portability	The operational aspects of the transfer of contractual positions, funds or securities from one party to another party.

Term	Definition
potential future exposure	Any potential credit exposure that a central counterparty could face at a future point in time. Potential future exposure is technically defined as the maximum exposure estimated to occur at a future point in time at a high level of statistical confidence. Potential future exposure arises from potential fluctuations in the market value of a participant's open positions between the time they are incurred or reset to the current market price, and the time they are liquidated or effectively hedged.
prefunded default arrangements	Financial resources of a central counterparty that are contributed to the central counterparty on an ongoing basis prior to, and available in the event of, a participant default. Examples include margin, a guarantee fund and a central counterparty's own capital.
principal risk	The risk that a counterparty will lose the full value involved in a transaction, for example, the risk that a seller of a financial asset will irrevocably deliver the asset but not receive payment.
procyclicality	Changes in risk management requirements or practices that are positively correlated with business or credit cycle fluctuations and that may cause or exacerbate financial instability.
real-time gross settlement (RTGS)	The real-time settlement of payments, transfer instructions or other obligations individually on a transaction-by-transaction basis.
related body	A 'related body corporate' as defined in section 9 of the *Corporations Act 2001*.
replacement cost	The unrealised gain on the unsettled contract or the cost of replacing the original contract at market prices that may be changing rapidly during periods of stress.
repurchase agreement (repo)	A contract to sell and subsequently repurchase securities at a specified date and price.
securities	Any financial product (within the meaning given in the *Corporations Act 2001*) of a kind in relation to which obligations are prescribed under the Corporations Regulations 2001 for the purposes of section 768A(1)(b) of the Corporations Act.
securities settlement facility	A clearing and settlement facility that enables its participants to transfer title to or other interests in securities, typically in return for payment. A securities settlement facility may also operate a central securities depository.
segregation	A method of protecting customer collateral and contractual positions by holding or accounting for them separately from those of the direct participant (such as a carrying firm or broker).
settlement bank	The entity that maintains accounts with the money settlement agent in order to settle payment obligations arising from securities transfers, or other clearing and settlement activities, both on its own behalf and for other market participants.
settlement risk	The general term used to designate the risk that settlement in a funds or securities transfer system will not take place as expected. This risk may comprise both credit and liquidity risk.
specific wrong-way risk	The risk that an exposure to a counterparty is highly likely to increase when the creditworthiness of that counterparty is deteriorating.
stress testing	The estimation of credit and liquidity exposures that would result from the realisation of extreme price changes.

Term	Definition
systemic risk	The risk that the inability of one or more participants to perform as expected will cause other participants to be unable to meet their obligations when due.
systemically important	A central counterparty is systemically important if its distress or disorderly failure, because of its size, complexity and systemic interconnectedness, would cause significant disruption to the wider financial system and economic activity. In assessing the systemic importance of a central counterparty in Australia, the Reserve Bank will take into account relevant factors, including: the size of the central counterparty in Australia; the availability of substitutes for the central counterparty's services in Australia; the nature and complexity of the products cleared by the central counterparty; and the degree of interconnectedness with other parts of the Australian financial system.
trade repository	An entity that maintains a centralised electronic record (database) of transaction data.
unwinding	The process used to recalculate obligations in some net settlement systems where transfers between the accounts of participants are provisional until all of them have finally discharged their settlement obligations. If a particular participant fails to settle, some or all of the provisional transfers involving that participant are deleted from the system and the settlement obligations of the remaining participants are recalculated.
value date	The day on which the payment, transfer instruction or other obligation is due and the associated funds and securities are typically available to the receiving participant.
variation margin	Funds that are collected and paid out to reflect current exposures resulting from actual changes in market prices.
zero-hour rule	A provision in the insolvency law of some countries whereby the transactions conducted by an insolvent institution after midnight on the date the institution is declared insolvent are automatically ineffective or revocable by operation of law.