FINANCIAL MARKET INFRASTRUCTURES STANDARDS: GUIDANCE

March 2024

Reserve Bank of New Zealand
Te Pūtea Matua

FMA
FINANCIAL MARKETS AUTHORITY
TE MANA TĀTAI HOKOHOKO

Ref #20368230 v1.0

Contents

Glossary of Acronyms

CCP	Central counterparty
CSD	Central securities depository
DNS	Deferred net settlement
DvD	Delivery versus delivery
DvP	Delivery versus payment
HVPS	High-value payment system
PvP	Payment versus payment
RTGS	Real-time gross settlement
SSS	Securities settlement system

Definitions

The words and phrases used in the Financial Market Infrastructures (FMI) Standards have the same meaning as in the Financial Market Infrastructures Act 2021 (the **Act**). In the FMI Standards and this Guidance:

Applicable auditing and assurance standards has the same meaning as in section 5(1) of the Financial Reporting Act 2013.

Central bank money means a liability of a central bank, in the form of deposits held at the central bank, which can be used for settlement purposes.

Central counterparty or **CCP** means a designated FMI that is classed in a designation notice under section 29 of the Act as a central counterparty.

Central securities depository or **CSD** means a designated FMI that is classed in a designation notice under section 29 of the Act as a central securities depository.

Close out means terminating or liquidating a contract, or net position under multiple contracts (including through the acceleration or termination of obligations under one or more contracts or exercising rights to set-off or net financial exposures created under one or more contracts).

Close out rights means contractual rights that enable a party to terminate or liquidate a contract, or net position under multiple contracts (including through the acceleration or termination of obligations under one or more contracts, or exercising rights to set-off or net financial exposures created under one or more contracts).

Close out rules means any rules of the FMI designed to facilitate the exercise of close out rights.

Commercial bank money means a liability of a commercial bank, in the form of deposits held at the commercial bank, which can be used for settlement purposes.

Critical services means services that are necessary for an FMI to provide essential services without material disruption.

Critical service provider means a person or entity that provides critical services to an operator of an FMI.

Custodian means an entity that safe keeps and administers securities or other assets for its customers, such as a licensed deposit taker or regulated trustee company.

Custody risk means the risk of loss of assets held in custody in the event of an operator's insolvency, negligence, fraud, poor administration, or inadequate recordkeeping.

Cyber means relating to, within, or through the medium of the interconnected information infrastructure of interactions among persons, processes, data, and information systems.

Cyber event means any observable occurrence in an information system. Cyber events sometimes provide an indication that a cyber incident is occurring.

Cyber incident means a cyber event that:

a) jeopardises the cyber security of an information system or the information the system processes, stores or transmits; or

b) violates the security policies, security procedures or acceptable use policies, whether resulting from malicious activity or not.

Cyber resilience means the ability of an organisation to continue to carry out its mission by anticipating and adapting to cyber threats and other relevant changes in the environment and by withstanding, containing and rapidly recovering from cyber incidents.

Cyber resilience framework means the policies, procedures, and internal systems an entity has established to identify, protect, detect, respond to, and recover from the reasonably foreseeable sources of cyber risks it faces.

Cyber resilience strategy means an entity’s high-level principles and medium-term plans to achieve its objective of managing cyber risk.

Cyber risk means the combination of the probability of cyber incidents occurring and their impact.

Cyber risk appetite means the level of tolerance that an entity has for cyber risk. It includes how much cyber risk an entity is willing to tolerate and how much an entity is willing to invest or spend to manage the risk.

Cyber risk tolerance means the level of cyber risk an entity is willing to assume.

Deferred net settlement mechanism or **DNS mechanism** means a settlement mechanism which settles on a net basis at the end of a predefined settlement cycle.

Essential services means services provided by the FMI:

a) for designated FMIs which are assessed as systemically important by the regulator under section 24 of the Act, all services contributing to the assessment that an FMI is systemically important; and

b) for designated FMIs that are not assessed as systemically important under section 24 of the Act, any services covered by the protections in subpart 5 of Part 3 of the Act.

Exchange of value settlement system means a system that settles transactions that involve the settlement of two linked obligations (for example, securities or foreign exchange transactions).

FMI Standards means the standards issued under section 31 of the Act.

Haircut means a risk control measure applied to underlying assets where the value of those underlying assets is calculated as the market value of the assets reduced by a certain percentage.

High value payment system or **HVPS** means a funds transfer system that typically handles large value and high priority payments.

Internal systems means mechanisms within an FMI or operator to implement policies, procedures, or controls.

Investor central securities depository means a central securities depository that opens an account with an issuer central securities depository to enable the cross-system settlement of securities transactions.

Issuer central securities depository means a central securities depository where securities are issued or immobilised.

Link means a set of arrangements, which may be contractual or operational, or both, between two or more FMIs that connect the FMIs directly or through an intermediary.

Margin means collateral that is collected to protect against current or potential future exposures resulting from market price changes or in the event of a counterparty default.

Margin model means an economic model used for calculating the amount of margin needed.

Margin system means a system for managing margin, including the margin model, transferring, and holding margin.

Material aspects of an FMI's activities means those activities that relate to the provision of essential services by the FMI.

Material incident means an event —

a) that causes:

i) a slowdown in the operation of the FMI system; or

ii) a restriction or partial availability of the FMI system; or

iii) a security threat to the system; or

iv) an increase in the risk of an outage, slowdown, restriction, or security threat, or

v) a potential or actual adverse impact on the future operation of the system; and

b) that has a substantive adverse impact on the FMI's participants (or for an overseas-equivalent FMI, the FMI's New Zealand participants) or the New Zealand financial system.

Nostro agent means a bank or other financial institution in a jurisdiction other than the one the FMI operates in holding an account on behalf of an operator that is denominated in the currency of that other jurisdiction and used for the purposes of settlement.

Outage means an event that causes the system to be unavailable for use by any or all participants (or for an overseas-equivalent FMI, the FMI's New Zealand participants), regardless of:

a) the cause; and

b) the length of time of the outage.

Overseas-equivalent FMI means a designated FMI that is specified in its designation notice under section 29(2)(f) of the Act as falling within the class of an overseas-equivalent FMI.

Portability means the ability to transfer contractual positions, funds, or securities from one party to another party.

Principal risk means the risk arising where one of two linked obligations is settled but the other obligation is not.

Qualified auditor means any of the following:

a) a licensed auditor as defined in section 6(1) of the Auditor Regulation Act 2011; or

b) a registered audit firm as defined in section 6(1) of the Auditor Regulation Act 2011; or

c) the Auditor-General as defined in section 4 of the Public Audit Act 2001.

RBNZ Act means the Reserve Bank of New Zealand Act 2021.

Relevant jurisdiction mean any jurisdictions in which the FMI operates, and will always include New Zealand.

Segregation means the protection of customer collateral and contractual positions by holding or accounting for them separately from those of the direct participant.

Tiered participation arrangement means an arrangement that occurs when some indirect participants rely on the services provided by direct participants to use the FMI's central payment, clearing, or settlement facilities.

Value date means the day on which the payment, transfer instruction or other obligation is due.

About this Guidance

Background

This guidance is intended to assist operators of Financial Market Infrastructures (FMIs), designated under the Financial Market Infrastructures Act 2021 (the Act), meet the requirements set out in the FMI Standards issued under section 31 of the Act.

The Act establishes a comprehensive framework for the oversight and regulation of FMIs. The purposes of the Act include promoting the maintenance of a sound and efficient financial system and promoting and facilitating the development of fair, efficient, and transparent financial markets.

FMIs are a set of critical systems which allow electronic payments and financial market transactions to occur. More precisely, FMIs are multilateral systems that provide clearing, settlement, and reporting services in relation to payments, securities, derivatives, and other financial transactions. There are several types of FMIs, including payment systems, securities settlement systems, central securities depositories, central counterparties, and trade repositories. The services provided by FMIs are managed or administered in different ways by different operators. As a result, the FMI Standards apply to operators of different types of designated FMIs in different ways.

The Reserve Bank of New Zealand (RBNZ) and the Financial Markets Authority (FMA) are jointly the 'regulator' of FMIs as defined in the Act except:

- in relation to pure payment systems, where the RBNZ is the sole regulator; and
- in circumstances where the RBNZ and FMA agree that one of them will act as the sole regulator.

The FMI Standards and this guidance are based on the *Principles for financial market infrastructures* (PFMI) issued by the Committee on Payments and Market Infrastructure (CPMI) and the International Organization of Securities Commissions (IOSCO). The FMI Standards largely incorporate the PFMI into New Zealand law.

Under section 31 of the Act the regulator may impose standards on operators of designated FMIs or otherwise require operators to ensure compliance with the standards. This is because an operator is a legal person who has the responsibility of providing or managing the services of the FMI, or maintaining or administering the FMI's rules, and an FMI is a system that is in operation. Therefore, the FMI Standards impose obligations on operators of designated FMIs rather than on the FMIs themselves. While an operator may not need to directly fulfil a requirement outlined in the FMI Standards, an operator bears the legal obligation to ensure that the requirement is fulfilled.

In some areas, we have elaborated on the PFMI to make the FMI Standards more applicable to the New Zealand operating environment. This includes more detailed requirements relating to operational risk, including contingency planning, management of risk associated with third-party critical service providers and cyber risk, and also in relation to disclosure and notification requirements.

Central bank operated FMIs

We have also modified the PFMI in their application to central bank operated FMIs in line with CPMI-IOSCO's guidance on the issue: *Application of the "Principles for financial market infrastructures" to central bank FMIs*.

In general, the FMI Standards apply in the same way to central bank-operated FMIs as they apply to other FMIs, which we consider appropriate given the importance of RBNZ-operated FMIs to New Zealand's financial system. However, there are scenarios where the FMI Standards need to be interpreted in light of the broader context in which central banks operate. For example:

- Standard 2: 'Governance' should be interpreted in light of the governance requirements the RBNZ is subject to under the Reserve Bank of New Zealand Act 2021; and
- requirements under Standard 4: 'Credit risk' and Standard 5: 'Collateral' are not intended to affect central bank policies relating to lender of last resort functions; and
- requirements under Standard 13: 'Participant-default rules and procedures' and Standard 18: 'Access and participation requirements' are not intended to affect a central bank's ability to act to support financial stability (as central banks do not generally bear a risk of becoming insolvent, it does not make sense to impose financial resource requirements on them – see Standard 7: 'Liquidity risk' and Standard 15: 'General business risk'); and
- where the operator is the central bank, contingency planning requirements are different due to monetary sovereignty's inherent financial soundness, and the fact that it does not bear investment or credit risk like most entities (scenarios such as liquidity shortfalls, credit losses, general business losses or realisation of investment losses are therefore unlikely to be relevant – see Standard 17A: 'Contingency Plans').

Status of this guidance

This guidance document does not itself impose legal obligations on operators of FMIs. Instead, it provides guidance on how the regulator expects operators to consider and apply the obligations imposed by the FMI Standards. It also outlines international best practice for managing risks associated with operating FMIs, and should be read in line with *Guidance Note: Overseas FMIs*.

Table 1: General applicability of standards to Operators of specific types of FMIs.

Standard	PSs	CSDs	SSSs	CCPs	Overseas equivalent FMIs
1. Legal basis	✓	✓	✓	✓	
2. Governance	✓	✓	✓	✓	
3. Framework for the comprehensive management of risks	✓	✓	✓	✓	
4. Credit risk	✓		✓	✓	
5. Collateral	✓		✓	✓	
6. Margin				✓	
7. Liquidity risk	✓		✓	✓	
8. Settlement finality	✓		✓	✓	
9. Money settlements	✓		✓	✓	
10. Physical deliveries		✓	✓	✓	
11. Central securities depositories		✓			
12. Exchange-of-value settlement systems	✓		✓	✓	
13. Participant-default rules and procedures	✓	✓	✓	✓	
14. Segregation and portability				✓	
15. General business risk	✓	✓	✓	✓	
16. Custody and investment risks	✓	✓	✓	✓	
17. Operational risk	✓	✓	✓	✓	
17A. Contingency plans	✓	✓	✓	✓	
17B. Critical service providers	✓	✓	✓	✓	
17C. Cyber resilience	✓	✓	✓	✓	
18. Access and participation requirements	✓	✓	✓	✓	
19. Tiered participation requirements	✓	✓	✓	✓	
20. FMI links		✓	✓	✓	
21. Efficiency and effectiveness	✓	✓	✓	✓	
22. Communication procedures and standards	✓	✓	✓	✓	
23. Disclosure of rules, key procedures, and market data	✓	✓	✓	✓	
23A. Disclosing compliance with the FMI Standards	✓	✓	✓	✓	
23B. Notifying the regulator	✓	✓	✓	✓	✓

STANDARD 1: LEGAL BASIS

1.1 A robust legal basis for an operator's and material aspects of an FMI's activities (as defined in Standard 1: 'Legal basis') in all relevant jurisdictions is critical to an FMI's overall soundness. The legal basis provides the foundation for relevant parties to define the rights and obligations of an operator, the FMI, its participants, and other relevant parties, such as the FMI's participants' customers, custodians, settlement banks, 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 FMI. Therefore, for risk management to be sound and effective, the enforceability of rights and obligations relating to an FMI and its risk management must be clearly established. If the legal basis for the material aspects of an operator's or FMI's activities and operations is inadequate, uncertain, or opaque, then an operator, an FMI, its participants, and their customers may face unintended, uncertain, or unmanageable credit or liquidity risks, which could create or amplify systemic risks.

Legal basis

1.2 The legal basis must provide a high degree of certainty for each of the material aspects of an FMI's activities including those that apply to the operator and its FMI's activities in all relevant jurisdictions in which the FMI operates, including New Zealand. The legal basis includes the legal framework and the FMI's rules 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. The legal framework that governs competition, and consumer and investor protection may also be relevant in some jurisdictions. Laws specific to an operator's or the FMI's activities include:

a) those governing its authorisation and its regulation, supervision, and oversight;and

b) rights and interests in financial instruments; and

c) settlement finality; and

d) netting; and

e) immobilisation and dematerialisation of securities; and

f) arrangements for DvP, PvP, or DvD; and

g) collateral arrangements (including margin arrangements); and

h) default procedures; and

i) the resolution of an FMI.

1.3 An operator should establish rules and contracts that are clear, understandable, and consistent with applicable legislation and regulations, and any relevant overseas standard, and provide a high degree of legal certainty. An operator must also consider whether the rights and obligations of the operator or the FMI's participants,

and other parties, as outlined in its rules and contracts, are consistent with relevant industry standards and market protocols.

1.4 An operator must be able to articulate the legal basis and enforceability for all material aspects of an FMI's activities to the regulator, participants, and, when requested, participants' customers, in a clear and understandable way. Standard 1: 'Legal basis', requires an operator to articulate the legal basis for the enforceability of an FMI's rules and contracts by obtaining independent legal opinion(s). The legal opinion(s) should demonstrate the enforceability of the FMI's rules across all relevant jurisdictions and provide reasoned support for its conclusions. An operator must review and update legal opinion(s) on the enforceability of its rules and procedures whenever there is a material change of circumstances or at a minimum, every two years from the date of the last review or update (as relevant). In addition, an operator should seek to ensure that all material aspects of the FMI's activities have an effective legal basis in all relevant jurisdictions. For the purposes of Standard 1: 'Legal basis' in considering what a relevant jurisdiction is, an operator should consider its legal risk in relation to:

a) where an FMI is conducting business (including through linked FMIs); and

b) where its participants are incorporated, located, or otherwise conducting business for the purposes of participation, noting that the legal risk is likely to increase with the number of participants being located in a particular jurisdiction; and

c) where collateral is located or held; and

d) the jurisdiction indicated in relevant contracts the FMI operates under.

Rights and interests

1.5 An operator should ensure that the rules and contracts for the FMI clearly define the rights and interests of the operator and the FMI, 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 FMI. An operator should ensure that the legal basis for material aspects of the FMI's activities and the operator's protects both a participant's assets held in custody and, where appropriate, a participant's customer's assets held by or through the FMI, from the insolvency of relevant parties and other relevant risks. The legal basis should also ensure that the operator is able to protect these assets when they are held at a custodian or linked FMI. In particular, consistent with Standard 11: 'Central securities depositories' and Standard 14: 'Segregation and portability', the legal basis should protect the assets and positions of a participant's customers in a designated CSD or CCP.

1.6 In addition, the legal basis should provide certainty with respect to an operator's interests in, and rights to use and dispose of, collateral; an operator's authority to transfer ownership rights or property interests; and an operator's rights to make and receive payments, in all cases, notwithstanding the bankruptcy or insolvency of its participants, participants' customers, or custodian bank.

1.7 An operator should structure the FMI's current and future 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.

Settlement finality

1.8 If the FMI's designation notice states that it is subject to subpart 5 of Part 3 of the Act, then the Act provides legal certainty about the finality of settlements. In other cases, the operator should ensure the FMI rules promote settlement finality (see also Standard 8: 'Settlement finality'). An operator should consider, in particular, the actions that would need to be taken in the event of a participant's insolvency. If an FMI is not covered by subpart 5 of Part 3 of the Act, 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. An operator also should consider the legal framework for the external settlement mechanisms the FMI uses, such as funds transfer or securities transfer systems. The laws of the relevant jurisdictions should support the provisions of an operator's or FMI's (as appropriate) contractual arrangements with its participants and settlement banks relating to finality.

Netting arrangements

1.9 If the FMI's designation notice states that it is subject to subpart 5 of Part 3 of the Act, this subpart of the Act provides legal certainty regarding the enforceability of netting under the FMI's rules. In other cases, if an FMI's rules include 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. Current and future netting arrangements should be designed to be explicitly recognised and supported under the law of all relevant jurisdictions (including New Zealand) and enforceable against an FMI and an FMI's failed participants in an insolvency event. Without such legal assurances of enforceability, insolvency proceedings in New Zealand or elsewhere could undermine netting arrangements. If these challenges are successful, an operator and its participants could be liable for gross settlement amounts that could drastically increase obligations because gross obligations could be many multiples of net obligations.

1.10 Where a CCP's designation notice states that it is covered by subpart 5 of Part 3 of the Act, this provides legal certainty about the enforceability of the CCP's rules (including under the CCP's rules that enable an FMI to act as a CCP). In other cases, these devices should also be founded on a sound legal basis. In novation (and substitution), the original contract between the buyer and seller is discharged and two new contracts are created, one between the CCP and the buyer, and the other between the CCP and the seller. The CCP thereby assumes the original parties' contractual obligations to each other. In an open-offer system, the CCP 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, 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 CCP is supporting the transaction.

Enforceability

1.11 Where an FMI's designation notice states that it is covered by subpart 5 of Part 3 of the Act, this provides legal certainty about the enforceability of the FMI's rules. The rules and contracts related to an FMI's operation must be enforceable in all relevant jurisdictions. In particular, the FMI's legal arrangements should support the enforceability of the participant-default rules and procedures that an operator uses 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 Standard 13: 'Participant-default rules and procedures'). An operator 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. Ambiguity about the enforceability of procedures could delay and possibly prevent an operator from taking actions to fulfil its obligations to non-defaulting participants or to minimise its potential losses.

1.12 An operator should ensure current and future rules, and contracts related to the FMI's operations are enforceable when an operator is implementing the plans for recovery or orderly wind-down (to the extent this is not already addressed by the application of subpart 5 of Part 3 of the Act). Where relevant, the rules and contracts should adequately address issues and associated risks resulting from (a) cross-border participation and interoperability of FMIs; and (b) foreign participants in the case of an FMI which is being wound down. There should be a high degree of certainty that actions taken by an operator under such rules will not be voided, reversed, or subject to stays. Ambiguity about the enforceability of rules and contracts that facilitate the implementation of the contingency plan of the FMI could delay and possibly prevent an operator, or the regulator, from taking appropriate actions and hence increase the risk of a disruption to its critical services or a disorderly wind-down of the FMI. In the case that an FMI is being wound down or resolved, the legal basis should support decisions or actions concerning termination, close out netting, the transfer of cash and securities positions of an FMI, or the transfer of all or parts of the rights and obligations provided in a link arrangement to a new entity.

Conflict-of-laws issues

1.13 Legal risk due to conflict of laws may arise if an operator or FMI is, or reasonably may become, subject to the laws of various other jurisdictions (for example, when an operator accepts participants established in those jurisdictions, when assets are held in multiple jurisdictions, or when business is conducted in multiple jurisdictions). In such cases, an operator should identify and analyse potential conflict-of-laws issues and develop rules to mitigate this risk. For example, the rules governing the FMI's activities should clearly indicate the law that is intended to apply to each aspect of an FMI's operations. An operator and its participants should be aware of applicable constraints on their abilities to choose the law that will govern the FMI's activities when there is a difference in the substantive laws of the relevant jurisdictions. For example, such constraints may exist because of jurisdictions' differing laws on insolvency and irrevocability. A jurisdiction ordinarily does not permit contractual choices of law that would circumvent that jurisdiction's fundamental public policy. Thus, when uncertainty exists regarding the enforceability of an operator's choice of law in relevant jurisdictions, an operator should obtain reasoned and independent legal opinions (referred to above in paragraph 1.3) in order to address properly such uncertainty.

Mitigating legal risk

1.14 In general, there is no substitute for a sound legal basis and full legal certainty in the operation of an FMI. In some practical situations, however, full legal certainty may not be achievable. In this case, an operator 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 and if legally enforceable, participant requirements, exposure limits, collateral requirements, and prefunded default arrangements. The use of such tools may limit an FMI's exposure if its activities are found to be not enforceable under New Zealand law or the laws and regulations of other relevant jurisdictions. If such controls are insufficient or not legally viable, an FMI could apply activity limits and, in extreme circumstances, restrict access or not perform the problematic activity until the legal situation is addressed.

STANDARD 2: GOVERNANCE

2.1 Governance is the set of relationships between an FMI's operator(s), owners, board of directors, management, and other relevant parties, including participants, indirect participants, regulators, and other stakeholders (such as participants' customers, other interdependent FMIs, and other market participants). Governance (i.e., organisational management and structure) provides the mechanism 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 an operator's board and management to pursue objectives that are in the interest of the FMI's stakeholders and that support relevant public interest considerations.

2.2 The Act defines directors as including a person occupying the position of director of the body, by whatever name called. If there are no directors, a trustee, manager, or other person who acts, in relation to the body, in the same way as, or in a way that is similar to the way in which a director would act if the body were a company incorporated under the Companies Act 1993. This means that governance arrangements that apply to a 'board of directors' or 'directors' under Standard 2: 'Governance', may apply to the management or executive groups of organisations that are not incorporated, or do not have formally appointed directors.

Multiple operators

2.3 Where an FMI has multiple operators, the FMI Standards will apply to each operator that is specified in the FMI's designation notice. However, the regulator will be satisfied that an operator has discharged its obligations in relation to the FMI it operates so long as that operator has ensured that another operator of the same FMI has acted to discharge such obligation (that is, generally only one operator will be required to satisfy the obligations in the standards). We note however that should the obligation not be discharged by any of the operators of the FMI, all operators remain liable for failing to meet the requirements.

2.4 The exclusion to the above approach is when applying the requirements in clauses 2(c), 2(d), and 2(e) of Standard 2: 'Governance'. We expect every operator to comply on an individual basis with the requirements in these clauses, as they relate to the structure and functioning of the operator's board of directors.

FMI objectives

2.5 Given the importance of FMIs and the fact that the decisions of operators can have widespread impact, affecting multiple financial institutions, markets, and jurisdictions, it is essential for each operator to place a high priority on the safety and efficiency of the operations of the FMI and explicitly support financial stability and other relevant public interests (including the purposes set out in section 3 of the Act). For example, in certain over-the-counter derivatives markets, industry standards and market protocols have been developed to increase certainty, transparency, and stability in the market. If a CCP 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. An operator must ensure that its governance arrangements for the FMI also include appropriate consideration of the interests of the FMI's participants, participants' customers, the regulator, and

other stakeholders. For all classes of FMIs, governance arrangements must provide for fair and open access (see Standard 18: 'Access and participation requirements') and for effective implementation of recovery or wind-down plans, or resolution.

Governance arrangements

2.6 Governance arrangements, which define the structure under which the board and management operate, must be clearly and thoroughly documented. These arrangements should include certain key components such as the:

a) role and composition of the board and any board committees (or equivalent bodies); and

b) senior management structure; and

c) reporting lines between management and the board (or equivalent body); and

d) ownership structure; and

e) structure of the corporate group (if an operator is part of a broader corporate group); and

f) internal governance policy; and

g) design of risk management and internal systems (including controls); and

h) procedures for the appointment of members of the board (or equivalent body) and senior management; and

i) processes for ensuring performance accountability.

2.7 Governance arrangements must provide clear and direct lines of responsibility and accountability, particularly between management and the board (including any board committees), and ensure sufficient independence from management for key functions such as risk management, internal control, and audit. These arrangements must be disclosed to owners, the regulator, participants, and, in summary form (i.e., via an internal governance structure diagram or by other means), to the public. An operator should ensure that information provided to its owners, the regulator and participants includes enough detail to allow its owners, the regulator, and participants to form their own view of the sufficiency of the governance arrangements. Governance arrangements disclosed to the public in summary form should be easily accessible on an operator or FMI's website as appropriate.

2.8 No single set of governance arrangements is necessarily appropriate for all FMIs, and their operators in relevant jurisdictions. Arrangements may differ significantly because of ownership structure or organisational form. While specific arrangements vary, this standard is intended to be generally applicable to all ownership and organisational structures.

2.9 Depending on its ownership structure and organisational form, an operator may need to focus particular attention on certain aspects of its and the FMI's governance arrangements. An operator that is part of a larger organisation, for example, should place particular emphasis on the clarity of its governance arrangements, including in relation to any conflicts of interests and outsourcing issues that may arise because

of the parent or other affiliated organisation's structure. Governance arrangements should also be adequate to ensure that decisions of affiliated organisations (including members of any corporate group the operator is a part of) are not detrimental to the FMI and do not conflict with the operator's legal obligations. An operator that is, or is part of, a for-profit entity may need to place particular emphasis on managing any conflicts between income generation and the soundness of the FMI's operation. Where relevant, cross-border issues should be appropriately identified, assessed, and dealt with in the governance arrangements, in respect of the FMI, the operator, and the operator's parent entity.

2.10 An operator may also need to focus particular attention on certain aspects of the risk management arrangements for it and the FMI, as a result of the ownership structure or organisational form. If an FMI provides services that present a distinct risk profile from, and potentially pose significant additional risks to, its payment, clearing or settlement function, an operator needs to manage those additional risks adequately. This may include separating the additional services that the FMI provides from its payment, clearing or settlement function, legally, or taking equivalent action. The ownership structure and organisational form may also need to be considered in the preparation and implementation of the recovery or wind-down plans for the FMI or in assessments of the FMI's resolvability.

2.11 In relation to central bank operated FMIs, and in particular the possible or perceived conflicts of interest relating to RBNZ operated FMIs (where the RBNZ is both the operator and the regulator) refer to the Memorandum of Understanding between the FMA and the RBNZ, and RBNZ's Statement of Prudential Policy, which refers to the RBNZ's policies in this respect. See also 2.22 for further information on RBNZ-operated FMIs and the application of the standard.

Roles, responsibilities, and composition of the board of directors

2.12 An operator's board has multiple roles and responsibilities that must be clearly specified. These roles and responsibilities should include:

a) establishing clear strategic aims for the FMI; and

b) ensuring effective monitoring of senior management (including selecting its senior managers, setting their objectives, evaluating their performance, and, where appropriate, removing them); and

c) establishing appropriate remuneration policies (which should be consistent with best practices and based on long-term achievements, in particular, the safety and efficiency of the FMI); and

d) establishing and overseeing the risk management function and material risk decisions; and

e) overseeing internal control functions (including ensuring independence and adequate resources); and

f) ensuring compliance with all supervisory and oversight requirements; and

g) ensuring consideration of financial stability and other relevant public interests; and

h) providing accountability to the owners, participants, and other relevant stakeholders.

2.13 Policies and procedures related to the functioning of the board of directors must be clear and well documented. These policies include the responsibilities and functioning of board committees. A board of directors would normally be expected to have, among others: a risk committee, an audit committee, and a remuneration committee, or equivalents. The regulator expects these committees to have clearly assigned responsibilities and procedures. Board policies and procedures must include processes to identify, address, and manage potential conflicts of interest of board members. Conflicts of interest include, for example, circumstances in which a director has material competing business interests with the FMI. Further, policies and procedures should also include regular reviews of the board of directors' performance and the performance of each individual director, as well as periodic independent assessments of performance, at least on an annual basis.

2.14 Governance policies related to board composition, appointment, and term must also be clear and documented. The board must be composed of suitable directors with an appropriate mix of skills (including strategic and relevant technical skills), experience, and knowledge of the entity (including an understanding of the FMI's interconnectedness with other parts of the financial system). Members of the board 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. Independence from the views of management typically requires the inclusion of non-executive board members, including independent board members, as appropriate. Definitions of an independent board member vary, but 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 an operator should be specified and publicly disclosed, and should exclude parties with significant business relationships with the FMI, cross-directorships, or controlling shareholdings, as well as employees of the organisation. Further, an operator should publicly disclose which board members it regards as independent. An FMI may also need to consider setting a limit on the duration of board members' terms.

Roles and responsibilities of management

2.15 An operator must have clear and direct reporting lines between FMI management and the board in order to promote accountability, and the roles and responsibilities of management should be clearly specified. An operator must ensure an FMI's management has the appropriate experience, a mix of skills, and the integrity necessary to discharge their responsibilities for the operation and risk management of the FMI. Under the direction of the board of directors, management should ensure that the FMI's activities are consistent with the objectives, strategy, and risk tolerance of the FMI, as determined by the board of directors. Management should ensure that internal systems (including controls) and related procedures are appropriately designed and executed in order to promote the FMI's objectives, and that these procedures include a sufficient level of management oversight. Internal systems and related procedures should be subject to regular review and testing by well-trained and staffed risk management and internal audit functions. Additionally,

we would expect that senior management would be actively involved in the risk-control process and ensure that significant resources are devoted to the risk management framework.

Risk management governance

2.16 The board of directors of an operator is ultimately responsible for managing an FMI's risks, and an operator should ensure the board establishes a clear, documented risk management framework that includes the FMI's risk-tolerance policy, assigns responsibilities and accountability for risk decisions, and addresses decision making in crises and emergencies. The operator should ensure the board regularly monitors the FMI's risk profile to ensure that it is consistent with the business strategy and risk-tolerance policy for the FMI. In addition, the operator should ensure the FMI has an effective internal systems and oversight, including adequate governance and project management processes, over the models used to quantify, aggregate, and manage the FMI's risks. Senior executive/board of director (the highest level of decision making within the organisation) approval should be required for material decisions that would have a significant impact on the risk profile of the FMI, 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 the over-the-counter derivatives markets, an operator of a CCP is expected to act consistently with practices or arrangements that have become established market conventions (unless an operator of the CCP has reasonable grounds not to do so and that does not conflict with the market's wider interest). In this regard, where a CCP supports a market and is expected to fully adhere to market wide protocols and related decisions, an operator of the CCP should be involved in the development and establishment of such standards. It is critical that governance processes for the market fully reflect the role of the CCP in the market. The arrangements adopted by an operator of a CCP should also be transparent to its participants and regulators.

2.17 An operator should ensure that its board of directors and governance arrangements support the use of clear and comprehensive rules and key procedures, including detailed and effective participant default rules and procedures (see Standard 13: 'Participant default rules'). The operator should have procedures in place to support its capacity to act appropriately and immediately if any risks arise that threaten the FMI'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 FMI.

2.18 The governance of the risk management function is particularly important. It is essential that an operator's risk management personnel for the FMI have sufficient independence, authority, resources, and access to the board to ensure that the operations of the FMI 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 FMI, 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 of directors discharge its risk-related responsibilities, an operator should consider the case for a risk committee responsible for advising the board on the FMI's overall current and future risk tolerance and strategy. A CCP,

however, should have such a risk committee or its equivalent. An operator's risk committee should be chaired by a sufficiently senior and knowledgeable individual who is independent of an operator's executive management and be composed of a majority of members who are non-executive members, and appropriately senior. The committee should have a clear and public mandate and operating procedures and, where appropriate, have access to external expert advice.

Model validation

2.19 An operator 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. An operator of an FMI should validate, on an ongoing basis, the models and their methodologies used to quantify, aggregate, and manage the FMI's risks. The validation process should be independent of the development, implementation, and operation of the models and their methodologies, and the validation process should be subjected to an independent review of its adequacy and effectiveness. Validation should include:

a) an evaluation of the conceptual soundness of (including developmental evidence supporting) the models; and

b) an ongoing monitoring process that includes verification of processes and benchmarking; and

c) an analysis of outcomes that includes back testing.

Internal controls and audit

2.20 The board of an operator is responsible for establishing and overseeing internal systems (including controls) and audit. An operator should have sound internal control policies and procedures for the FMI to help manage its risks. For example, as part of a variety of risk controls, the board should ensure that there are adequate internal controls to protect against the misuse of confidential information. An operator 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 an operator's risk management and control processes for the FMI (see also Standard 3: 'Framework for the comprehensive management of risks'). The board of directors will typically establish an audit committee (or equivalent) to oversee the internal audit function. In addition to reporting to senior management, the audit function should have regular access to the board through an additional reporting line.

Stakeholder input

2.21 In making major decisions, an operator must consider all relevant stakeholders' interests, (which includes its direct and indirect participants), including those decisions that relate to the FMI's design, rules, and overall business strategy. In particular, an operator of an FMI with cross-border operations should ensure that the full range of views across the relevant jurisdictions in which the FMI operates is appropriately considered in any decision-making process. Mechanisms for involving stakeholders in the operator's decision-making process may include stakeholder representation on the board of directors (if any) (including direct and indirect

participants), user committees, and public consultation processes. As opinions among interested parties are likely to differ, an operator should have clear processes for identifying and appropriately managing the diversity of stakeholder views and any conflicts of interest between stakeholders and the operator or FMI. Without prejudice to local requirements on confidentiality and disclosure, an operator must clearly and promptly inform the FMI's owners, participants (direct or indirect), 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.

Application of the standard where the operator is the RBNZ

2.22 Governance arrangements for the RBNZ are set out in the RBNZ Act. Where the operator is the RBNZ, the requirements in Standard 2: 'Governance' should be read in line with the governance requirements in subpart 4 of Part 3 of the RBNZ Act, which includes provisions relating to the RBNZ Board, its members and the role of the Governor.

STANDARD 3: FRAMEWORK FOR THE COMPREHENSIVE MANAGEMENT OF RISKS

3.1 An operator of an FMI must take an integrated and comprehensive view of the FMI's risks, including the risks the FMI 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, settlement banks, liquidity providers, and service providers (for example, matching and portfolio compression service providers). An operator of an FMI should consider how various risks relate to, and interact with, each other. An operator must have a sound risk management framework (including policies, procedures, and internal systems) that enable it to effectively identify, measure, monitor, and manage the range of risks that arise in or are borne by the FMI. An FMI's risk management framework should include the identification and management of interdependencies between the FMI and other FMIs or entities. An operator of an FMI must also provide appropriate incentives and the relevant information for the FMI's participants and other entities to manage and contain their risks vis-à-vis the FMI (for example, this might include appropriate mechanisms for allocating FMI related losses suffered by the operator to the FMI's participants). As discussed in Standard 2: 'Governance', the board of directors of the operator plays a critical role in establishing and maintaining a sound risk management framework.

Identification of risks

3.2 To establish a sound risk management framework, an operator should first identify the range of risks that arise within the FMI 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 the FMI's ability to perform or to provide services as expected. Typically, these would include legal, credit, liquidity, and operational risks. An operator 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 FMI and may undermine an FMI's financial soundness as well as the stability of the broader financial markets. In identifying risks, an operator must take a broad perspective and identify the risks that the FMI bears from other entities, such as other FMIs, settlement banks, liquidity providers, service providers, direct and indirect participants, and any entities that could be materially affected by the FMI's inability to provide services. For example, the relationship between an SSS and an HVPS to achieve DvP settlement can create system-based interdependencies.

Comprehensive risk policies, procedures, and internal systems

3.3 An operator's board of directors and senior management are ultimately responsible for managing the FMI's risks (see Standard 2: 'Governance'). An operator should ensure its board of directors determines an appropriate level of aggregate risk tolerance and capacity for the FMI. An operator's board of directors and senior management should establish policies, procedures, and internal systems that are consistent with the FMI's risk tolerance and capacity. An operator's policies, procedures, and internal systems serve as the basis for identifying, measuring, monitoring, and managing the FMI's risks and should cover routine and non-routine

events, including the potential inability of a participant, or the FMI itself, to meet its obligations. An operator's policies, procedures, and internal systems should address all relevant risks, including legal, credit, liquidity, general business, and operational risks. These policies, procedures, and internal systems must be part of a coherent and consistent framework that is reviewed and updated periodically and should be shared with the regulator on request (under section 14 of the Act).

Information and control systems

3.4 In addition, an operator should employ robust information and risk-control systems across the FMI to provide the operator with the capacity to obtain timely information necessary to apply risk management policies, procedures, and internal systems. In particular, these systems should allow for the accurate and timely measurement and aggregation of risk exposures across the FMI, 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 FMI. Information systems should also enable an operator to monitor the FMI's credit and liquidity exposures, overall credit and liquidity limits, and the relationship between these exposures and limits.

3.5 An operator may consider it beneficial to provide the FMI's 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. For example, where an operator permits participants' customers to create exposures in the FMI that are borne by the participants, an operator should provide participants with the capacity to limit such risks.

Incentives to manage risks

3.6 In establishing risk management policies, procedures, and systems, an operator must provide incentives to the FMI's participants and, where relevant, their customers, to manage and contain the risks they pose to the FMI. There are several ways in which an operator may provide incentives. For example, an operator could take steps which make using the FMI more costly or less efficient for participants that fail to settle securities in a timely manner or to repay intraday credit by the end of the operating day. Another example is the use of loss-sharing arrangements proportionate to the exposures brought to the FMI. Such approaches 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.

Interdependencies

3.7 An operator of an FMI should regularly review the material risks the FMI bears from and poses to other entities (such as other FMIs, settlement banks, liquidity providers, or service providers) as a result of interdependencies and develop appropriate risk management tools to address these risks (see also Standard 20: 'FMI links'). In particular, an operator must have effective risk management tools to manage all relevant risks, including the legal, credit, liquidity, general business, and operational risks that the FMI 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 contingency plans that

allow for rapid recovery and resumption of critical operations and services in the event of operational disruptions (see Standard 17A: 'Contingency plans'), liquidity risk management techniques (see Standard 7: 'Liquidity risk'), and recovery or orderly wind-down plans should the FMI become non-viable (see Standard 17A: 'Contingency plans'). Due to the interdependencies between and among systems, an operator should ensure that its crisis management arrangements for the FMI allow for effective coordination among the affected entities, including cases in which the FMI's viability or the viability of an interdependent entity is in question.

Internal systems

3.8 An operator of an FMI also should have comprehensive internal processes to help the board and senior management monitor and assess the adequacy and effectiveness of the risk management policies, procedures, controls, and internal systems for the FMI. 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 programmes and independent audits. A robust internal audit function can provide an independent assessment of the effectiveness of risk management and internal systems. An emphasis on the adequacy of internal systems by senior management and the board of directors 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, operators that involve their internal audit function in pre-implementation reviews will often reduce their need to expend additional resources to retrofit processes and internal systems with critical controls that had been overlooked during initial design phases and construction efforts.

STANDARD 4: CREDIT RISK

4.1 Credit risk is broadly defined as the risk that a counterparty will be unable to fully meet 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 disruptions to an FMI, its other direct or indirect participants, and the financial markets more broadly. Therefore, an operator should measure, monitor, and manage credit exposures to the FMI's participants and the credit risks arising from payment, clearing, and settlement processes (see also Standard 3: 'Framework for the comprehensive management of risks', Standard 9: 'Money settlements', and Standard 16: 'Custody and investment risks'). Credit exposure may arise in the form of current exposures, potential future exposures, or both. Current exposure, in this context, is defined as the loss that an operator (or in some cases, an FMI's participants) would face immediately if a participant were to default. Potential future exposure is broadly defined as any potential credit exposure to participants that an operator could face at a future point in time. Note that, where the operator is a central bank, the requirements in Standard 4 should not be read as constraining the central bank's ability to act (either as operator, or in another capacity) to promote financial stability. For example, it should not be read as constraining a central bank's ability to act when it is acting as a lender of last resort.

Use of financial resources

4.2 The rules of an FMI should expressly set out the "waterfall", which is a sequence of prefunded financial resources, 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 operator's own funds, and other participants' contributions to a prefunded default arrangement. The rules should include the circumstances in which specific resources of the FMI can be used in a participant default (see Standard 13: 'Participant-default rules and procedures' and Standard 23: 'Disclosure of rules, key procedures, and market data'). For the purposes of this standard, an operator should not include as "available" resources 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 other activities in which the FMI is engaged (see Standard: 15 'General business risk'). In addition, if an FMI 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 be legally enforceable in both markets, be clear to all participants, and avoid significant levels of contagion risk between markets and participants. The design of an FMI'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.

4.3 Refer to Standard 17A: 'Contingency Plans' and corresponding guidance material for contingency planning for uncovered credit losses.

Credit risk in payment systems

4.4 *Sources of credit risk.* A payment system (or pure payment system) may face credit risk from its participants, its payment and settlement processes, or both. This credit risk is driven mainly by current exposures from extending intraday credit to

participants. For example, a central bank that operates a payment system and provides intraday credit will face current exposures. A payment system can avoid carrying over current exposures to the next day by requiring its participants to refund any credit extensions before the end of the day. Intraday credit can lead to potential future exposures even when the FMI accepts collateral to secure the credit. A payment system would face potential future exposure if the value of collateral posted by a participant to cover intraday credit were to fall below the amount of credit extended to the participant by the FMI, leaving a residual exposure.

4.5 *Sources of credit risk in DNS systems.* A payment system that employs a DNS mechanism may face financial exposures arising from its relationship with its participants or its payment and settlement processes. An operator of a DNS payment system may explicitly guarantee settlement, whether the guarantee is provided by an operator, or its participants. In such systems, the guarantor of the arrangement would face current exposure if a participant were not to meet its payment or settlement obligations. Even in a DNS system that does not have an explicit guarantee, participants in the payment system may still face settlement risk vis-à-vis each other. Whether this risk involves credit exposures or liquidity exposures, or a combination of both, will depend on the type and scope of obligations, including any contingent obligations, the participants bear. The type of obligations will, in turn, depend on factors such as the payment system's design, rules, and legal framework.

4.6 *Measuring and monitoring credit risk*. An operator of a pure payment system or payment system should frequently and regularly measure and monitor its credit risks, throughout the day using timely information. An operator of a payment system should ensure it has access to adequate information, such as appropriate collateral valuations, to allow it to measure and monitor its current exposures and degree of collateral coverage. In a DNS payment system without a settlement guarantee, an operator must provide the capacity to its participants to measure and monitor their current exposures to each other in the system or adopt rules that require participants to provide relevant exposure information. Current exposure is relatively straightforward to measure and monitor; however, potential future exposure may require modelling or estimation. To monitor risks associated with current exposure, an operator of a payment system should monitor market conditions for developments that could affect these risks, such as collateral values. To estimate the FMI's potential future exposure and associated risk, an operator of a payment system should model possible changes in collateral values and market conditions over an appropriate liquidation period. An operator, where appropriate, needs to monitor the existence of large exposures to the payment system's participants and their customers. Additionally, an operator should monitor any changes in the creditworthiness of its participants.

4.7 *Mitigating and managing credit risk*. An operator should mitigate the payment system's credit risks to the extent it is possible to do so. An operator of a payment system can, for example, eliminate some of its or its participants' credit risks associated with the settlement process by employing a Real Time Gross Settlement (RTGS) mechanism. In addition, an operator should limit the payment system's current exposures by limiting intraday credit extensions and avoid carrying over these exposures to the next day by requiring participants to refund any credit extensions before the end of the day. Such limits should balance the usefulness of credit to facilitate settlement within the system against the payment system's credit exposures.

4.8 To manage the risk from a participant default, an operator of a payment system should consider the impact of participant defaults and robust techniques for managing collateral. An operator of a payment system must ensure the FMI covers its current and, where they exist, potential future exposures to each participant fully with a high degree of confidence using collateral and other equivalent financial resources as appropriate (equity can be used after deduction of the amount dedicated to cover general business risk) (see Standard 5: 'Collateral' and Standard 15: 'General business risk'). By requiring collateral to cover the credit exposures, an operator of a payment system mitigates, and in some cases eliminates, its current exposure and may provide participants with an incentive to manage credit risks they pose to the payment system or other participants. Further, this collateralisation reduces the need in a DNS payment system to unwind payments should a participant default on its obligations. However, collateral or other equivalent financial resources can fluctuate in value, so the payment system should establish prudent haircuts to mitigate the resulting potential future exposure.

4.9 An operator of a DNS payment system that explicitly guarantees settlement, whether the guarantee is from the operator itself or from its participants, must ensure the FMI maintains sufficient financial resources to cover fully all current and potential future exposures using collateral and other equivalent financial resources. An operator of a DNS payment system in which there is no settlement guarantee, but where its participants face credit exposures arising from its payment and settlement processes, must ensure the FMI maintains, at a minimum, sufficient resources to cover the exposures of the two participants and their affiliates that would create the largest aggregate credit exposure in the system. A higher level of coverage should be considered for a payment system that creates large exposures or that could have a significant systemic impact if more than two participants and their affiliates were to default.

Credit risk in SSS systems

4.10 *Sources of credit risk.* An SSS may face a number of credit risks from its participants or its settlement processes. An SSS faces counterparty credit risk when it extends intraday or overnight credit to participants. This extension of credit creates current exposures and can lead to potential future exposures, even when the SSS accepts collateral to secure the credit. An SSS would face potential future exposure if the value of collateral posted by a participant to cover this credit might fall below the amount of credit extended to the participant by the SSS, leaving a residual exposure. In addition, an SSS that explicitly guarantees settlement would face current exposures if a participant were not to fund its net debit position or meet its obligations to deliver financial instruments. Further, if an SSS does not use a DvP settlement mechanism, an operator of the SSS or its participants face principal risk, which, in the context of an SSS, is the risk of loss of securities or payments made to the defaulting participant prior to the detection of the default.

4.11 *Sources of credit risk in DNS systems.* An SSS may settle securities on a gross basis and funds on a net basis (DvP model 2) or settle both securities and funds on a net basis (DvP model 3). Further, an operator of an SSS that uses a DvP model 2 or 3 settlement mechanism may explicitly guarantee settlement, whether the guarantee is by the FMI itself or by its participants. In such systems, this guarantee represents an extension of intraday credit from the guarantor. In an SSS that does not provide an explicit settlement guarantee, participants may face settlement risk vis-à-vis each other if a participant defaults on its obligations. Whether this

settlement risk involves credit exposures, liquidity exposures, or a combination of both will depend on the type and scope of the obligations, including any contingent obligations, the participants bear. The type of obligations will depend on factors such as the SSS's design, rules, and legal framework.

4.12 *Measuring and monitoring credit risk*. An operator of an SSS should frequently and regularly measure and monitor the credit risks of the SSS throughout the day using timely information. An operator of an SSS should ensure it has access to adequate information, such as appropriate collateral valuations, to allow it to measure and monitor the current exposures and degree of collateral coverage. If credit risk exists between participants, an operator of the SSS must provide the capacity to participants to measure and monitor their current exposures to each other in the FMI system or adopt rules that require participants to provide relevant exposure information. Current exposure should be relatively straightforward to measure and monitor; however, potential future exposure may require modelling or estimation. To monitor the risks associated with current exposure, an operator of an SSS should monitor market conditions for developments that could affect these risks, such as collateral values. To estimate its potential future exposure and associated risk, an operator of an SSS should model possible changes in collateral values and market conditions over an appropriate liquidation period. An operator of an SSS, where appropriate, needs to monitor the existence of large exposures to its participants and their customers. Additionally, it should monitor any changes in the creditworthiness of its participants.

4.13 *Mitigating and managing credit risk*. An operator of an SSS should mitigate credit risks to the extent it is possible to do so. An operator of an SSS should, for example, eliminate its or its participants' principal risk associated with the settlement process by employing an exchange-of-value settlement system (see Standard 12: 'Exchange-of-value settlement systems'). The use of a system that settles securities and funds on a gross, obligation-by-obligation basis (DvP model 1) would further reduce credit and liquidity exposures among participants, and between participants and the SSS. In addition, an operator should limit the SSS's current exposures by limiting intraday and overnight (where relevant) credit extensions. Such limits should balance the usefulness of credit to facilitate settlement within the system against the SSS's credit exposures.

4.14 To manage the risk from a participant default, an operator of an SSS should consider the impact of participant defaults and use robust techniques for managing collateral. An operator of an SSS must cover its current and, where they exist, potential future exposures to each participant fully with a high degree of confidence using collateral and other equivalent financial resources (equity can be used after deduction of the amount dedicated to cover general business risk) (see Standard 5: 'Collateral' and Standard 15: 'General business risk'). By requiring collateral to cover the credit exposures, an operator of an SSS mitigates, and in some cases eliminates, its current exposures and may provide participants with an incentive to manage the credit risks they pose to the SSS or other participants. Further, this collateralisation allows an operator of an SSS that employs a DvP model 2 or 3 mechanism to avoid unwinding transactions or to mitigate the effect of an unwind should a participant default on its obligations. However, collateral and other equivalent financial resources can fluctuate in value, so an operator of the SSS needs to establish prudent haircuts to mitigate the resulting potential future exposures.

4.15 An operator of an SSS that uses a DvP model 2 or 3 mechanism and explicitly guarantees settlement, whether the guarantee is from an operator itself or from its participants, should maintain sufficient financial resources to cover fully, with a high degree of confidence, all current and potential future exposures using collateral and other equivalent financial resources. An operator of an SSS that uses a DvP model 2 or 3 mechanism and does not explicitly guarantee settlement, but where its participants face credit exposures arising from its payment, clearing, and settlement processes, should maintain, at a minimum, sufficient resources to cover the exposures of the two participants and their affiliates that would create the largest aggregate credit exposure in the system. A higher level of coverage should be considered for an SSS that has large exposures or that could have a significant systemic impact if more than two participants and their affiliates were to default.

Credit risk in CCP

4.16 *Sources of credit risk.* A CCP 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 CCP and its participants. 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 CCP following an event of default. For example, during the period in which a CCP 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 CCP's credit exposure, potentially significantly. A CCP can also face potential future exposure due to the possibility of collateral (initial margin) declining significantly in value over the close out period.

4.17 *Measuring and monitoring credit risk.* An operator of a CCP should frequently and regularly measure and monitor its credit risks throughout the day using timely information. An operator of a CCP should ensure that it has access to adequate information to allow it to measure and monitor its current and potential future exposures. 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, an operator of a CCP should identify risk factors and monitor prospective market developments and conditions that could affect the size and likelihood of its losses in the close out of a defaulting participant's positions. An operator of a CCP must monitor the existence of large exposures to the CCP's participants and, where appropriate, their customers. Additionally, an operator should monitor any changes in the creditworthiness of the CCP's participants.

4.18 *Mitigating and managing credit risk*. An operator of a CCP should mitigate its credit risk to the extent it is possible to do so. For example, to control the build-up of current exposures, a CCP 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, an operator of a CCP should have the authority and operational capacity to make intraday margin calls, both scheduled and unscheduled, from participants. Further, an operator of a CCP may choose to place

limits on credit exposures in some cases, even if collateralised. Limits on concentrations of positions or additional collateral requirements may also be warranted.

4.19 A CCP 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 CCP's own funds, and other participants' contributions to a prefunded default arrangement. Initial margin is used to cover a CCP'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 CCP generally remains exposed to residual risk (or tail risk) if a participant defaults and market conditions concurrently change more drastically than is anticipated in the margin calculations. In such scenarios, a CCP'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, an operator of a CCP should maintain additional financial resources, such as additional collateral or a prefunded default arrangement, to cover a portion of the tail risk.

4.20 An operator of a CCP must ensure it covers 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 Standard 6: 'Margin', a CCP should establish initial margin requirements that are commensurate with the risks of each product and portfolio. Initial margin should meet an established single-tailed confidence level of at least 99 percent of the estimated distribution of future exposure. For a CCP that calculates margin at the portfolio level, this standard applies to the distribution of future exposure of each portfolio. For a CCP that calculates margin at more-granular levels, such as at the sub-portfolio level or product level, the standard must be met for the corresponding distributions of future exposure.

4.21 In addition to fully covering its current and potential future exposures, an operator of a CCP must maintain additional financial resources sufficient to cover a wide range of potential stress scenarios involving extreme but reasonably foreseeable market conditions. Specifically, an operator of a CCP, must maintain additional financial resources sufficient to cover a wide range of potential stress scenarios that should include but not be limited to:

a) where the operator is an operator of an FMI engaging in simple CCP activities, and the FMI is not systemically important in multiple jurisdictions, the default of the participant and its affiliates that would potentially cause the largest aggregate credit exposure in extreme but plausible market conditions; and

b) where the operator is an operator of an FMI engaging in complex CCP activities, and the FMI is systemically important in multiple jurisdictions (including in New Zealand), the default of the two participants and their affiliates that would potentially cause the largest aggregate credit exposure in extreme but plausible market conditions.

Note that an FMI would be considered systemically important in multiple jurisdictions where the FMI is designated as systemically important in New Zealand, and where it is assessed by an overseas regulator as so important to the market in that jurisdiction that it is subject to additional regulation or requirements. For example, where the FMI is subject to a regime that applies to

prominent, significant, or systemically important FMIs in that jurisdiction.

Testing the sufficiency of a CCP's total financial resources

4.22 An operator of a CCP should determine the amount and regularly test the sufficiency of an operator's total financial resources for the FMI through stress testing. An operator of a CCP should also conduct reverse stress tests, as appropriate, to test how severe stress conditions would be covered by an operator's total financial resources in relation to the FMI. As initial margin is a key component of a CCP's total financial resources, a CCP should also test the adequacy of its initial margin requirements and model through back-testing and sensitivity analysis, respectively (see Standard 6: 'Margin' for further discussion on testing of the initial margin requirements and model).

4.23 *Stress testing*. An operator of a CCP should determine the amount and regularly test the sufficiency of the FMI's total financial resources available in the event of a default or multiple defaults in extreme but reasonably foreseeable market conditions through rigorous stress testing. An operator of a CCP should have clear procedures to report the results of its stress tests to appropriate decision makers and to use these results to evaluate the adequacy of and adjust its total financial resources. Stress tests should be performed daily using standard and predetermined parameters and assumptions. On a monthly basis, an operator of a CCP 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 FMI's required level of default protection in light of current and evolving market conditions. An operator of a CCP should perform this analysis of stress testing more than once a month when the products cleared or markets served display high volatility, become less liquid, or when the size or concentration of positions held by an FMI's participants increases significantly. A full validation of a CCP's risk management model should be performed at least annually by an operator.

4.24 In conducting stress testing, an operator of a CCP should consider 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 reasonably foreseeable market conditions. Extreme but reasonably foreseeable conditions should not be considered a fixed set of conditions, but rather, conditions that evolve. Stress tests should quickly incorporate emerging risks and changes in market assumptions (for example, departures from usual patterns of co-movements in prices among the products a CCP clears). An operator of a CCP proposing to clear new products should consider movements in prices of any relevant related products.

4.25 *Reverse stress tests.* An operator of a CCP should 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 an operator of a CCP to model hypothetical positions and extreme market conditions that may go beyond what are considered extreme but reasonably foreseeable market conditions in order to help understand margin calculations and the sufficiency of financial resources given the underlying

assumptions modelled. Modelling extreme market conditions can help an operator of a CCP determine the limits of its current model and resources, but requires an operator of the CCP to exercise judgment when modelling different markets and products. An operator of a CCP should develop hypothetical 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 an operator of the CCP's determination of the appropriate level of financial resources.

STANDARD 5: COLLATERAL

5.1 Collateralising credit exposures protects an operator (see Standard 4: 'Credit risk'). An operator 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 reasonably foreseeable market conditions. Additionally, an operator should have the capacity to use the collateral promptly when needed. Note that, where an operator is a central bank, the requirements in Standard 5: 'Collateral' (e.g., what it accepts as eligible collateral) should not read as constraining a central bank's ability to act (either as operator of an FMI or in another capacity) to promote financial stability. For example, when it is acting as a lender of last resort.

Acceptable collateral

5.2 An operator must ensure the FMI only accepts collateral with low credit, liquidity, and market risks. In the normal course of business, an operator may be exposed to risk from certain types of collateral that are not considered to have low credit, liquidity, and market risks. However, in some instances, these assets may be acceptable collateral for credit purposes if an appropriate haircut is applied. An operator of an FMI 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. An operator of an FMI that accepts collateral with credit, liquidity, and market risks above minimum levels should demonstrate that it sets and enforces appropriately conservative haircuts and concentration limits.[1]

5.3 Further, an operator should regularly adjust its requirements for acceptable collateral in accordance with changes in underlying risks. When evaluating types of collateral, an operator should consider potential delays in accessing the collateral due to the settlement conventions for transfers of the asset. In addition, it is recommended that participants not be allowed to post their own debt or equity securities, or debt or equity of companies closely linked to them, as collateral. More generally, an operator 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 defaults. An operator of the FMI should measure and monitor the correlation between a participant's creditworthiness and the collateral posted and take measures to mitigate the risks, for instance by setting more-conservative haircuts.

5.4 If an operator plans to use assets held as collateral to secure liquidity facilities in the event of a participant default, an operator will also need to consider, in determining acceptable collateral, what will be acceptable as security to lenders offering liquidity facilities (see Standard 7: 'Liquidity risk').

Valuing collateral

5.5 To have adequate assurance of the collateral's value in the event of liquidation, an operator must establish prudent valuation practices and develop haircuts that are

[1] Guarantees are not generally acceptable collateral. However, in the absence of reasonably available alternatives, a guarantee fully backed by collateral that is realisable on a same-day basis may serve as acceptable collateral.

regularly tested and take into account stressed market conditions. An operator of an FMI 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 an FMI 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, an operator should have the authority to exercise discretion in valuing assets according to predefined and transparent methods. An FMI's haircut procedures should be independently validated at least annually.[2]

Limiting procyclicality

5.6 An operator of an FMI must 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 low market stress and increase during periods of high market stress. For example, in a stressed market, an operator may require the posting of additional collateral both because of the decline of 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 FMI operators, but result in additional protection and potentially less-costly and less-disruptive adjustments in periods of high market stress.

Avoiding concentrations of collateral

5.7 An operator of an FMI must avoid concentrated holdings of certain assets for the FMI where this would significantly impair the ability to liquidate such assets quickly without significant adverse price effects. 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 an operator. Concentration charges penalise participants for maintaining holdings of certain assets beyond a specified threshold as established by an operator. 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 an operator to determine their adequacy.

[2] Validation of the FMI's haircut procedures should be performed by personnel of sufficient expertise who are independent of the personnel that created and applied the haircut procedures. These expert personnel could be drawn from within the FMI. However, a review by personnel external to the FMI may also be necessary at times.

Cross-border collateral

5.8 If an operator accepts cross-border collateral, an operator should identify and mitigate any additional risks associated with its use and ensure that it can be used in a timely manner. 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 and risks to FMIs that need to be evaluated and managed by the affected FMIs (see also Standard 17: 'Operational risk' and Standard 20: 'FMI links'). For example, an operator should ensure the FMI has 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. An operator of an FMI 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. An operator of the FMI should have the capacity to address potential operational challenges of operating across borders, such as differences in time zones or operating hours of foreign CSDs or custodians.

Collateral management systems

5.9 An operator should use a well-designed and operationally flexible collateral management system for the FMI. 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 an FMI to the collateral provided to it by its counterparties. An operator should ensure an FMI's collateral management system also has functionality to accommodate the timely deposit, withdrawal, substitution, and liquidation of collateral. An operator of an FMI 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 FMI'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.

Reuse of collateral

5.10 Reuse of collateral refers to an operator's subsequent reuse of collateral that has been provided by participants in the normal course of business. This differs from an operator's use of collateral in a default scenario during which the defaulter's collateral, which has become the property of the FMI, can be used to access liquidity facilities or can be liquidated to cover losses (see Standard 13: 'Participant-default rules and procedures'). An operator should ensure that the FMI's rules are clear and transparent regarding the reuse of collateral (see also Standard 23: 'Disclosure of rules, key procedures, and market data'). In particular, the rules should clearly specify when an operator may reuse its participant collateral and the process for returning that collateral to participants. In general, an operator of an FMI may invest any cash collateral received from participants on their behalf (see also Standard 16: 'Custody and investment risks').

STANDARD 6: MARGIN

6.1 An effective margining system is a key risk management tool for an operator of a CCP to manage the credit exposures posed by the CCP's participants' open positions (see also Standard 4: 'Credit risk'). An operator of a CCP should collect margin, which is a deposit of collateral in the form of money, securities, or other financial instruments to assure performance and to mitigate the FMI's credit exposures, for all products that it clears, if a participant were to default (see also Standard 5: 'Collateral'). Margin systems typically differentiate between initial margin and variation margin. 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.

Margin requirements

6.2 One of the most common risk management tools used by CCPs to limit their credit exposure is a requirement that each participant provide collateral to protect the CCP against a high percentile of the distribution of future exposure. In this Guidance, such requirements are described as margin requirements. Margining, however, is not the only risk management tool available to a CCP (see also Standard 4: 'Credit risk'). In the case of some CCPs for cash markets, the CCP may require each participant to provide collateral to cover credit exposures. They may call these requirements margin, or they may hold this collateral in a pool known as a clearing fund.

6.3 When setting margin requirements, an operator must ensure a CCP has a margin system that establishes margin levels commensurate with the risks and particular attributes of each product, portfolio, and the 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. 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 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, an operator of a CCP 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 the CCPs margin methodology. In a fails-to-deliver scenario, an operator of the CCP should continue to margin positions for which a participant fails to deliver the required security (or other relevant instrument) on the settlement date.

Price information

6.4 An operator of a CCP must have a reliable source of timely price data because such data is critical for a CCP's margin system to operate accurately and effectively. In most cases, an operator of a CCP should rely on market prices from continuous, transparent, and liquid markets. If an operator of a CCP acquires pricing data from third-party pricing services, the operator should continually evaluate the data's reliability and accuracy. An operator 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. An operator of a CCP should have its valuation models validated under a variety of market scenarios at least annually by a qualified and independent party to ensure that its model accurately produces appropriate prices, and where appropriate, an operator should adjust its calculation of initial margin to reflect any identified model risk. An operator of a CCP should address all pricing and market liquidity concerns on an ongoing basis to conduct daily measurement of its risks.

6.5 For some markets, such as OTC markets, prices may not be reliable because of the lack of a continuous liquid market. In contrast to an exchange-traded market, there may not be a steady stream of live transactions from which to determine current market prices. Although independent third-party sources would be preferable, in some cases, participants may be an appropriate source of price data, as long as there is 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 an operator of the CCP's ability to accurately and promptly measure its exposure. In cases where price data is not available or reliable, an operator of a CCP 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, to determine appropriate prices. When prices are estimated, the systems and models used for this purpose must be subject to annual validation and testing.

Initial margin methodology

6.6 In accordance with the standard, an operator of a CCP must adopt initial margin models and parameters that are risk-based and generate margin requirements that are sufficient to cover its potential future exposures to participants in the interval between the last margin collection and the close out of positions following a participant default. An operator must ensure that initial margin meets an established single-tailed confidence level of at least 99 percent with respect to the estimated distribution of future exposure. For a CCP that calculates margin at the portfolio level, this requirement applies to each portfolio's distribution of future exposure. For an operator that calculates margin at more-granular levels, such as at the sub-portfolio level or by product, the requirement must be met for the corresponding distributions of future exposure at a stage prior to margining among sub-portfolios or products. The method selected by an operator 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 CCP. The estimation may account for the CCP's ability to implement effectively the hedging of future exposure. An operator of the CCP should take into account correlations across product prices, market liquidity for close out or hedging, and the

potential for non-linear risk exposures posed by certain products, including jump-to-default risks. An operator of a CCP should have the authority and operational capacity to make intraday initial margin calls, both scheduled and unscheduled, to its participants.

6.7 *Close out period*. An operator of a CCP should select an appropriate close out period for each product that the CCP clears and document the close out periods and related analysis for each product type. An operator of a CCP 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 CCP's ability to effectively hedge 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. An operator of a CCP should also consider and address position concentrations, which can lengthen close out timeframes and add to price volatility during close outs.

6.8 *Sample period for historical data used in the margin model*. An operator of a CCP should select an appropriate sample period for the CCP's 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, an operator of a CCP may need to determine margin levels using a shorter historical period to reflect new or current volatility in the market more effectively. Conversely, an operator of a CCP may need to determine margin levels based on a longer historical period in order to reflect past volatility. An operator of a CCP should also consider simulated data projections that would capture reasonably foreseeable events outside of the historical data especially for new products without enough history to cover stressed market conditions.

6.9 *Specific wrong-way risk*. An operator of a CCP should identify and mitigate any credit exposure that may give rise to specific wrong-way risk. Specific wrong-way risk arises where an exposure to a participant is highly likely to increase when the creditworthiness of that participant is deteriorating. For example, participants in a CCP 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. An operator of a CCP 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.

6.10 *Limiting procyclicality.* An operator of a CCP should appropriately address procyclicality in the CCP's margin arrangements. 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, an operator of a CCP 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, an operator of a CCP should adopt forward-looking and relatively stable and conservative margin requirements that are specifically designed to limit the need for destabilising, procyclical changes. To support this objective, an operator of a CCP could consider increasing the size of its prefunded default arrangements to limit the need and likelihood of large or unexpected margin calls in times of market stress.

Variation margin

6.11 A CCP 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 CCP's exposures to its participants (although some markets may impose trading limits or position limits that reduce this risk). An operator of a CCP can ascertain its current exposure to each participant by marking each participant's outstanding positions to current market prices. To the extent permitted by the rules of the CCP and supported by law, an operator of the CCP 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 (however, margin may still be collateralised so long as the requirements in Standard 5: 'Collateral' and Standard 6: 'Margin' are met). The regular collection of variation margin prevents current exposures from accumulating and mitigates the potential future exposures a CCP might face. An operator of a CCP should also have the authority and operational capacity to make intraday variation margin calls and payments, both scheduled and unscheduled, to its participants. An operator of a CCP 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.

Portfolio margining

6.12 In calculating margin requirements, an operator of a CCP 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. An operator of a CCP should base such offsets on an economically meaningful methodology that reflects the degree of price dependence between the products. Price dependence is often modelled through correlations, but more complete or robust measures of dependence should be considered, particularly for non-linear products. In any case, an operator of the CCP should consider how price dependence can vary with overall market conditions, including in stressed market conditions. Following the application of offsets, an operator of the CCP must ensure that the margin meets or exceeds the single-tailed confidence level of at least 99 percent with respect to the estimated distribution of the future exposure of the portfolio. If a CCP uses portfolio margining, an operator 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

6.13 Two or more CCPs may enter into a cross-margining arrangement, which is an agreement among the CCPs 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 Standard 20: 'FMI links'). The aggregate collateral requirements for positions held in cross-margined accounts may be reduced if the value of the positions held at the separate CCPs move inversely in a significant and reliable fashion. In the event of a participant default under a cross-margining arrangement, participating CCPs may be allowed to use any excess collateral in the cross-margined accounts to cover losses.

6.14 Operators of CCPs that participate in cross-margining arrangements should share information frequently and ensure that they have appropriate safeguards, such as joint monitoring of positions, margin collections, and price information. An operator of a CCP should thoroughly understand the other CCP's risk management practices and financial resources (whether or not the latter CCP is a designated CCP). An operator of a CCP should also have harmonised overall risk management systems for the CCPs in the cross-margining arrangement and should regularly monitor possible discrepancies in the calculation of their 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 above would apply to cross-margining regimes between or among CCPs. An operator of a CCP in a cross-margining arrangement should also analyse fully the impact of cross-margining on prefunded default arrangements and on the adequacy of overall financial resources. An operator of a CCP should have in place arrangements for the CCP that are legally robust and operationally viable to govern the cross-margining arrangement.

Testing margin coverage

6.15 An operator of a CCP should analyse and monitor its model performance and overall margin coverage by conducting rigorous daily back testing and at least a monthly sensitivity analysis. An operator of a CCP must also conduct an annual assessment of the theoretical and empirical properties of the FMI margin model for all products the FMI clears. To validate the FMI's margin models and parameters, an operator of a CCP should have a back testing programme that tests its initial margin models against identified targets. Back testing is an ex-post comparison of observed outcomes with the outputs of the margin models. An operator of a CCP 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 back testing. The results of both the back testing and sensitivity analyses should be disclosed to participants.

6.16 *Back testing.* An operator of a CCP should back test the FMI's 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 consider portfolio effects across asset classes within the CCP. The initial margin model's actual coverage, along with projected measures of its performance, should at least meet the established single-tailed confidence level of 99 percent with respect to the estimated distribution of future exposure over an appropriate close out period. In case back testing indicates that the model did not perform as expected (that is, the model did not identify the appropriate amount of initial margin necessary to achieve the intended coverage), an operator of a CCP should have clear procedures for recalibrating its margining system, such as by making adjustments to parameters and sampling periods. In addition, an operator of a CCP should evaluate the source of back testing exceedances to determine if a fundamental change to the margin methodology is warranted or if only the recalibration of current parameters is necessary. Back testing procedures alone are not sufficient to evaluate the effectiveness of models and adequacy of financial resources against forward-looking risks.

6.17 *Sensitivity analysis*. An operator of a CCP should test the sensitivity of the CCP's margin model coverage using a wide range of parameters and assumptions that reflect possible market conditions to understand how the level of margin coverage might be affected by highly stressed market conditions. An operator 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 the FMI serves and extreme changes in the correlations between prices. An operator of CCP must conduct sensitivity analysis on its margin model coverage at least monthly using the results of these sensitivity tests and conduct a thorough analysis of the potential losses it could suffer. An operator of a CCP should evaluate the potential losses in individual participants' positions and, where appropriate, their customers' positions. Furthermore, for a CCP's clearing credit instruments, parameters reflective of the simultaneous default of both participants and 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 participant's increases significantly.

Validation of the margin methodology

6.18 An operator of a CCP must annually review (including by validating) the CCP's margin system. An operator should ensure a CCP's margin methodology is 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 Standard 2: 'Governance') and validated prior to implementation. Operators of CCPs operating a cross-margining arrangement should also analyse the impact of cross-margining on prefunded default arrangements and evaluate the adequacy of overall financial resources. Also, the margin methodology, including the initial margin models and parameters used by a CCP, should be 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. An operator of a CCP should make details of its margin methodology available to the participants for use in their individual risk management efforts.

Timeliness and possession of margin payments

6.19 An operator of a CCP should establish and rigorously enforce timelines for margin collections and payments and set appropriate consequences for failure to pay on time. An operator of a CCP 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 consider the liquidity of a participant's local funding market and the operating hours of relevant payment and settlement systems. Margin should be held by the CCP until the exposure has been extinguished. That is, margin should not be returned before settlement is successfully concluded.

STANDARD 7: LIQUIDITY RISK

7.1 Liquidity risk arises in an FMI 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 an FMI, liquidity risk can arise between the operator of an FMI and its participants, between the operator of an FMI and other entities (such as its settlement banks, nostro agents, custodian banks, and liquidity providers), or between participants in an FMI (such as in a DNS payment system or SSS). It is particularly important for an operator to manage carefully the FMI's liquidity risk if, as is typical in many systems, the FMI 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 FMI, the FMI may not have sufficient funds to meet its payment obligations to other participants. In such an event, the FMI would need to rely on its own liquidity resources (that is, liquid assets and prearranged funding arrangements) to cover the funds shortfall and complete settlement. An operator of an FMI must have a robust framework to manage liquidity risks for the FMI from its full range of participants and other entities. In some cases, a participant may play other roles within the FMI, such as a settlement or custodian bank or liquidity provider. These other roles should be considered in determining an FMI's liquidity needs. Note that the requirements in Standard 7: 'Liquidity risk' should not read as constraining a central bank's ability to act to promote financial stability (e.g., when it is acting as a lender of last resort).

Sources of liquidity risk

7.2 An operator should clearly identify the FMI's sources of liquidity risk and assess its current and potential future liquidity needs on a daily basis. An FMI can face liquidity risk from the default of a participant. For example, if an operator extends intraday credit, implicitly or explicitly, to the FMI's participants, such credit, even when fully collateralised, may create liquidity pressure in the event of a participant default. The FMI might not be able to quickly convert the defaulting participant's collateral into cash at short notice. If an operator does not have sufficient cash for the FMI to meet all of its payment obligations to participants, there will be a settlement failure. An FMI can also face liquidity risk from settlement banks, nostro agents, custodians, and liquidity providers, as well as linked FMIs and service providers, if these entities fail to perform as expected. Moreover, as noted above, an FMI may face additional risk from entities that have multiple roles within the FMI (for example, a participant that also serves as the FMI's settlement bank or liquidity provider). These interdependencies and the multiple roles that an entity may serve within an FMI should be taken into account by an operator.

7.3 An FMI that employs a DNS mechanism may create direct liquidity exposures between participants. For example, in a payment system that uses a multilateral net settlement mechanism, participants may face liquidity exposures to each other if one of the participants fails to meet its obligations. Similarly, in an SSS that uses a DvP model 2 or 3 settlement mechanism and does not guarantee settlement, participants may face liquidity exposures to each other if one of the participants fails to meet its obligations. A long-standing concern is that these types of systems may address a potential settlement failure by unwinding transfers involving the defaulting participant. This is not an issue where the system is covered by subpart 5 of Part 3 of the Act (which provides legal protections around finality of settlement), but in other cases where substantial unwinding of transactions is possible it may impose material liquidity pressures (and, potentially, replacement costs) on the non-

defaulting participants. If all such transfers must be deleted, and if the unwind occurs at a time when money markets and securities lending markets are illiquid (for example, at or near the end of the day), the remaining participants could be confronted with shortfalls of funds or securities that would be extremely difficult to cover. The potential total liquidity pressure of unwinding could be equal to the gross value of the netted transactions.

Measuring and monitoring liquidity risk

7.4 The standard requires that an operator of an FMI must 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, an operator should understand and assess the value and concentration of the FMI's daily settlement and funding flows through its settlement banks, nostro agents, and other intermediaries. An operator of an FMI 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 to operate the FMI. An operator should be able to determine the value of the FMI's available liquid assets, taking into account the appropriate haircuts on those assets (see Standard 5: 'Collateral' and Standard 6: 'Margin'). In a DNS system, an operator should provide sufficient information and analytical tools to help its participants measure and monitor their liquidity risks in the FMI.

7.5 If an operator maintains prearranged funding arrangements for the FMI, an operator should also identify, measure, and monitor the FMI's liquidity risk from the liquidity providers of those arrangements. An operator of an FMI should obtain a high degree of confidence through rigorous due diligence that each liquidity provider, whether or not it is a participant in the FMI, 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 RBNZ may be taken into account.

Managing liquidity risk

7.6 An operator of an FMI should also regularly assess its design and operations to manage liquidity risk in the FMI. An operator of an FMI that employs a DNS mechanism may be able to reduce its or its participants' liquidity risk by using alternative settlement designs, such as RTGS designs with liquidity-saving features or a continuous or extremely frequent batch settlement system. In addition, an operator could reduce the liquidity demands of participants by providing participants with sufficient information or internal systems to help them manage their liquidity needs and risks. Furthermore, an operator should ensure that the FMI is operationally ready to manage the liquidity risk caused by participants' or other entities' financial or operational problems. Among other things, an operator should have the operational capacity to reroute payments, where feasible, on a timely basis in case of problems with a correspondent bank.

7.7 An FMI has other risk management tools that an operator can use to manage the FMIs or, where relevant, its participants' liquidity risk. To mitigate and manage liquidity risk stemming from a participant default, an operator could use, either individually or in combination: exposure limits, collateral requirements, and

prefunded default arrangements. To mitigate and manage liquidity risks from the late-day submission of payments or other transactions, an operator could adopt rules or financial incentives for timely submission. To mitigate and manage liquidity risk stemming from a service provider or a linked FMI, an operator could use, individually or in combination: selection criteria, concentration or exposure limits, and collateral requirements. For example, an operator should seek to manage or diversify FMI settlement flows and 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. These tools are often also used by an operator to manage the FMI's credit risk.

Maintaining sufficient liquid resources for payment systems and SSSs

7.8 An operator must ensure that the FMI has sufficient liquid resources, as determined by rigorous stress testing, to effect settlement of payment obligations with a high degree of confidence under a wide range of potential stress scenarios. An operator of a payment system or SSS, including one employing a DNS mechanism, must ensure that sufficient liquid resources in all relevant currencies are available to effect same-day and, where appropriate, intraday or multiday settlement of payment obligations with a high degree of confidence under a wide range of potential stress scenarios that must include, but not be limited to, the default of the participant and its affiliates that would generate the largest aggregate payment obligation in extreme but reasonably foreseeable market conditions. In some instances, an operator of a payment system or SSS may need to have sufficient liquid resources to effect settlement of payment obligations over multiple days to account for any potential liquidation of collateral that is outlined in the FMI's participant-default procedures. An operator of a payment system or SSS will be treated as having sufficient liquid resources in all relevant currencies available if it ensures that such currencies are able to be obtained on an intraday basis in all reasonably foreseeable scenarios.

Maintaining sufficient liquid resources for central counterparties

7.9 Similarly, an operator must ensure a CCP has sufficient liquid resources available in all relevant currencies to settle securities-related payment obligations, 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. An operator must maintain additional liquidity resources sufficient to cover a wider range of potential stress scenarios that must include, but not be limited to:

a) where the operator is an operator of an FMI engaging in simple CCP activities, and the FMI is not systemically important in multiple jurisdictions, the default of the largest participant and its affiliates that would generate the largest aggregate payment obligation to the FMI in extreme but reasonably foreseeable market conditions; or

b) where the operator is an operator of an FMI engaging in complex CCP activities, or where the FMI is systemically important in multiple jurisdictions (including New Zealand), the default of the two largest participants and their affiliates that would generate the largest aggregate payment obligation to the FMI in extreme but reasonably foreseeable plausible market conditions.

i) An FMI would be considered systemically important in multiple jurisdictions where the FMI is designated as systemically important in New Zealand, and where it is assessed by an overseas regulator as so important to the market in that jurisdiction that it is subject to additional regulation or requirements. For example, where the FMI is subject to a regime that applies to prominent, significant, or systemically important FMIs in that jurisdiction.

7.10 An operator of the CCP should carefully analyse the FMI's liquidity needs and submit these to the regulator's review. In many cases, an operator of a CCP may need to maintain sufficient liquid resources to meet payments to settle required margin and other payment obligations over multiple days to account for multiday hedging and close out activities as directed by the CCP's participant default procedures. An operator of a CCP will be treated as having sufficient liquid resources in all relevant currencies available, if it ensures that such currencies are able to be obtained on an intraday basis in all reasonably foreseeable scenarios.

Liquid resources for meeting the minimum requirement

7.11 Unless the operator of an FMI is relying upon the ability to exchange another currency for the relevant currency, for the purpose of meeting its minimum liquid resource requirement, an operator must ensure the FMI'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 (repurchase agreements), 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 reasonably foreseeable market conditions. If an operator has access to routine credit at the central bank of issue, it may count such access as part of the minimum requirement to the extent an operator 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. However, such access does not eliminate the need for sound risk management practices and adequate access to private-sector liquidity resources.

Other liquid resources

7.12 An operator of an FMI may supplement its qualifying liquid resources with other forms of liquid resources. If an operator does so, then 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. An operator of an FMI may consider using such 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 FMI's participants and the financial system as a whole. An operator of an FMI must take into account what collateral is typically accepted by the relevant central bank of issue, as such assets may be more likely to be liquid in stressed circumstances. An operator must not assume the availability of emergency central bank credit as a part of its liquidity plan.

Assessing liquidity providers

7.13 If an FMI has prearranged funding arrangements, an operator 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 FMI or an external party, has sufficient information to understand and to manage the provider's associated liquidity risks, and that the provider 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. Additionally, an operator should adequately plan for the renewal of prearranged funding arrangements with liquidity providers in advance of their expiration.

Procedures regarding the use of liquid resources

7.14 An operator must have detailed procedures for using the FMI's liquid resources to complete settlement during a liquidity shortfall. An operator should ensure the FMI's procedures clearly document the sequence for using each type of liquid resource (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. In addition, an operator must annually test its procedures for accessing the FMI's liquid resources at a liquidity provider, this can include activating and drawing down test amounts from committed credit facilities and by testing operational procedures for conducting same-day repos.

Central bank services

7.15 If an FMI 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 Standard 9: 'Money settlements').

Stress testing of liquidity needs and resources

7.16 An operator must determine the amount and regularly test the sufficiency of the FMI's liquid resources through rigorous stress testing. An operator must have clear processes to report the results of its stress tests to appropriate decision makers and to use these results to evaluate the adequacy of and adjust its liquidity risk management framework. In conducting stress testing, an operator must consider a wide range of relevant scenarios. These scenarios must 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 reasonably foreseeable market conditions. Scenarios must also consider the design and operation of the FMI, include all entities that might pose material liquidity risks to the FMI (such as settlement banks, nostro agents, custodian banks, liquidity providers, and linked FMIs), and where reasonable, cover a multiday period. An operator should also consider any strong interlinkages or similar exposures between the FMI's participants, as well as the

multiple roles that participants may play with respect to the risk management of the FMI, and assess the probability of multiple failures and the contagion effect among its participants that such failures may cause.

7.17 *Reverse stress tests.* An operator of an FMI should conduct, as appropriate, reverse stress tests aimed at identifying the extreme default scenarios and extreme market conditions for which the FMI's liquid resources would be insufficient. In other words, these tests identify how severe stress conditions would be covered by the FMI's liquid resources. An operator 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 an operator to model extreme market conditions that may go beyond what are considered extreme but reasonably foreseeable market conditions in order to help understand the sufficiency of liquid resources given the underlying assumptions modelled. Modelling extreme market conditions can help an operator determine the limits of the FMI's current model and resources. However, it requires an operator to exercise judgment when modelling different markets and products. An operator should develop hypothetical extreme scenarios and market conditions tailored to the specific risks of the markets and of the products the FMI serves. Reverse stress tests should be considered a helpful risk management tool but they need not, necessarily, drive an operator's determination of the appropriate level of liquid resources.

7.18 *Frequency of stress testing*. 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, an operator 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 FMI's identified liquidity needs and resources in light of current and evolving market conditions. An operator 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 the FMI's participant's increases significantly. A full validation of an FMI's liquidity risk management model should be performed at least annually.

Contingency planning for uncovered liquidity shortfalls

7.19 In certain extreme circumstances, the liquid resources of an FMI or its participants may not be sufficient to meet the payment obligations of the FMI to its participants or the payment obligations of participants to each other within the FMI. In a stressed environment, for example, normally liquid assets held by an FMI may not be sufficiently liquid to obtain same-day funding, or the liquidation period may be longer than expected. An operator must establish explicit rules and procedures that enable the FMI 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 must address unforeseen and potentially uncovered liquidity shortfalls and must aim to avoid unwinding, revoking, or delaying the same-day settlement of payment obligations. These rules and procedures must also indicate the FMI's process to replenish any liquidity resources an operator may employ during a stress event, so that the FMI can continue to operate in a safe manner.

7.20 If an FMI allocates potentially uncovered liquidity shortfalls to its participants, an operator should have clear and transparent rules and procedures for the allocation of shortfalls (see also Standard 17A 'Contingency plans' and accompanying

guidance). These procedures could involve a funding arrangement between the FMI 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 should be discussed thoroughly with and communicated clearly to participants, as well as be consistent with participants' respective regulatory liquidity risk management requirements. Furthermore, an operator 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

8.1 Subpart 5 of Part 3 of the Act provides for the finality of settlements effected in accordance with the rules of an FMI (assuming the FMI is designated and the FMI's designation notice states that subpart 5 applies). This settlement finality guidance relates to circumstances where the FMI or the settlement finality issue is not covered by subpart 5 of Part 3.

8.2 An operator must ensure the FMI provides clear and certain final settlement of payments, transfer instructions, or other obligations. Final settlement is when there is an irrevocable and unconditional transfer of an asset or financial instrument, or the discharge of an obligation by the FMI or its participants in accordance with the terms of the underlying contract. A payment, transfer instruction, or other obligation that an FMI accepts for settlement in accordance with its rules and procedures must be settled with finality on the intended value date. The value date is 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. 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 an FMI's participants and other stakeholders, and potentially be a source of systemic risk. An operator should provide intraday or real-time settlement finality to reduce settlement risk.

8.3 Although some operators of FMIs guarantee settlement, this standard does not necessarily require an operator to provide such a guarantee. Instead, this standard requires operators to ensure FMIs clearly define the point at which the settlement of a payment, transfer instruction, or other obligation is final, and to complete the settlement process no later than the end of the value date, and preferably earlier in the value date. Similarly, this standard is not intended to eliminate fails to deliver in securities trades. 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, an operator should take steps to mitigate both the risks and the implications of such failures to deliver securities (see Standard 4: 'Credit risk', Standard 7: 'Liquidity risk', and other relevant standards).

Final settlement

8.4 An operator must ensure the rules and procedures for the FMI 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.

8.5 An FMI's legal framework and rules generally determine finality. In New Zealand, subpart 5 of Part 3 of the Act provides settlement and finality protection in relation to designated FMIs who have had this specified on their designation notice in accordance with section 29(2)(e) of the Act. An operator of an FMI should take reasonable steps to confirm the effectiveness of cross-border recognition and protection of cross-system settlement finality, especially when it is developing contingency plans in accordance with Standard 17A: 'Contingency Plans'. Due to the complexity of legal frameworks and system rules, particularly in the context of cross-border settlement where legal frameworks are not harmonised, the legal opinion required in accordance with Standard 1: 'Legal basis' should establish the point at which finality takes place.

Same-day settlement

8.6 An operator should ensure an FMI's processes are designed to complete 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 an FMI in accordance with its risk management and other relevant acceptance criteria should be settled on the intended value date. An FMI that is not designed to provide 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 an SSS or CCP 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 FMI and its other participants.

Intraday settlement

8.7 Depending on the type of obligations that an FMI settles, the use of intraday settlement, either in multiple batches or in real time, may be necessary or desirable to reduce settlement risk. As such, operators of some types of FMIs, such as HVPSs and SSSs, must adopt RTGS or multiple-batch settlement to complete final settlement intraday. RTGS is the real-time settlement of payments, transfer instructions, or other obligations individually on a transaction-by-transaction basis. Batch settlement is 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. With batch settlement, the time between the acceptance and final settlement of transactions should be kept short. To speed up settlements, an operator should encourage the FMI's participants to submit transactions promptly. To validate the finality of settlement, an operator also should inform the FMI's participants of their final account balances and, where practical, settlement date and time as quickly as possible, preferably in real time.

8.8 The use of multiple-batch settlement and RTGS involves different trade-offs. Multiple-batch settlement based on a DNS mechanism, for example, may expose participants to settlement risks for the period during which settlement is deferred. These risks, if not sufficiently controlled, could result in the inability of one or more participants to meet their financial obligations. Conversely, while an RTGS system can mitigate or eliminate these settlement risks, it requires participants to have sufficient liquidity to cover all their outgoing payments and can therefore require relatively large amounts of intraday liquidity. This liquidity can come from various sources, including balances at a central bank or commercial bank, incoming payments, and intraday credit. An operator of an RTGS system may be able to reduce its liquidity needs by implementing a queuing facility or other liquidity-saving mechanisms.

Revocation of unsettled payments, transfer instructions, or other obligations

8.9 An operator must clearly define the point after which unsettled payments, transfer instructions, or other obligations may not be revoked by a participant. In general, an

operator 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, 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, an operator may want to permit extensions for reasons connected with the implementation of monetary policy or widespread 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

9.1 An FMI 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, central bank money or commercial bank money is typically used. Central bank money is 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. Settlement in central bank money typically involves the discharge of settlement obligations on the books of the central bank of issue. Commercial bank money is a liability of a commercial bank, in the form of deposits held at the commercial bank, which can be used for settlement purposes. Settlement in commercial bank money typically occurs on the books of a commercial bank. In this model, an FMI typically establishes an account with one or more commercial settlement banks and requires each of its participants to establish an account with one of them. In some cases, the FMI itself can serve as the settlement bank. Money settlements are then effected through accounts on the books of the FMI, which may need to be funded and defunded. An FMI may also use a combination of central bank and commercial bank monies to conduct settlements, for example, by using central bank money for funding and defunding activities and using commercial bank money for the settlement of individual payment obligations.

Credit and liquidity risk in money settlements

9.2 An FMI and its participants may face credit and liquidity risks from money settlements. Credit risk may arise when a settlement bank has the potential to default on its obligations (for example, if the settlement bank becomes insolvent). When an FMI settles on its own books, participants face credit risk from the FMI itself. Liquidity risk may arise in money settlements if, after a payment obligation has been settled, participants or the FMI itself are unable to transfer readily their assets at the settlement bank into other liquid assets, such as claims on a central bank.

Central bank money

9.3 An operator must conduct the FMI's money settlements using central bank money, where reasonable and available, to avoid credit and liquidity risks. With the use of central bank money, a payment obligation is typically discharged by providing the FMI or its participants with a direct claim on the central bank, that is, 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. Indeed, one of the fundamental purposes of central banks is to provide a safe and liquid settlement asset. The use of central bank money, however, may not always be reasonable or available. For example, an FMI or its participants may not have direct access to all relevant central bank accounts and payment services. A multicurrency FMI that has access to all relevant central bank accounts and payment services may find that some central bank payment services do not operate, or provide finality, at the times when it needs to make money settlements.

Commercial bank money

9.4 If central bank money is not used, an operator must ensure the FMI conducts its money settlements using a settlement asset with little or no credit or liquidity risk. 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 FMI or its participants with a direct claim on the relevant commercial bank. To conduct settlements in commercial bank money, an operator 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 FMI and its participants. For example, if the commercial bank conducting settlement becomes insolvent, the FMI and its participants may not have immediate access to their settlement funds or ultimately receive the full value of their funds.

9.5 Where an FMI uses a commercial bank for its money settlements, an operator must monitor, manage, and limit the FMI's credit and liquidity risks arising from the commercial settlement bank. For example, an operator should limit both the probability of being exposed to a commercial settlement bank's failure and limit the potential losses and liquidity pressures to which it would be exposed in the event of such a failure. An operator must establish and monitor adherence to strict criteria for its commercial settlement banks that take into account, among other things, their regulation and supervision, creditworthiness, capitalisation, access to liquidity, and operational reliability. A commercial settlement bank 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.

9.6 In addition, an operator should take further steps to limit the FMI's credit exposures and liquidity pressures by diversifying the risk of a commercial settlement bank failure, where reasonable, through use of multiple commercial settlement banks. Even with multiple commercial settlement banks, the extent to which risk is actually diversified depends upon the distribution or concentration of participants using different commercial settlement banks and the amounts owed by those participants. An operator of an FMI should monitor and manage the full range and concentration of exposures to the FMI's commercial settlement banks and assess its potential losses and liquidity pressures as well as those of its participants in the event that the commercial settlement bank with the largest share of activity were to fail.

Settlement on the books of an FMI

9.7 Where money settlement does not occur in central bank money and the FMI conducts money settlements on an operator's or FMI's books, an operator must minimise and control its credit and liquidity risks. In such an arrangement, an FMI offers cash accounts to its participants, and payments or settlement obligations are discharged by providing an FMI's participants with direct claims on the FMI itself. The credit and liquidity risks associated with a claim on an FMI are therefore directly related to the FMI's overall credit and liquidity risks. One way an operator could minimise these risks is to limit the FMI's activities and operations to clearing and settlement and closely related processes. In some cases, an operator can further mitigate risk by having an FMI's participants fund and defund their cash accounts at the FMI using central bank money. In such an arrangement, an operator is able to

back the settlements conducted on the FMI's books with balances that it holds in its account at the central bank.

Finality of funds transfers between settlement accounts

9.8 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 Standard 1: 'Legal basis' and Standard 8: 'Settlement finality'). To this end, an operator must ensure an FMI's contractual arrangements with any settlement banks state clearly when transfers on the books of individual settlement banks are expected to occur, that transfers are to be final when effected, and that funds received are transferable as soon as possible (that is immediately), in order to enable the FMI and its participants to manage credit and liquidity risks. If an FMI conducts intraday money settlements (for example, to collect intraday margin), the arrangement should provide real time finality or intraday finality at the times when an FMI wishes to effect money settlement.

STANDARD 10: PHYSICAL DELIVERIES

10.1 An FMI may settle transactions using physical delivery, which is the delivery of an asset, such as an instrument or a commodity, in physical form. For example, the settlement of futures contracts cleared by a CCP may allow or require the physical delivery of an underlying financial instrument or commodity. An operator of an FMI that provides physical settlement must have rules that clearly state its obligations with respect to the delivery of physical instruments or commodities. In addition, an operator must identify, monitor, and manage the risks and costs associated with the storage and delivery of such physical instruments and commodities.

Rules that state the FMI's obligations

10.2 An operator must clearly state its and the FMI's obligations with respect to the delivery of physical instruments or commodities under the FMI's rules and procedures. The obligations that an FMI may assume with respect to physical deliveries vary based on the types of assets that the FMI settles. An operator of an FMI must clearly state which asset classes it accepts for physical delivery and the procedures surrounding the delivery of each. An operator 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 FMI and its participants to take the appropriate steps to mitigate the risks posed by such physical deliveries. An operator of an FMI should engage with the FMI's participants to ensure that they understand their obligations and the procedures for effecting physical delivery.

Risk of storage and delivery

10.3 An operator of an FMI must 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. An operator should plan for and manage physical deliveries by 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 an FMI is responsible for the warehousing and transportation of a commodity, an operator should make arrangements that take into account the commodity's particular characteristics (for example, storage under specific conditions, such as an appropriate temperature and humidity for perishables).

10.4 An operator should have appropriate processes, procedures, and internal systems to manage the risks of storing and delivering physical assets, such as the risk of theft, loss, counterfeiting, or deterioration of assets. The policies and procedures for the FMI should ensure that the record of physical assets accurately reflects the FMI's holdings of assets, for example, by separating duties between handling physical assets and maintaining records. An operator of an FMI 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, an operator 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

10.5 In some instances, an operator 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 must be clearly expressed in the rules, including default rules, and any related contracts. In particular, the rules and procedures for the FMI should be clear whether the receiving participant should seek compensation from the FMI or the delivering participant in the event of a loss. Additionally, an operator holding margin should not release the margin of the matched participants until it confirms that both have fulfilled their respective obligations. An operator should also monitor the FMI's participants' performance and, to the extent practicable, ensure that its participants have the necessary internal systems and resources to be able to fulfil their physical delivery obligations.

STANDARD 11: CENTRAL SECURITIES DEPOSITORIES

11.1 A CSD is an entity that provides securities accounts and, in some cases may also operate an SSS. A CSD also provides central safekeeping 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. Securities can be held at the CSD either in physical (but immobilised) form or in dematerialised form (as electronic records). An operator must ensure a CSD has clear and comprehensive rules and procedures to ensure that the securities it holds on behalf of its participants are appropriately accounted for on its books and protected from risks associated with the other services that the CSD may provide.

Rules, procedures, and internal systems to safeguard the integrity of securities issues

11.2 The preservation of the rights of issuers and holders of securities is essential for the orderly functioning of a securities market. Therefore, an operator must ensure a CSD employs appropriate rules, procedures, and internal systems to safeguard the rights of securities issuers and holders, prevent the unauthorised creation or deletion of securities, and conduct periodic and at least daily reconciliation of the securities issues that it maintains. An operator should, in particular, maintain robust accounting practices and perform end-to-end auditing to verify that its records are accurate and provide a complete accounting of its securities issues. If a CSD records the issuance of securities (alone or in conjunction with other entities), an operator should verify and account for the initial issuance of securities and ensure that newly issued securities are delivered in a timely manner. To further safeguard the integrity of the securities issues, an operator of a CSD should conduct periodic and at least daily reconciliation of the totals of securities issues in the CSD for each issuer (or its issuing agent), and ensure that the total number of securities recorded in the CSD for a particular issue is equal to the amount of securities of that issue held on the CSD's books. Reconciliation may require coordination with other entities if an operator of the CSD does not (or does not exclusively) record the issuance of the security or is not the official registrar of the security. For instance, if the issuer (or its issuing agent) is the only entity that can verify the total amount of an individual issue, it is important that the CSD and the issuer cooperate closely to ensure that the securities in circulation in a system correspond to the volume issued into that system. If the CSD is not the official securities registrar for the securities issuer, reconciliation with the official securities registrar should be required.

Overdrafts and debit balances in securities accounts

11.3 An operator of a CSD should prohibit overdrafts and debit balances in securities accounts to avoid credit risk and reduce the potential for the creation of securities. If a CSD were to allow overdrafts or a debit balance in a participant’s securities account in order to credit another participant’s securities account, a CSD would effectively be creating securities and would affect the integrity of the securities issue.

Immobilisation and dematerialisation

11.4 A CSD can maintain securities in physical form or dematerialised form. Securities held in physical form may be transferred via physical delivery or immobilised and transferred via book entry. The safekeeping and transferring of securities in physical form, however, creates additional risks and costs, such as the risk of destruction or theft of certificates, increased processing costs, and increased time to clear and settle securities transactions. By immobilising securities and transferring them via book entry, an operator of a CSD can improve efficiency through increased automation and reduce the risk of errors and delays in processing. Dematerialising securities also eliminates the risk of destruction or theft of certificates. An operator of a CSD must therefore maintain securities in an immobilised or dematerialised form and transfer securities via book entry.

Protection of assets

11.5 An operator of a CSD must protect assets against custody risk, which should include the risk of loss because of the CSD's negligence, misuse of assets, fraud, poor administration, inadequate recordkeeping, or failure to protect a participant's interests in securities or because of the CSD's insolvency or claims by the CSD's creditors. An operator of a CSD must have appropriate rules and procedures for the CSD to help ensure the integrity of the issue of securities issues and minimise and manage the risks associated with the safekeeping and transfer of securities, and should have robust internal systems to achieve these objectives. Where appropriate, an operator of a CSD should consider insurance or other compensation schemes to protect participants against misappropriation, destruction, and theft of securities.

11.6 An operator must employ a robust internal system for the FMI that ensures the segregation of assets belonging to the CSD from the securities belonging to its participants. In addition, an operator of the CSD must segregate participants' securities from those of other participants through the provision of separate accounts. While the title to securities is typically held in a CSD, often the beneficial owner, or the owner depending on the legal framework, of the securities does not participate directly in the system. Rather, the owner establishes relationships with CSD participants (or other intermediaries) that provide safekeeping and administrative services related to the holding and transfer of securities on behalf of customers. An operator also must operationally support the segregation of securities belonging to a participant's customers on the participant's books and facilitate the transfer of customer holdings to another participant. Where relevant, the segregation of accounts typically helps provide appropriate protection against the claims of a CSD's creditors or the claims of the creditors of a participant in the event of its insolvency.

Other activities

11.7 If a CSD provides services other than central safekeeping and administration of securities, an operator must identify, measure, monitor, and manage the risks associated with those activities, particularly credit and liquidity risks (see also Standard 4: 'Credit risk' and Standard 7: 'Liquidity risk'). Additional tools may be necessary to address these risks, including the need for an operator to separate legally the other activities. For example, a CSD that operates an SSS may provide a

centralised securities lending facility to help facilitate timely settlement and reduce settlement fails or may otherwise offer services that support the bilateral securities lending market. If the CSD acts as a principal in a securities lending transaction, an operator must identify, monitor, and manage its risks, including potential credit and liquidity risks, in accordance with the requirements of Standards 4 and 7. For example, the securities lent by the CSD may not be returned when needed because of a counterparty default, operational failure, or legal challenge. An operator of the CSD would then need to acquire the lent securities in the market, perhaps at a cost, thus exposing the CSD to credit and liquidity risks.

STANDARD 12: EXCHANGE-OF-VALUE SETTLEMENT SYSTEMS

12.1 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. 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). As 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 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). An operator of an FMI must mitigate principal and replacement risks through the use of a DvP, DvD, or PvP settlement mechanism.

Linking final settlement of obligations

12.2 An operator of an FMI that is an exchange-of-value settlement system must eliminate principal risk by linking the final settlement of one obligation to the final settlement of the other through an appropriate DvP, DvD, or PvP settlement mechanism (see also Standard 4: 'Credit risk', Standard 7: 'Liquidity risk', and Standard 8: 'Settlement finality'). DvP, DvD, and PvP settlement mechanisms eliminate principal risk by ensuring that the final settlement of one obligation occurs if and only if the final settlement of the linked obligation occurs. 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. DvP can and should be achieved for both the primary and secondary markets. 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 on a net basis, and the timing of when finality occurs.

Models of gross or net settlement of obligations

12.3 The final settlement of two linked obligations may be achieved either on a gross basis or on a net basis. For example, an SSS can settle the transfers of both securities and funds on a gross basis throughout the settlement day. Alternatively, an SSS can settle securities transfers on a gross basis throughout the day but settle funds transfers on a net basis at the end of the day or at certain times during the day. An SSS can also settle both securities and funds transfers on a net basis at the end of the day or at certain times during the day. Regardless of whether an FMI settles on a gross or net basis, the legal, contractual, technical, and risk management framework must ensure that the settlement of an obligation is final if and only if the settlement of the corresponding obligation is final.

Timing of settlement

12.4 DvP, DvD, and PvP can be achieved through different timing arrangements. Strictly speaking, DvP, DvD, and PvP do not require a simultaneous settlement of obligations. In some cases, settlement of one obligation could follow the settlement

of the other. For example, when an SSS does not itself provide cash accounts for settlement, it may first block the underlying securities in the account of the seller. The SSS may then request a transfer of funds from the buyer to the seller at the settlement bank for funds transfers. The securities are delivered to the buyer or its custodian if and only if the SSS receives confirmation of settlement of the cash leg from the settlement bank. In such DvP arrangements, however, the length of time between the blocking of securities, the settling of cash, and the subsequent release and delivery of the blocked securities should be minimised. Further, blocked securities must not be subject to a claim by a third party (for example, other creditors, tax authorities, or even the SSS itself) because these claims would give rise to principal risk.

STANDARD 13: PARTICIPANT-DEFAULT RULES AND PROCEDURES

13.1 Participant-default rules, policies, and procedures facilitate the continued functioning of an FMI in the event that a participant fails to meet its obligations. These rules, policies, and procedures help limit the potential for the effects of a participant's failure to spread to other participants and undermine the viability of the FMI. Key objectives of default rules, policies, and procedures should include (a) ensuring timely completion of settlement, even in extreme but reasonably foreseeable market conditions; (b) minimising losses for the FMI and for non-defaulting participants; (c) limiting disruptions to the market; (d) providing a clear framework for accessing FMI liquidity facilities as needed; and (e) managing and closing out the 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. An operator may also decide to auction or allocate open positions to the FMI's participants. To the extent consistent with these objectives, an operator should allow non-defaulting participants to continue to manage their positions as normal.

Rules, policies, and procedures

13.2 An operator must have default rules, policies, and procedures that enable the FMI to continue to meet its obligations to non-defaulting participants in the event of a participant default. An operator should explain clearly in its rules, policies, and procedures what circumstances constitute a participant default, addressing both financial and operational defaults. An operator of an FMI should describe the method for identifying a default. In particular, an operator 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, policies, and procedures include:

a) the actions that an operator can take when a default is declared; and \

b) the extent to which such actions are automatic or discretionary; and

c) potential changes to the normal settlement practices, should these changes be necessary in extreme circumstances, to ensure timely settlement; and

d) the management of transactions at different stages of processing; and

e) the expected treatment of proprietary and customer transactions and accounts; and

f) the probable sequencing of actions; and

g) the roles, obligations, and responsibilities of the various parties, including non-defaulting participants; and

h) the existence of other mechanisms that may be activated to contain the impact of a default.

An operator should involve the FMI's participants, the regulator, and other relevant stakeholders in developing its default rules, policies, and procedures (see Standard 2 'Governance' and Standard 17A 'Contingency plans').

Use and sequencing of financial resources

13.3 An operator's default rules, policies, and procedures should enable the FMI to take timely action to contain losses and liquidity pressures, before, at, and after the point of participant default (see also Standard 4: 'Credit risk' and Standard 7: 'Liquidity risk'). Specifically, the rules, policies, and procedures should allow the operator to use promptly any financial resources that it maintains for covering losses and containing liquidity pressures arising from default, including liquidity facilities. An operator should ensure the rules of the FMI specify the order in which different types of resources will be used. This information enables participants to assess their potential future exposures from using the FMI's services. Typically, an FMI 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 an FMI. The application of previously provided collateral should not be subject to prevention, stay, or reversal under applicable law and the rules of the FMI. An operator should also have a credible and explicit plan for replenishing the FMI's 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, an operator should ensure the FMI's rules and policies define the 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 without any disruptive effects.

Proprietary and customer positions

13.4 An operator of a CCP should have rules, policies, 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 CCP, the larger the CCP's potential credit exposures resulting from changes in market prices or other factors will be. An operator of a CCP 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 an operator of a CCP has the authority to act promptly to contain its exposure, while having regard for overall market effects, such as sharp declines in market prices. An operator of a CCP should have the information, resources, and tools to close out positions promptly. In circumstances where prompt close out is not practicable, an operator of a CCP should have the tools to hedge positions as an interim risk management technique. In some cases, a CCP may use seconded personnel from non-defaulting participants to assist in the close out or hedging process. An operator should ensure the CCP's rules, policies, and procedures clearly state the scope of duties and term of service expected from seconded personnel. In other cases, an operator of the CCP may elect to auction positions or portfolios to the market. An operator should ensure the CCP's rules, policies, and procedures 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 FMI.

Management discretion

13.5 An operator of an FMI should be well prepared to implement its default rules, policies, and procedures, including any appropriate discretionary procedures provided for in the rules. Management of the operator should ensure that the FMI has the operational capacity, including sufficient well-trained personnel, to implement its rules, policies, and procedures in a timely manner. An FMI's rules, policies, 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 FMI or authority is involved. In addition, timely communication with stakeholders, in particular with the regulator, is of critical importance. An operator of the FMI, 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 FMI's arrangements.

Public disclosure of key aspects of default rules and procedures

13.6 To provide certainty and predictability regarding the measures that an operator may take in a participant default event, an operator must publicly disclose key aspects of its default rules, policies, and procedures, which should include (a) the circumstances in which action may be taken; (b) who may take those actions; (c) the scope of the actions which may be taken, including the treatment of both proprietary and customer positions, funds, and other assets; (d) the mechanisms to address an FMI's obligations to non-defaulting participants; and (e) where direct relationships exist with participants' customers, the mechanisms to help address the defaulting participant's obligations to its customers. This transparency fosters the orderly handling of defaults, enables participants to understand their obligations to the FMI and to their customers, and gives participants the information they need to make informed decisions about their activities in the market. An operator should ensure that the FMI's participants and their customers, as well as the public, have appropriate access to the FMI's default rules, policies, 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.

Periodic testing and review of default procedures

13.7 An operator must involve the FMI's participants and other stakeholders in the testing and review of its default procedures, including any close out procedures. An operator must conduct such testing and review annually and following material changes to the rules, policies, and procedures to ensure that they are practical and effective. The periodic testing and review of default procedures is important to help the FMI and its participants understand fully the procedures and to identify any lack of clarity in, or discretion allowed by, the rules, policies, 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 regulator, and

any related service providers. This is particularly important where an FMI 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 board of directors, risk committee, and the regulator.

13.8 Furthermore, part of an FMI's participant-default testing should include the implementation of the resolution regime for an FMI's participants, as relevant. An operator should be able to take all appropriate steps to address the resolution of a participant. Specifically, an operator, 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.

STANDARD 14: SEGREGATION AND PORTABILITY

14.1 Segregation of the participant's customers' positions and collateral plays an important part in the safe and effective holding and transfer of these customers' positions and collateral, especially in the event of a participant's default or insolvency. Segregation refers to a method of protecting the participant's customer collateral and contractual positions by holding or accounting for them separately. A participant's customer collateral should be segregated from the assets of the participant through which the customers clear. Standard 14: 'Segregation' permits an operator to hold customer assets in individual or omnibus accounts (that is accounts where customer assets are pooled, but are segregated from participant assets), as set out below. Where individual participant customer collateral is held separately from the collateral of other customers of the same participant this structure protects customers from each other's default. Where the operator offers this structure, customer accounts, positions and collateral should be protected effectively from the concurrent default or insolvency of both a customer and the participant.

14.2 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 customer's positions and related collateral. Segregation also protects a participant's customers' collateral from becoming lost to a participant's other creditors. In addition, segregation facilitates the transfer of the participant's 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 the participant's customers' confidence in their clearing participants and may reduce the potential for "counterparty runs" on a deteriorating clearing participant.

14.3 Portability refers to the operational aspects of the transfer of contractual positions, funds, or securities from one party to another party. 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.

14.4 Effective segregation and portability of a participant's customers' positions and collateral depend not only on the measures taken by a CCP itself but also on applicable legal frameworks, including those in foreign jurisdictions in the case of remote participants. Effective segregation and portability also depend on measures taken by other parties, for example, where customers post additional collateral to the participant.

Legal framework

14.5 An operator of a CCP must structure its segregation and portability arrangements (including applicable rules) in a manner that protects the interests of a participant's customers and achieves a high degree of legal certainty under applicable law. An operator of a CCP should also consider potential conflict of laws when designing its arrangements. In particular, the CCP's rules and procedures that set out its segregation and portability arrangements should avoid any potential conflict with applicable legal or regulatory requirements (see Standard 1: 'Legal basis').

Customer account structures

14.6 This standard is particularly relevant for CCPs that clear positions and hold collateral belonging to customers of a participant. This clearing structure allows customers (such as buy-side firms) that are indirect participants of a CCP 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 CCP's default resources). An operator of a CCP must 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 CCP can be achieved in different ways, including through individual or omnibus accounts.

14.7 The degree of protection achievable for the participant's customer collateral will depend on whether the customers are protected on an individual or omnibus basis and the way initial margin is collected (gross or net basis) by the CCP. Each of these decisions will have implications for the risks the CCP faces from its participants and, in some cases, their customers. An operator of the CCP should understand, monitor, and manage these risks. Similarly, there are advantages and disadvantages to each type of account structure that the CCP should consider when designing its segregation regime.

Individual account structure

14.8 The individual account structure provides a high degree of protection to the clearing level collateral of customers of participants in a CCP, even in the case where the losses associated with another customer's default exceed the resources of the participant (see paragraph 14.10). Under this approach, the collateral for each customer of a participant is held in a separate, segregated individual account at the CCP, and 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 participant's customers' 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 participant's customers' positions only, an operator of the CCP 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 participant's customers' portfolio may be ported to another participant or group of participants. Maintaining individual accounts, however, can be operationally and resource intensive for the CCP in settling transactions and ensuring accurate bookkeeping. This approach could impact the overall efficiency of the CCP's operations.

Omnibus account structure

14.9 Another approach would be 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, can be more efficient when porting positions and collateral

for a group of customers of a defaulting participant (where there has been no customer default or where customer collateral is legally protected on an individual basis), and can be structured to protect customers' collateral from being used to cover a default by the direct participant.

14.10 However, depending on the CCP's rules, omnibus accounts where the customer collateral is protected on an omnibus basis 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.

14.11 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 an operator of the CCP 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 CCP to individual customers in the event a participant becomes insolvent.

14.12 The degree to which portability is fostered for a participant's customer whose assets are held in an omnibus account also varies depending on whether the CCP 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 CCP 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 preclude the possibility of under-margined customer positions when ported. As a result, CCPs 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 transactions 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.

14.13 When margin is collected by the CCP 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 collateralise a customer's positions on a going-forward basis. 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 CCP 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.

Factors to consider in choosing the level of protection

14.14 In considering whether to offer individual customer collateral protection at the clearing level, an operator of the CCP should take into account all relevant circumstances. Such circumstances include applicable insolvency regimes, the application of the Act (especially subpart 5 of Part 3), costs of implementation, and risk management challenges associated with the use of individual customer accounts, as well as the important benefits of individual customer protection. If an operator of the CCP determines that individual customer accounts should be offered, then an operator should endeavour to offer them at reasonable cost and in an unrestrictive manner and encourage direct participants to offer those accounts to their customers at a reasonable cost and in an unrestrictive manner.

Transfer of positions and collateral

14.15 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. A CCP'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. An operator of a CCP must 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, an operator should have the ability to identify positions that belong to customers, identify and assert its rights to related collateral held by or through the CCP, transfer positions and related collateral to one or more other participants, identify potential participants to accept the positions, disclose relevant information to such participants so that they can evaluate the counterparty credit and market risk associated with the customers and positions, respectively, and facilitate the CCP's ability to carry out its default management procedures in an orderly manner. An operator should ensure a CCP's rules and procedures 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.

14.16 However, there may be circumstances where it may be unnecessary to facilitate portability. For example, where a position is very short-dated and the applicable client positions will settle before porting can be completed.

14.17 An operator of the CCP 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, an operator should be set out in the CCP's rules. A CCP's policies and procedures also should provide for the proper handling of positions and collateral of customers of a defaulting participant.

Disclosure

14.18 An operator of a CCP must state the FMI's segregation and portability arrangements, in its rules and procedures. It would be useful for the CCP to include in the rules, the method for determining the value at which customer positions will

be transferred. A CCP's disclosure should ensure 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 the related risks and conduct due diligence when entering into transactions that are cleared or settled through a direct participant in the CCP. Customers should have sufficient information about which of its positions and collateral held at or through a CCP are segregated from positions and collateral of the participant and the CCP. Disclosure regarding segregation should include (a) whether the segregated assets are reflected on the books and records at the CCP or unaffiliated third-party custodians that hold assets for the CCP; (b) who holds the customer collateral (for example, CCP or third-party custodian); and (c) under what circumstances customer collateral may be used by the CCP. In particular, an operator of the CCP should disclose whether customer collateral is protected on an individual or omnibus basis.

STANDARD 15: GENERAL BUSINESS RISK

15.1 An operator must have robust management and internal systems to identify, monitor, and manage general business risk. General business risk refers to the risks and potential losses arising from an FMI's administration and operation as a business enterprise that are neither related to participant default nor separately covered by financial resources under the credit or liquidity risk Standards. General business risk includes any potential impairment of an operator or 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 FMI's custody arrangements), investment risk affecting the FMI's resources, and operational risk (in the case of fraud, theft, or loss). In these cases, general business risk may cause an FMI to experience an extraordinary one-time loss as opposed to recurring losses.

Identifying business risk

15.2 An operator should identify and assess the sources of business risk and their potential impact on the FMI's operations and services, taking into account past loss events and financial projections. An operator should assess and thoroughly understand the FMI's business risk and the potential effect that this risk could have on its cash flows, liquidity, and capital positions. In doing so, an operator 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, assess the impact and probability of the risks, and the effectiveness of the controls. Scenario analysis should examine how specific scenarios would affect the FMI. Sensitivity analysis should test how changes in one risk affect the FMI's financial standing, for example, conducting the analysis of how the loss of a key customer or service provider might impact the FMI's existing business activities. In some cases, an operator may want to consider an independent assessment of specific business risks.

15.3 An operator should clearly understand the FMI's general business risk profile so that an operator is able to assess the FMI's ability to either (a) avoid, reduce, or transfer specific business risks; or (b) accept and manage those risks. This requires the ongoing identification of risk-mitigation options that an operator may use in response to changes in its business environment. When planning an expansion of activity, an operator should conduct a comprehensive enterprise risk assessment. In particular, when considering any major new product, service, or project, an operator should project potential revenues and expenses as well as identify and plan how it will cover any additional capital requirements. Further, an operator 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

15.4 Once an operator has identified and assessed the FMI's business risk, an operator should measure and monitor these risks on an ongoing basis and develop

appropriate information systems as part of a robust enterprise risk management program. Key components of a robust enterprise risk management program include establishing strong financial and internal systems so that the FMI can monitor, manage, and control its cash flows and operating expenses and mitigate any business-related losses (see Standard 3: 'Framework for the comprehensive management of risks'). In particular, an operator 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. An operator should also ensure that it has rigorous and appropriate investment guidelines and monitoring procedures (see Standard 16: 'Custody and investment risks').

Determining sufficient liquid net assets

15.5 An operator must hold liquid net assets funded by equity (such as common stock, disclosed reserves, or retained earnings) so that the FMI can continue operations and services if it incurs general business losses. Equity allows an FMI to absorb losses on an ongoing basis and should be permanently available for this purpose. The amount of liquid net assets funded by equity that an operator should hold must 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. Accordingly, an operator must maintain a viable plan for the FMI to achieve recovery and orderly wind-down and should hold sufficient liquid net assets funded by equity to implement this plan. 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 FMI, the scope of its activities, the types of actions included in the plan, and the length of time needed to implement them. An operator 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. An operator must hold liquid net assets funded by equity equal to at least six months of current operating expenses.

15.6 To estimate the amount of liquid net assets funded by equity that a particular FMI would need, an operator 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 FMI's business model or because of external changes. An operator of an FMI 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 to cover general business risk.

15.7 Assets held to cover risks or losses other than business risk (for example, the financial resources required under Standard 4 and Standard 7) or to cover losses from other business lines that are unrelated to its activities as an FMI should not be included when accounting for liquid net assets available to cover business risk. However, equity held under international risk-based capital standards can be included where relevant and appropriate to avoid duplicate capital requirements.

15.8 Assets held to cover general business risk must be of high-quality and sufficiently liquid, such as cash, cash equivalents, or liquid securities, to allow the FMI to meet its current and projected operating expenses under a range of scenarios including in

adverse market conditions. To ensure the adequacy of the FMI's own resources, an operator should regularly assess its liquid net assets funded by equity relative to its potential business risks.

Maintaining sufficient equity

15.9 An operator must have a viable plan for raising additional equity should an operator's or FMI's capital fall close to or below the amount needed. This plan should be approved by an operator (this should include the board of directors) and be reviewed annually. An operator may also need to consult the FMI's participants and others during the development of its plan.

15.10 In developing a capital plan, an operator should consider a number of factors, including the FMI's ownership structure and any insured business risks. For example, an operator should determine if and to what extent specific business risks are covered by (a) explicit insurance from a third party; or (b) 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 timeframe. Given the contingent nature of these resources, an operator 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 FMI's capital adequacy.

STANDARD 16: CUSTODY AND INVESTMENT RISKS

16.1 An operator has the responsibility to safeguard assets held for the FMI, such as cash and securities, as well as the assets that participants have provided to the FMI. Custody risk is 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. Assets that are used by an operator to support the FMI's operating funds or capital funds or that have been provided by participants to secure their obligations under the rules of the FMI should be held at supervised or regulated entities or FMI's that have strong processes, internal systems, and credit profiles (for example, CSDs). In addition, assets should generally be held in a manner that assures an operator of prompt access to those assets in the event that the FMI needs to draw on them. Investment risk refers to the risk of loss faced by an operator or FMI when it invests its own or its participants' assets. Note that, where an operator is a central bank the requirements in Standard 16: 'Custody and investment risks' should not be read as constraining a central bank's ability to act to promote financial stability (e.g., when it is acting as a lender of last resort).

Use of custodians

16.2 An operator must mitigate the FMI's custody risk by using only supervised or regulated entities or FMIs with robust accounting practices, safekeeping procedures, and internal systems 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 Standard 1: 'Legal basis' and Standard 11: 'Central securities depositories'). The custodian also should have a strong financial position to be able to sustain losses from operational problems or non-custodial activities. An operator should confirm that its interest or ownership rights in the assets can be enforced and must 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, an operator should confirm it has prompt access to the assets in the event of a default of a participant.

16.3 An operator must evaluate the FMI's exposures to its custodians, taking into account the full scope of its relationships with each custodian bank. For example, a financial institution may serve as a custodian bank to an FMI as well as a settlement bank and liquidity provider to the FMI. The custodian bank also might be a participant in the FMI and offer clearing services to other participants. An operator should carefully consider all of the relationships with a particular custodian bank to ensure that the FMIs overall risk exposure to an individual custodian remains within acceptable concentration limits. Where feasible, an operator could consider using multiple custodians for the safekeeping of the FMI's assets to diversify its exposure to any single custodian. For example, a CCP may want to use one custodian for its margin assets and another custodian for its prefunded default arrangement. Such a CCP, 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, an operator should monitor the concentration of risk exposures to, and financial condition of, the FMI's custodian banks on an ongoing basis.

Investment strategy

16.4 An operator must have a strategy for investing its own and participants' assets that is consistent with its overall risk management strategy and fully disclosed to the FMI's participants. When making its investment choices, an operator should not allow pursuit of profit to compromise its liquidity risk management or the FMI's financial soundness. Investments should be secured by, or be claims on, high-quality obligors to mitigate the credit risk to which the FMI is exposed. Also, because the value of an FMI's investments may need to be realised quickly, investments should allow for quick liquidation with little, if any, adverse price effect. For example, an operator could invest the FMI's assets in overnight reverse repo agreements backed by liquid securities with low credit risk. An operator should carefully consider the FMI's overall credit risk exposures to individual creditors, including other relationships with the creditor that create additional exposures such as a creditor that is also a participant or an affiliate of a participant in the FMI. In addition, an operator should not invest participant assets in the participant's own securities or those of its affiliates. If an FMI's own resources can be used to cover losses and liquidity pressures resulting from a participant default, the investment of those resources should not compromise the ability to use them when needed.

STANDARD 17: OPERATIONAL RISK

17.1 Standard 17: 'Operational risk' should be read in conjunction with other standards and accompanying guidance that relate to operational risk, including Standard 3: 'Framework for comprehensive management of risks', Standard 17A: 'Contingency plans', Standard 17B: 'Critical service providers' and 17C: 'Cyber risk management'.

17.2 Standard 17: 'Operational risk' is largely based on principle 17 of the PFMI, however, some of the requirements and guidance from principle 17 have been moved and adapted within 17A, 17B, 17C as necessary to give additional prominence to specific risk management issues, such as contingency planning, critical service providers, and cyber risk management.

17.3 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 an FMI. Operational failures can result in disruption to essential services provided by an FMI, damage an FMI's reputation or perceived reliability, lead to legal consequences, and result in financial losses incurred by the FMI, participants, and other parties. In certain cases, operational failures can also be a source of systemic risk.

17.4 An operator must establish a robust framework to manage the FMI's operational risks with appropriate policies, procedures, and internal systems. As part of the operational risk management framework, an operator should identify and document the plausible sources of operational risk; deploy appropriate systems; establish appropriate policies, procedures, and systems; set operational reliability objectives; and develop contingency plans (see Standard 17A: 'Contingency plans') in response to identified risks. An operator should take a holistic approach when establishing the FMI's operational risk management framework and the framework should require the regular review of the policies, procedures, and internal systems to identify, assess, monitor and respond to operational risks.

17.5 An operator must actively identify the plausible sources of operational risk and mitigate their impact through the use of appropriate systems, policies, procedures and internal systems.

Identifying sources of operational risk

17.6 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 (a) errors or delays in message handling; (b) miscommunication; (c) service degradation or interruption; (d) fraudulent activities by staff; and (e) disclosure of confidential information to unauthorised entities. If an FMI provides services in multiple time zones, it may face increased operational risk due to longer operational hours and less downtime for maintenance.

17.7 The regulator expects an operator of an FMI to identify and document all potential single points of failure in the FMI's operations. The regulator's expectation is that an operator would do this on a continuous basis. Additionally, the regulator expects an operator to assess and document the evolving nature of the operational risk the FMI faces on an ongoing basis (for example, pandemics, cyber-attacks, and natural disasters), so that it can analyse its potential vulnerabilities and implement appropriate defence mechanisms.

Operational risk management

17.8 An operator must establish clear policies, procedures, and internal systems that mitigate the impact of the FMI's 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 an operator accepting, mitigating, or avoiding risks consistent with its operational reliability objectives for the FMI. An operator's governance arrangements, along with the FMI's governance arrangements, are pertinent to the FMI's operational risk management framework (see also Standard 2: 'Governance'). In particular, an operator's board must explicitly define the roles and responsibilities for addressing operational risk and endorse the FMI's operational risk management framework.

17.9 To ensure the proper functioning of its risk controls, an operator should establish sound internal controls for the FMI. For example, an operator should have adequate management controls, such as setting operational standards, measuring and reviewing performance, and correcting deficiencies. There are many relevant international, domestic, and industry-level standards, guidelines, or recommendations that an operator may use in designing the FMI's operational risk management framework. Conformity with commercial standards can help an operator reach its operational objectives for the FMI. For example, commercial standards exist for information security, business continuity, and project management. An operator should have protocols to regularly assess and document the need to integrate the applicable commercial standards into the FMI's operational risk management framework. In addition, an operator should seek to comply with relevant commercial standards in a manner commensurate with the FMI's importance and level of interconnectedness.

17.10 An operator should, test the FMI's policies, operational procedures and arrangements with participants at least annually. The regulator expects an operator to review these policies, operational procedures, and arrangements whenever necessary, and especially after significant changes occur to the system or a major incident occurs.

17.11 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).

17.12 Consistent with the evolving nature of operational risk management, the operational objectives for the FMI should be annually reviewed to incorporate new technological and business developments.

17.13 The proper performance of an operator's employees is a core aspect of any operational risk management framework, because of this an operator should employ sufficient, well-qualified personnel. An operator's personnel should be able to

operate the FMI safely and efficiently, and consistently follow operational and risk management procedures during normal and abnormal circumstances. An operator 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, an operator should have appropriate human resources and risk management policies to address fraud prevention.

17.14 The operational risk management framework for the FMI should include formal change management and project management processes to mitigate operational risk arising from modifications to operations, policies, procedures, and internal systems. Change management processes should provide mechanisms for preparing, approving, tracking, testing, and implementing all changes to the system (and the documenting of these occurring). Project management processes, in the form of policies and procedures, should mitigate the risk of any inadvertent effects on an FMI'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 in-house.

Operational reliability

17.15 An operator must have clearly defined operational reliability objectives for the FMI and policies in place that are designed to achieve those objectives. These objectives serve as benchmarks for an operator to evaluate the FMI's efficiency and effectiveness and evaluate the FMI's performance against expectations. These objectives should be designed to promote confidence among the FMI's participants. Operational reliability objectives should include the operational performance objectives for the FMI 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 an operator is intending the FMI to meet.

17.16 An operator should monitor, assess and document regularly whether the internal system is meeting its established objectives and service-level targets. The internal system's performance should be reported regularly to senior management, relevant board committees, participants, and authorities. In addition, the operational objectives for the FMI should be reviewed and updated annually to incorporate new technological and business developments.

Incident and outage management

17.17 An operator should have comprehensive and well-documented procedures in place to record, report, analyse, and resolve all FMI operational incidents (refer to Standard 23B: 'Notifying the regulator' for the requirement to report material incidents and outages).

17.18 In addition to reporting material incidents and all outages under Standard 23B, Standard 17: 'Operational risk' requires an operator seek an external assurance engagement to review the operational risk framework and compliance with that framework following material incidents and material outages. Material incidents are limited to events that have a substantive adverse impact on the FMI's participants or the financial system, while material outages are only those outages that have a

substantive adverse impact on the FMI's participants or the financial system. Note that, if appropriate, the extent of the external engagement report on the operational risk framework may be limited in scope to those areas of the framework affected by the incident or outage.

17.19 The external assurance engagement must be done by a qualified auditor.

17.20 The exception to this requirement is where an operator forms the opinion that it is not reasonable to seek an external assurance engagement. An example of this would be where the cost of the external assurance engagement would significantly outweigh the benefit of the external assurance engagement or where an internal review could adequately address concerns following material incidents and outages. If the operator forms this opinion then the operator must provide the relevant justification for this opinion to the regulator.

17.21 In addition to the requirements above it is best practice after every significant incident or outage, for an operator to undertake and document 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 and reasonable, include the FMI's participants.

Operational capacity

17.22 An operator must ensure that the FMI 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 an operator monitors, reviews, and tests (including stress testing) the actual capacity and performance of the FMI's system on an ongoing basis. An operator should carefully forecast demand and make appropriate plans to adapt to any reasonably foreseeable change in the volume of business or technical requirements. These plans should be documented and based on a sound, comprehensive methodology so that the required service levels and performance can be achieved and maintained. As part of capacity planning, an operator should determine a required level of redundant capacity for the FMI, taking into account the FMI'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.

Physical and information security

17.23 An operator must have comprehensive physical and information security policies that address all potential vulnerabilities and threats to the FMI (see also Standard 17B: 'Critical service providers').

17.24 In particular, the regulator expects an operator to have policies effective in assessing and mitigating vulnerabilities in the FMI's physical sites from attacks (see also Standard 17C: 'Cyber resilience'), intrusions, and natural disasters. The regulator expects an operator to have sound and robust information security policies, standards, practices, and internal systems (including controls) to ensure an appropriate level of confidence and trust in the FMI by all stakeholders. These policies, standards, practices, and internal systems should include the identification, assessment, and management of security threats and vulnerabilities for the purpose of implementing appropriate safeguards into its systems. Data should be protected

from loss and leakage, unauthorised access, and other processing risks, such as negligence, fraud, poor administration, and inadequate recordkeeping. An operator's information security objectives and policies for the FMI should conform to commercially reasonable standards for confidentiality, integrity, authentication, authorisation, non-repudiation, availability, and auditability (or accountability).

Interdependencies

17.25 An FMI is connected directly and indirectly to its participants, other FMIs, and its service and utility providers. Accordingly, an operator should identify both direct and indirect effects on the FMI's ability to process and settle transactions in the normal course of business and manage risks that stem from an external operational failure of connected entities. These effects include those transmitted through the FMI's participants, which may participate in multiple FMIs. An operator of an FMI must identify, monitor, and manage the risks the FMI faces from, and poses to, other FMIs (see Standard 20 'FMI links'). To the extent possible, an operator should coordinate business continuity arrangements between its FMI and interdependent FMIs (refer to Standard 17A: 'Contingency plans'). An operator also should consider the risks associated with the FMI's service and utility providers and the operational effect on the FMI if service or utility providers fail to perform as expected. An FMI 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.

17.26 To manage the operational risks associated with its participants, an operator should consider establishing minimum operational requirements for the FMI's participants (see also Standard 18: 'Access and participation requirements'). For example, an operator may want to define operational and business continuity requirements for participants in accordance with the participant's role and importance to the FMI. In some cases, an operator may want to identify critical participants based on the consideration of transaction volumes and values, services provided to the FMI 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 an operator and FMI. An operator should have clear and transparent criteria, methodologies, or standards for critical participants to ensure that the FMI's operational risks are managed appropriately.

Operational risk management and rule setting bodies

17.27 Where an operator is the operator of an FMI that is a rule-setting body only, the operator should mitigate operational risk using the tools it has available, such as by setting rules that manage operational risk to the extent reasonably possible.

STANDARD 17A: CONTINGENCY PLANS

17A.1 Comprehensive and effective contingency plans are a key part of the crisis management framework for FMIs in New Zealand. The requirements are designed as a first line of defence in crisis management and should avoid the need for the regulator to use statutory crisis management powers in the majority of circumstances. Contingency plans under the Act cover both requirements to have business continuity plans based on the requirements in the PFMI, and recovery and orderly wind-down plans to respond to financial threats to the continued provision of essential services. That is, an operator's contingency plan for the FMI must cover both:

a) non-financial matters that may threaten its ongoing provision of essential services. In particular, how the plan will achieve the rapid recovery and timely resumption of those services, and if necessary, the replacement of an operator; and

b) how an operator will address threats to FMI's financial ability to continue to provide essential services and the process of winding down the operation of the FMI should it be unable to continue for any reason. Where relevant, this must include mechanisms that allocate losses caused by participant default, and that allow for the financial recovery of an operator.

17A.2 Section 47 of the Act requires contingency plans to be: comprehensive, adequate, and credible (taking into account the type of FMI concerned and the activities carried out under it) and which are capable of being activated and implemented effectively when appropriate.

17A.3 Standard 17A: 'Contingency plans' applies to operators of FMIs with different business models and structures and therefore contingency planning requirements are designed to be outcomes focused to be appropriate to different types of FMIs.

17A.4 The contingency plan must identify the FMI's essential services. An example of an FMI essential service is the clearing or settling a significant class of payments or other financial transactions.

17A.5 Note that essential services are services provided by the FMI, rather than services provided to the FMI (see Standard 17B: 'Critical service providers'). A crisis situation could arise out of a number of quite different events, such as:

a) the failure of an operator or FMI, such as due to insolvency or operational or non-financial failure (such as a natural disaster);

b) a participant defaulting on its obligations under the rules of the FMI;

c) the failure of a critical service provider;

d) credit losses or liquidity shortfalls;

e) general business losses or the realisation of investment losses; or

f) the failure of related entities or linked FMIs.

17A.6 The contingency plans should consider all of the above scenarios and any other reasonably foreseeable scenarios or events, and outline how the FMI's rules should interact with those scenarios. Both internal and external threats should be considered, and the impact of each threat should be identified and assessed.

17A.7 However, where an operator is a central bank, the operator should only develop contingency plans that consider scenarios that are appropriate for a central bank.

17A.8 An operator must also put in place procedures ensuring that, following a non-financial or operational failure, an acceptable degree of recovery can be reached within two hours or if this timeframe is not possible, the plans should explain why another timeframe is appropriate. An operator should explain the likely impact of the failure on the FMI's participants and the broader financial system in New Zealand. The plans should be designed to enable the FMI to complete settlement (where this is part of the FMI's essential services) by the end of the day even in case of extreme circumstances. Contingency plans for all FMIs should ensure that the status of all transactions at the time of the disruption can be identified with certainty within two hours, or if this is not possible, the appropriate alternative timeframe. Reasoning for any alternative timeframe should also be documented within the contingency plan.

17A.9 Depending on the nature of the FMI, and its interconnectedness with the New Zealand financial system, it may be appropriate for an operator to set up secondary and tertiary sites and alternative arrangements (for example, manual procedures) that could operate as part of the contingency plan. Contingency plans (or other related policies) should document an operator's consideration of whether such requirements are necessary to provide sufficient confidence that the FMI can process time-critical transactions and that its business continuity objectives will be met in all scenarios identified in contingency plans.

17A.10 If an operator considers a secondary and/or tertiary site to be appropriate, the site should be resourced with sufficient capabilities, functionalities and appropriate staffing arrangements that would not be affected by a wide-scale disruption and would allow the secondary or tertiary site to take over operations if needed. The secondary site should provide the level of essential services necessary to perform the functions consistent with the recovery time objective and be located at a geographical distance from the primary site that is sufficient to have a distinct risk profile, for example, a secondary site must be located such that it would not be affected by a natural disaster such as a flooding event or earthquake that affected the primary site. Similarly, a tertiary site should be located at a geographical distance from both the primary and secondary sites that allows a distinct risk profile.

17A.11 Following an event threatening the FMI's financial ability to continue to deliver essential services, the contingency plans must provide a set of financial recovery tools, taking into account the nature of the FMI's operations. The set of tools should be comprehensive and effective in allowing an operator to, where relevant, allocate any uncovered losses and cover liquidity shortfalls. The set of tools should also include reasonably foreseeable means of addressing unbalanced positions (where relevant) and replenishing financial resources, including the FMI's own capital, in order to continue to provide essential services (refer to Standard 13: 'Participant-Default Rules and Procedures'). Examples of such tools are the payment waterfalls featured in the rules of CCPs and rules for the pro-rating of losses across security account holders that are typically a feature of CSDs. Allocating losses in the rules provides ex ante certainty for participants and regulators, limiting the need for such matters to be resolved through statutory powers or legal proceedings.

17A.12 Each recovery tool should be designed to be effective (timely, reliable, and have a strong legal basis) as well as be transparent to allow those who would bear losses and liquidity shortfalls to measure, manage and control their potential exposure. The set of recovery tools should create appropriate incentives for the FMI's owners, participants, and other relevant stakeholders to control the amount of risk that they bring to, or incur in, the system, monitor the FMI's risk-taking and risk management activities, and assist in the FMI's default management process.

17A.13 The contingency plans should be designed to minimise the negative impact on direct and indirect participants and the New Zealand financial system more broadly.

17A.14 While the contingency plans should be standalone documents, the plans should also be operationalised through specific provisions in the rules of the FMI in appropriate cases. For example, to the extent that a participant default creates losses, the rules of the FMI should provide for the allocation of losses to participants.

17A.15 The contingency plans should also include clearly defined procedures for crisis and scenario management. The plans should also address the need for rapid deployment of a multi-skilled crisis and event management team as well as procedures to consult and quickly inform participants, interdependent FMIs, the regulator and others (such as service providers and, where relevant, the media). Communication with the regulator is critical in case of a major disruption to an FMI's operations or a wider market distress that affects the FMI, particularly where the regulator might rely on data held by the FMI for crisis management. Depending on the nature of the problem, external communication channels may also need to be activated, for example with:

a) local civil authorities, for physical attacks or natural disasters; or

b) information technology experts for software malfunctions or cyber-attacks such as CERT (the Computer Emergency Response Team).

17A.16 Where an FMI 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.

17A.17 Contingency plans must also:

a) ensure that the FMI is severable from an operator. That is, the contingency plans must allow for another operator to operate the FMI in the event of an operator failure or another financial event (note that this requirement is not relevant for contingency plans for central bank operated FMIs, given the impracticalities of replacing an operator); and

b) set out how an FMI would be wound down in an orderly manner if the FMI is not able to continue delivering essential services on an ongoing basis and an alternative operator is not available to ensure the continued functioning of the FMI. This should include clear timeframes for the orderly wind-down process to ensure that participants and any other impacted parties are able to plan ahead. The requirement does not apply where an operator is a central bank, given the nature of the FMIs operated by the central banks.

17A.18 The standard also requires operators to have plans that clearly state objectives and includes policies and procedures which are designed to respond to identified

operational and financial events. An operator should devote appropriate resources to this planning. All aspects of the contingency plans should be clearly and fully documented. An operator must also clearly set out in the contingency plans those persons who are responsible for ensuring the plans are regularly assessed and updated, as well as who is responsible for activating the plan.

17A.19 The contingency plans should be subject to regular (at least annual) review and testing. Tests should address various scenarios that simulate wide-scale disasters and transfers from primary to secondary and tertiary sites (where applicable). Employees should be thoroughly trained to execute the contingency plan. An operator should involve participants, critical service providers, and linked FMIs in the testing of the FMI's contingency plans. An operator should also consider the need to participate in industry-wide tests.

17A.20 An operator should make appropriate adjustments to the FMI's contingency plans and associated arrangements based on the results of the testing exercises, and records should be maintained to evidence these regular assessments and resulting changes.

17A.21 In accordance with section 48(1) of the Act, an operator must give details of the activation of its FMI contingency plans to the regulator as soon as practicable after it has activated the plans.

STANDARD 17B: CRITICAL SERVICE PROVIDERS

17B.1 The operational reliability of an FMI may be dependent on the continuous and adequate functioning of service providers that are critical to an FMI's operations, such as information technology and messaging providers. Standard 17B: 'Critical service providers' sets out requirements that an operator must take reasonable steps to ensure an FMI's critical service providers are able to meet (see also Standard 17C: 'Cyber resilience'). The expectations outlined below are intended to ensure an FMI's critical service provider supports the FMI's delivery of essential services. Standard 17B: 'Critical service providers' covers risk identification and management, robust information security management, reliability and resilience, effective technology planning, and strong communications with FMIs and operators. These expectations are written at a broad level, allowing operators flexibility in how they ensure an FMI's critical service providers meet the expectations. The requirements in Standard 17B: 'Critical service providers' and expectations on critical service providers set out below are intended to help ensure the operations of a critical service provider are held to the same standards as if the FMI provided the service.

17B.2 The regulator expects that the requirements in clause 1 of Standard 17B: 'Critical service providers' would be met through the terms of a contract between the critical service provider and an operator wherever possible. However, there may be circumstances where this is not reasonable, such as where there is no existing contract between an operator and the critical service provider, or because it may take several years for a contract to be negotiated.

17B.3 In situations where it is not reasonable to enforce the requirements in Standard 17B 'Critical service providers' via contractual terms, reasonable steps to meet the requirements may include (but are not limited to):

a) requesting relevant information from the critical service provider during the contract negotiation process; and/or

b) including service level agreements in contracts to encourage critical service providers to maintain reliable and resilient systems; and/or

c) requiring regular performance meetings with critical service providers; and/or

d) requiring regular reporting on issues and performance from critical service providers.

Note that these examples are illustrative only and may not be reasonable steps for the operator to take in all circumstances, such as when the critical services offered are highly standardised and not specific to the FMI's operations.

Risk identification and management

17B.4 An operator must take reasonable steps to ensure that a critical service provider identifies and manages relevant operational and financial risks to its critical services and ensures that its risk management processes are effective.

17B.5 An operator should take reasonable steps to ensure that a critical service provider has effective processes and internal systems for:

a) identifying and documenting risks;

b) implementing controls to manage risks; and

c) making decisions to accept certain risks.

17B.6 A critical service provider may face risks related to information security, reliability and resilience, and technology planning, as well as legal and regulatory requirements pertaining to its organisation and conduct, relationships with customers, strategic decisions that affect its ability to operate as a going concern, and dependencies on third parties. An operator should require a critical service provider to reassess its risks, as well as the adequacy of its risk management framework in addressing the identified risks, on an ongoing basis.

17B.7 Where an operator is in a position to do so, an operator should ensure that the critical service provider's board of directors is overseeing the identification and management of risks and that these risks are assessed by an independent, internal audit function.

Information security

17B.8 An operator must take reasonable steps to ensure that a critical service provider 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 its obligations to an operator (or the FMI, as appropriate).

17B.9 An operator must take reasonable steps to ensure a critical service provider has a robust information security framework that appropriately manages its information security risks. Such a framework should be expected to include sound policies and procedures to protect information from unauthorised disclosure, ensure data integrity, and guarantee the availability of its services. In addition, operators should expect a critical service provider to have policies and procedures for monitoring its compliance with its information security framework. The information security framework should also include capacity planning policies and change management practices. For example, a critical service provider that plans to change its operations should be expected to assess the implications of such a change on its information security arrangements.

Reliability and resilience

17B.10 An operator should take reasonable steps to ensure that a critical service provider implements appropriate policies and procedures, and devotes sufficient resources, to ensuring that its critical services are available, reliable, and resilient. The critical service provider's 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 its obligations to an operator (or the FMI, as appropriate).

17B.11 An operator should require a critical service provider to ensure that it provides reliable and resilient operations to an operator and the FMI's participants. An operator should expect a critical service provider to have robust operations that

meet or exceed the needs of the FMI. An operator should expect a critical service provider to:

a) record and report operational incidents; and

b) provide analysis on such incidents promptly to prevent recurrences that could have greater implications.

17B.12 An operator should take reasonable steps to ensure that a critical service provider has robust business continuity and disaster recovery objectives and plans. These plans should include routine business continuity testing and a review of these test results to assess the risk of a major operational disruption.

Technology planning

17B.13 An operator must take reasonable steps to ensure that a critical service provider has robust methods in place to plan for the entire lifecycle of the use of technologies and the selection of technological standards.

17B.14 A critical service provider should have effective technology planning that minimises overall operational risk and enhances operational performance. Planning should entail a comprehensive information technology strategy that considers the entire lifecycle for the use of technologies, and a process for selecting standards when deploying and managing a service. Proposed changes to a critical service provider's technology should include a comprehensive consultation with an operator and, where appropriate, its participants. An operator should require a critical service provider to regularly review its technology plans, including assessments of its technologies and the processes it uses for implementing change.

Communication with an operator and FMI participants

17B.15 An operator must take reasonable steps to ensure that a critical service provider provides an operator with sufficient information to clearly understand its roles and responsibilities in managing risks related to the FMI's use of a critical service provider.

17B.16 An operator should expect a critical service provider to have effective communication procedures and processes. In particular, a critical service provider should provide an operator and the FMI's participants (where they are affected), with sufficient information to clearly understand their roles and responsibilities, enabling them to manage adequately their risks related to their use of the services provided.

17B.17 Useful information that an operator should expect from a critical service provider may include, but is not limited to, information concerning the critical service provider's management processes and internal systems (and independent reviews of the effectiveness of these processes and controls). As a part of its communication procedures and processes, a critical service provider should be expected to have mechanisms to consult with the FMI and the broader market on any technical changes to its operations that may affect its risk profile, including incidences of absent or non-performing risk controls of services. In addition, operators should expect a critical service provider to have a crisis communication plan to handle operational disruptions to its services.

Treatment of basic utilities

17B.18 The definition of critical services in Standard 17B: 'Critical service providers' is not intended to cover the supply of basic utilities such as:

a) the retail supply of gas;

b) the retail supply of electricity;

c) the supply of water; and

d) the supply of generic telecommunication services that are necessary to operate all, or almost all, businesses (for example telephone or voice messaging services or web-browsing services).

STANDARD 17C: CYBER RESILIENCE

17C.1 This guidance draws upon international and national cyber security standards and guidelines. This guidance is designed to assist operators to understand how they can fulfil the cyber resilience requirements in Standard 17C: 'Cyber resilience', which outline an overarching framework for the governance and management of cyber risk. A key objective of Standard 17C: 'Cyber resilience' and this accompanying guidance is to promote cyber resilience in the financial sector by setting expectations and raising awareness of good practice at the board and senior management level.

17C.2 Standard 17C: 'Cyber resilience' and this guidance are not a checklist for cyber resilience minimum requirements. Instead, an operator must ensure that the FMI designs and develops a cyber resilience strategy and framework that adequately addresses the specific cyber threats faced by the FMI. In meeting this requirement, an operator is encouraged to consult more detailed guidance on specific aspects of cyber resilience which are available in various cyber resilience frameworks.

Cyber resilience strategy and framework

17C.3 An operator must ensure that the FMI has a comprehensive, adequate, and credible cyber resilience strategy and framework. Operators must also ensure that an FMI's cyber resilience strategy and framework is based on internationally and nationally recognised frameworks and guidelines. The cyber resilience strategy and framework can be standalone files or embedded in the FMI's other strategies and frameworks (for example, an information technology security strategy or framework).

17C.4 A comprehensive, adequate, and credible cyber resilience strategy should outline:

a) the importance of cyber resilience to the FMI;

b) the high-level requirements of the FMI's stakeholders;

c) the FMI's vision and mission regarding cyber resilience;

d) the FMI's cyber resilience objectives;

e) the FMI's cyber risk appetite;

f) the FMI's cyber resilience targets and implementation plan;

g) the high-level scope of technology and assets which will be used to manage cyber resilience;

h) how cyber resilience initiatives will be delivered, managed, and funded; and

i) the integration of cyber resilience with people, processes, technology, and new or existing business initiatives.

17C.5 A comprehensive, adequate, and credible cyber resilience framework should:

a) set out how the entity sets its risk tolerance and cyber resilience objectives, and how the entity identifies, mitigates, and manages its cyber risk to support its objectives;

b) incorporate the recommendations of this guidance related to governance, capability building, information sharing. and third-party management;

c) be consistent with the entity's risk management framework; and

d) be annually tested and updated. All elements of an FMI's cyber resilience framework should be annually tested and updated, to remain effective against ever-evolving cyber risk. This testing could include penetration testing, vulnerability assessments, or business impact analysis.

Capability building

17C.6 This section provides guidance on the areas operators should focus on when implementing a cyber resilience strategy and framework for the FMI. It follows the structure of the US National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity, being:

a) Identify; and

b) Protect; and

c) Detect; and

d) Respond and recover.

17C.7 This section also provides further guidance on information sharing and the management of third-party service providers.

Identify

17C.8 An operator should identify, classify (according to criticality and sensitivity), record, and regularly update all of the FMI's essential services, including the information assets, key personnel roles, and processes that support these essential services. This will enable an operator to prioritise the processes of protection, detection, response and recover for each of these essential services.

17C.9 Identification and classification of essential services ensures that an operator can effectively prioritise and protect the FMI's most important information assets and operations against potential cyber threats. Additionally, an operator's ability to understand the FMI's external responsibilities to the stability of the wider financial sector is necessary in ensuring it efficiently recovers from cyber incidents.

17C.10 An operator should also create and maintain an up-to-date inventory of all of the FMI's individual and system accounts, taking care to include those with remote access or privileged access rights, in order to ensure access to sensitive information and supporting systems is kept on an as-needed basis only.

17C.11 An operator should create and regularly update a map of the FMI's network resources, including IPs, devices, servers, and any external network links that support the FMI's essential services.

17C.12 An operator should make sure these identification and classification efforts are integrated with other relevant processes, such as acquisition and change management, in order to ensure inventories are kept up to date, as well as remaining both accurate and complete.

17C.13 Cyber risk assessments should be conducted before new or updated technologies, products, services, or processes are introduced, to identify any associated threats or vulnerabilities. An operator should also carry out risk assessments on a regular basis to identify new vulnerabilities and cyber threats as they emerge and feed these issues and mitigating actions back into the FMI cyber resilience strategy and cyber resilience framework.

Protect

17C.14 An operator should have security controls in place, based on the FMI's identified essential services, which allow it to achieve its security objectives and meet business requirements for the FMI while minimising the probability and potential impact of a cyber-attack. The security objectives for the FMI should include ensuring the continuity and availability of its information systems as well as protection of the integrity, confidentiality, and availability of data and information while stored, in use or in transit.

17C.15 An operator should regularly update the FMI's security controls to ensure the approaches it adopts remain commensurate to the FMI's essential services, cyber threat landscape, and systemic importance.

17C.16 An operator should regularly monitor the FMI's systems throughout their life cycle, to identify weaknesses. It should also ensure all available updates are installed and sufficient support is maintained, as appropriate. Additional layers of security should be implemented and tested where vulnerabilities are identified in systems.

17C.17 An operator should ensure that access to the FMI's systems and information is controlled so that only staff who are authorised to access them can do so. This includes ensuring that:

a) authorisation is restricted according to the principle of least privilege, meaning granting the bare minimum access only to those who have a legitimate business reason for it, and are trained to use the system or information appropriately; and

b) controls are in place that strictly limit and monitor staff with greater/privileged access entitlements; and

c) processes are in place to monitor system and information access and trigger an alert when unauthorised access is attempted or granted; and

d) processes are in place to monitor employees changing roles or leaving the FMI, to ensure all access rights are updated accordingly when the change takes place.

17C.18 An operator should implement appropriate screening and background checks for all new employees and contractors of the FMI before they are hired/contracted.

17C.19 An operator should have policies, procedures, and internal systems in place for the FMI regarding change management and ensure cyber security is considered throughout the life cycle of the change management process. Such process should include identifying patches to technology and software assets, evaluating patch criticality and risk, and testing and applying the patch in an appropriate timeframe.

17C.20 Legacy systems that are outdated, have limited or no support, or have vulnerabilities that cannot be adequately patched or mitigated through segregation from other systems, should be decommissioned and replaced.

17C.21 An operator should adopt a 'resilience by design' approach to designing the FMI's systems, processes, products, and services. This means embedding the resilience measures within the systems, processes, products, and services from the first stage of design and development. The process to instil resilience by design should ensure that (a) software, network configurations, and hardware supporting or connected to critical systems are subject to rigorous testing against related security standards; (b) that attack surfaces are limited to the extent practicable; and (c) that common information security principles relating to confidentiality, integrity, and availability are adhered to (including by ensuring access to systems is limited to authorised personnel, as discussed above).

17C.22 An operator should have strong controls in place to identify and prevent data loss through removal from the FMI's internal systems. This includes ensuring that the FMI's protective controls enable the monitoring and detection of anomalous activity across multiple layers of the FMI's infrastructure, which requires an operator to have a baseline profile of the FMI's system activity. Controls should be implemented in a way that will assist in monitoring for, detecting, containing, and analysing anomalous activities should protective measures fail. This may require an operator to introduce more segmentation (covered in further detail below), intermediate checkpoints, and intermediate reconciliations allowing for quicker detection, identification, and repair/recovery from a disruption.

17C.23 An operator should consider segmenting the FMI's networks in a manner that segregates systems and data of varying criticality. This will help the FMI to insulate systems in one segment from a security compromise in other segments. This will, in turn, assist more efficient recovery of the FMIs services because, in the event of a compromise, only affected segments have to be restored, rather than the entire information and communication technology infrastructure and all data sets.

17C.24 An operator should implement protective measures to mitigate risks arising from entities connected to the FMI within its wider ecosystem. The appropriate controls will depend on the risk arising from connected entities and the nature of the relationship with such entities. An operator should ensure that it implements appropriate measures to effectively mitigate risks arising from connected entities, including ensuring the FMI's participation requirements are designed to provide adequate support to its cyber resilience framework.

Detect

17C.25 Cyber-attacks are increasing in frequency and sophistication and are generally stealthy in their execution. Therefore, possessing the capability to spot the signs of

an impending cyber incident and detect a breach is vital to an FMI's cyber resilience. Early warning allows an operator the time to defend against or contain a potential breach, effectively mitigating the negative impact the cyber incident otherwise might have had.

17C.26 An operator should document the normal baseline performance for the FMI's identified essential services and supporting systems, so that any deviation from the baseline can be detected and anomalous activities and events can be flagged for investigation.

17C.27 An operator should ensure that the FMI has the right capabilities in terms of people, processes, and technologies in place to monitor and detect deviations from normal system activity. This includes ensuring:

a) relevant staff are trained to be able to identify and report anomalous activities, events, and incidents; and

b) training be updated regularly to be commensurate with any changes to the FMI's cyber threat environment; and

c) criteria are in place to trigger alerts when anomalous activities occur in the FMI. This should also include thresholds for triggering a cyber incident alert and response process; and

d) controls have the capability to detect cyber-attacks and to isolate the point of corruption; and

e) alert thresholds are defined for the FMI's monitoring and detection systems to trigger and facilitate its incident response plan.

17C.28 Staff members of the operator should be provided with cyber resilience training. Such training should include current cyber threats, attack tactics, and appropriate incident responses. The frequency and content of cyber resilience training should be adjusted according to respective roles and responsibilities, and any additional account permissions or security access the employee might have.

17C.29 An operator should ensure that these detection and monitoring capabilities, as well as the system performance baselines, trigger criteria, and alerts are reviewed, tested, and updated regularly to ensure accuracy in cyber risk screening and remain commensurate with the FMI's cyber threat environment.

17C.30 An operator should ensure that detection capabilities within the FMI also address misuse of access by service providers or other trusted agents, potential insider threats, and other advanced threat activity.

17C.31 An operator should ensure that the detection and monitoring capabilities for the FMI allow for sufficient information collection to support forensic investigation of events and incidents. This includes ensuring that information held in system and data logs is being backed up to a secure location and controls are in place to ensure the logs remain accurate, uncompromised, and free from interference.

17C.32 An operator should ensure analysis of the information collected from the monitoring of systems and user activity is carried out in a timely manner. This analysis should be used to enhance the FMI's detection capabilities, tactics, and incident response process.

17C.33 An operator should conduct security tests on the FMI's internal systems and networks to detect weaknesses that could be exploited by a cyber-attack or leave them exposed to a cyber incident. The tests should be conducted on a regular basis, as well as each time a major change occurs to the cyber threat status of the FMI, such as when an operator implements new systems or technologies. The tests should involve, if deemed necessary, all relevant internal staff and departments that are critical to the cyber resilience of the FMI and relevant third parties.

Respond and recover

17C.34 Response and recovery plans are essential to an operator's ability to return the FMI to business as usual when a cyber incident has occurred. As a result, these plans are also fundamental in ensuring continued stability of the financial system as a whole. It is incumbent upon an operator to have arrangements in place to resume the FMI's essential services as quickly and accurately as can be safely achieved. Post-incident analysis is important in understanding learnings from cyber incidents and integrating them back into the response and recovery plans (see also guidance for Standard 17: 'Operational risk').

17C.35 An operator should have response and recovery plans in place for the FMI, commensurate to the FMI's requirements and its importance to the financial system, to be activated when a cyber incident or breach occurs. These plans should:

a) be based on the aforementioned identification and categorisation of the FMI's essential services and include plans for:

   i) operating in a diminished capacity; and

   ii) safe restoration of systems and services in the order of their relative priority; and

   iii) recovery point objectives; and

   iv) recovery time objectives; and

b) work to avoid or limit as much damage as possible following a cyber incident or breach, while also reducing recovery time and costs; and

c) outline the internal and external stakeholders that must be notified of a cyber incident, when such notification must occur, and what information needs to be included in the notification. The level of stakeholder engagement should be informed by the severity and impact of a cyber incident; and

d) outline the criteria for escalation within an operator and FMI, including to senior management and the board, based on the potential impact of the cyber incident; and

e) include clearly defined roles and responsibilities for all staff involved in cyber incident escalation, response, and recovery, across all teams and departments within an operator and FMI; and

f) be aligned with the FMI's contingency plan (See Standard 17A: 'Contingency plans'), as well as any other relevant plans or policies; and

g) be regularly reviewed and tested, using a range of different scenarios, to ensure their continued effectiveness.

17C.36 An operator should contemplate a wide range of different cyber incident scenarios when formulating the response and recovery plans for the FMI, and in doing so conduct business impact analyses to assess how each scenario would impact the FMI so that an operator can respond accordingly. These impact analyses should be conducted regularly and updated to reflect the ever-evolving cyber threat landscape that the FMI faces.

17C.37 An operator should utilise the FMI's process for triggering cyber incident alerts, outlined under 'Detect', to ensure the right staff are aware of the incident or breach and have the most up-to-date information so that they can respond accordingly. The staff responsible for responding to cyber incidents and breaches should have the required skills and training to address the situation appropriately.

17C.38 An operator should have processes in place that enable the FMI to collate and review information from cyber incidents and testing results, ensure post-incident analysis is conducted to identify root causes of the FMI's cyber security incidents, and integrate its findings back into the FMI's response and recovery plans.

17C.39 We recommend operators develop models to estimate and capture financial losses resulting from cyber incidents. This information should help inform and improve the FMI's overall cyber risk management practices and be useful for information sharing purposes.

Information sharing

17C.40 A crucial component of a collective response to cyber threats is the sharing of information and how quickly that information can be acted upon. In addition to the cyber threat environment, it is also crucial for an operator to understand the adequacy of the FMI's cyber risk mitigation measures through sharing and learning from industry best practice.

17C.41 Operators of FMIs must ensure that the FMI's cyber resilience strategy and cyber resilience framework contains provision for sharing information regarding cyber threats and cyber incidents securely with relevant external stakeholders (including the regulator). Operators of FMIs should also consider participating in cyber security information exchange groups (for example, the Financial Sector Security Information Exchange organised by the National Cyber Security Centre (NCSC)) and collaborate with trusted stakeholders within and outside of the industry. Operators should also meet all regulatory requirements regarding reporting and sharing information on cyber resilience.

17C.42 Information that could be shared includes, but is not limited to, indicators of compromise (IOC), cyber incidents, threats, vulnerabilities, risk mitigation, best practice, and strategic analysis. Sufficiently detailed anonymised data shared on appropriate platforms can help entities to react quickly and appropriately to cyber threats.

17C.43 An operator should plan for information sharing through trusted channels, including collecting and exchanging timely information that could facilitate the detection, response, and recovery of the FMI's systems from cyber incidents. Operators should participate in information sharing groups and collectives to gather, distribute

and assess information about cyber practices, cyber risk, and early warning indicators relating to cyber threats.

17C.44 An operator should determine in the FMI's cyber resilience strategy and cyber resilience framework:

a) which types of information will be shared; and

b) the circumstances under which sharing is permitted; and

c) with whom the information can and should be shared; and

d) how any information provided to an operator via trusted channels should be acted upon.

17C.45 An operator should have in place a process that enables it to access and share information with external stakeholders (for example, the regulator and cyber security agencies) in a timely manner, as well as meet regulatory reporting timeframes, if required. The process for information sharing, especially contact information, should be maintained and updated regularly.

17C.46 We recommend that operators adopt the Traffic Light Protocol[3] to ensure that sensitive information is shared with the correct audience.

External assurance engagement

17C.47 An operator must engage an external party to undertake an assurance review of the FMI's cyber resilience framework at least every two years or otherwise when a cyber incident occurs that that materially impacts, or could materially impact, the FMI's continuing operations. Such review should include assessing:

a) whether the FMI's policies and internal systems are fit for purpose, taking into account its risk profile; and

b) the FMI's compliance with such policies and internal systems.

17C.48 As the FMI's cyber resilience framework must be based on leading internationally recognised standards and guidelines, an operator should consider whether it is appropriate to structure the assurance review on the standards and guidelines used to develop the cyber resilience framework.

17C.49 However, there may be circumstances where it is not reasonable to obtain an external assurance engagement. Examples include circumstances where the cost of the external assurance engagement clearly outweighs the benefit of the review or the internal review can adequately address concerns following a cyber incident described above. If the operator forms the opinion that it is not reasonable to seek an external assurance engagement following such a cyber incident then the operator must explain the rationale for this opinion to the regulator.

[3] For details on what a Traffic Light Protocol entails see: https://www.cert.govt.nz/it-specialists/guides/traffic-light-protocol/

Board of directors and senior management responsibilities

17C.50 Cyber resilience governance is concerned with the overall formation, execution, and evaluation of a cyber risk management approach. Effective and efficient governance is key to the resilience of an FMI. Executed properly, cyber resilience governance allows for rapid and thorough decision-making and information dissemination, which is necessary in managing cyber risk.

17C.51 An operator must ensure its board of directors understand the cyber risk environment the FMI is operating in. This includes approving the FMI's cyber resilience strategy and cyber resilience framework from conception to implementation and reviews these frameworks frequently to ensure their continuing effectiveness in the dynamic cyber threat environment. The expertise required for an operator's board of directors to understand the cyber risk environment could be accessed through experienced in-house staff or external independent organisations.

17C.52 Clearly defined cyber security roles and responsibilities, and fostering a culture in which all FMI staff understand their individual and collective roles in promoting resilience, are integral aspects of an effective cyber resilience framework. The highly interconnected nature of the financial sector means the ability to respond quickly and accurately can be instrumental in preventing the most catastrophic of cyber-attack consequences.

17C.53 An operator should ensure that all staff with cyber resilience-related roles and responsibilities have the skills, knowledge, experience, and resources to perform their required tasks effectively, and are informed and empowered to act in a timely manner.

17C.54 An operator should ensure that the senior executive accountable for the cyber resilience strategy and cyber resilience framework directly reports observance/issues of the cyber resilience of the FMI to the board of directors. When senior management keep the board of directors apprised of the cyber resilience status of the FMI, this should include a plan for future resource allocation, including for both ongoing and forecasted cyber resilience needs.

Culture and awareness

17C.55 An operator should promote an organisational culture that fosters cyber resilience by ensuring that all staff have cyber resilience responsibilities. This includes an operator making the use of clear internal communications and sharing relevant information related to the cyber resilience strategy and cyber resilience framework with all its staff.

17C.56 An operator should build a strong level of awareness of, and commitment to, cyber resilience business-wide. This includes an operator having a process for gathering and analysing cyber threat intelligence as threats emerge and sharing this intelligence with its staff to aid in business-wide situational awareness.

Management of third-party service providers

17C.57 Refer to Standard 17B: 'Critical service providers' for additional requirements regarding third-party service providers.

17C.58 It has become standard practice for organisations to rely on a multitude of third-party service providers (including related parties, like parent companies or subsidiaries) to support core business functions. It is also common for these third-party entities to have access to an organisation's data and internal systems. If used prudently, third-party services may reduce an FMI's cyber risk, especially for those entities that lack cyber expertise. However, the third-party ecosystem provides an environment that makes it easier for cyber criminals to infiltrate an organisation.

17C.59 Extensive use of third-party services increases the difficulty of assessing an FMI's level of cyber resilience and exposure to cyber risk, both for the FMI itself and its regulators. In addition, third parties increasingly rely on other service providers, introducing additional vulnerabilities and threats.

17C.60 An operator must identify and assess the cyber risk associated with third-party service providers and outline how this risk will be managed, this includes complying with the requirements of Standard 17B: 'Critical service providers'.

17C.61 This section of the guidance outlines how an operator should plan, screen, review, and use contracts to manage its (or the FMI's) relationships with third-party service providers and undertake ongoing contract and relationship management to ensure cyber risks arising from third parties are under control.

17C.62 This section also provides high-level recommendations regarding the use of third-party cloud computing service providers.

Process and due diligence

17C.63 An operator should assess the criticality and sensitivity of the activities, data, and processes being outsourced before entering into any outsourcing arrangements, and ensure that any due diligence and ongoing arrangements are commensurate with this assessment.

17C.64 An operator should ensure due diligence procedures include evaluating the third party's ability to meet the cyber resilience requirements of the FMI. The results of such due diligence should be clearly documented before deciding on whether to enter into the arrangement.

17C.65 Operators should use a standard assessment questionnaire to assess cyber resilience during the due diligence process or develop a custom questionnaire according to the FMI's risk appetite and its business requirement.

17C.66 When conducting due diligence on third-party service providers, operators should obtain independent security attestation reports and certifications to provide assurance as to the security posture of prospective third-party service providers.

Contract terms

17C.67 Where possible, an operator should use contracts with third parties to capture cyber security considerations that are commensurate with the FMI's cyber risk appetite. This may include roles and responsibilities of each involved party regarding amongst other things, data access, incident response and communication, business continuity planning, termination, and data portability.

17C.68 Operators should seek to be fully informed about any related subcontracting by third parties that the FMI has an outsourcing arrangement with. An operator could agree to allow a third party to subcontract only when the subcontractors can fully meet the obligations existing between the FMI and their outsourcing service providers.

17C.69 Operators should consider portability and interoperability of their data and applications and include provisions in its outsourcing contracts to avoid vendor lock-in.

Ongoing cyber risk management

17C.70 An operator should consider the cyber risk associated with its third parties when implementing the FMI's cyber resilience strategy and framework. An operator should:

a) clearly identify and document the cyber risk associated with using third-party service providers and update this information on a regular basis; and

b) design and verify security controls to detect and prevent intrusions from third-party connections; and

c) ensure that third-party employee access to the FMI's confidential data is tracked actively, based on the principle of least privilege; and

d) integrate third parties that provide services for the FMI's essential services into the FMI's response plan.

17C.71 An operator should assess the substitutability of the third parties that provide services for the FMI's essential services and include transitioning to alternative service providers or performing essential services in-house in its business continuity plan that is commensurate with the criticality of the services and the FMI's risk appetite.

17C.72 Operators should conduct response and recovery testing with any third-party service providers and use the testing results to improve the FMI's response and recovery plans.

Relationship management

17C.73 An operator should regularly assess the FMI's third-party service providers' cyber security capabilities. The assessment could be achieved through the services providers' self-assessment, an operator's own assessment, or assessment by independent third parties.

17C.74 Operators should obtain assurance of its third-party service providers' cyber resilience capabilities by using tools such as certifications, external audits and/or summary of test reports.

17C.75 An operators should maintain an up-to-date, comprehensive inventory of the FMI's third-party service providers and interconnection with other entities, as well as regularly updating the networking map of its external dependencies.

17C.76 An operator should establish a termination/exit strategy for the third parties that provide services related to the essential services of the FMI.

Outsourcing to cloud service providers

17C.77 If managed prudently, migrating to the cloud presents a number of benefits including geographically dispersed infrastructures, agility to scale more quickly, improved automation, sufficient redundancy, and reduced initial investment costs for individual financial institutions. However, using cloud services brings challenges to assess legal and regulatory obligations, and operators may also run the risk of potentially underinvesting in risk mitigation if the shared tasks are not well articulated and understood. The trend of relying on a narrow set of major cloud service providers also puts concentration risks on the financial system. Therefore, operators should pay special attention when outsourcing to cloud service providers.

17C.78 When considering outsourcing an FMI's activities to cloud service providers, an operator should:

a) inform the regulator if the outsourcing involves the FMI's essential services early in the decision-making process; and

b) evaluate and have a clear understanding of the rationale and the potential impacts of outsourcing to cloud service providers; and

c) assess the potential legal risk, compliance issues and oversight limitations associated with outsourcing to cloud service providers; and

d) assess the jurisdiction risk associated with data stored, processed, and transmitted in the cloud, including data replicated for provision of backup or availability services; and

e) take account of the cloud service provider's adherence to any relevant international standards.

17C.79 An operator should carefully consider the different levels of roles and responsibilities when entering into an agreement with its cloud service provider using the shared responsibility model. An operator may refer to the NCSC's high-level guidance on the shared responsibility model.

17C.80 An operator should consider and make it clear in the outsourcing agreement about how data will be segregated if using a public cloud service provider.

17C.81 The assessment of the design and operating effectiveness of controls within the shared responsibility model (for both provider and an operator) should be commensurate with the impact of the outsourced functions/systems on the FMI.

STANDARD 18: ACCESS AND PARTICIPATION REQUIREMENTS

18.1 Access refers to the ability to use an FMI's services and includes the direct use of the FMI'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. An operator must allow for fair and open access to the FMI's services. An operator should control the risks to which the FMI is exposed by its participants by setting reasonable risk-related requirements for participation in its services, that is, relative to the risks the potential participant might pose to the FMI. An operator should ensure that the FMI's 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 FMI and other participants. An operator must ensure an FMI's participation requirements are clearly stated and publicly disclosed to eliminate ambiguity and promote transparency.

Fair and open access to payment systems, CSDs, SSSs, and CCPs

18.2 Fair and open access to FMI services encourages competition among market participants and promotes efficient and low-cost payment, clearing, and settlement. As an FMI often benefits from economies of scale, there is typically only one FMI, or a small number of FMIs, for a particular market. As a result, participation in an FMI may significantly affect the competitive balance among market participants. In particular, limiting access to an FMI's services may disadvantage some market participants (and their customers), other FMIs (for example, a CCP that needs access to a CSD), and service providers that do not have access to the FMI's services. Further, access to one or more FMIs may play an important role in a market-wide plan or policy for the safe and efficient clearing of certain classes of financial instruments and the promotion of efficient financial markets (including the recording of transaction data). An operator's participation requirements for the FMI must be based on reasonable risk-related participation requirements. However, where an operator is a central bank, access requirements should also promote financial stability considerations. Moreover, open access may reduce the concentrations of risk that may result from highly tiered arrangements for payment, clearing, and settlement.

Risk-related participation requirements

18.3 An operator should always consider the risks that an actual or prospective participant may pose to the FMI and other participants. Accordingly, an operator must establish risk-related participation requirements adequate to ensure that its participants meet appropriate operational, financial, and legal requirements to allow them to fulfil their obligations to the FMI, including the other participants, on a timely basis. Where participants act for other entities (indirect participants), it may be appropriate for an operator to impose additional requirements to ensure that the direct participants have the capacity to do so (see also Standard 19: 'Tiered participation arrangements'). Operational requirements may include reasonable criteria relating to the participant's ability and readiness (for example, its IT capabilities) to use an FMI's services. Financial requirements may include reasonable risk-related capital requirements, contributions to prefunded default arrangements, and appropriate indicators of creditworthiness. Legal requirements

may include appropriate licences and authorisations to conduct relevant activities as well as legal opinions or other arrangements that demonstrate that possible conflict of laws issues would not impede the ability of an applicant (for example, a foreign entity) to meet its obligations to the FMI. An operator also may require participants to have appropriate risk management expertise. If an FMI admits non-regulated entities, an operator should take into account any additional risks that may arise from their participation and design the FMI's participation requirements and risk management controls accordingly.

18.4 An operator must ensure an FMI's participation requirements are justified in terms of the safety and efficiency of the FMI and the markets it serves, are tailored to the FMI's specific risks, are imposed in a manner commensurate with such risks, and are publicly disclosed. Where an operator is a central bank, tailoring of access requirements will also include financial stability considerations. The requirements should be objective and should not unnecessarily discriminate against particular classes of participants or introduce competitive distortions. For example, participation requirements based solely on a participant's size are typically insufficiently related to risk and deserve careful scrutiny. Subject to maintaining acceptable risk control standards, an operator must set requirements that have the least-restrictive impact on access that circumstances permit. However, an operator can consider the degree of regulation of a participant as a factor in assessing the risk associated with participants (including regulation by an overseas regulator). Requirements should also reflect the risk profile of the activity as an FMI may have different categories of participation based on the type of activity. For example, a participant in the clearing services of a CCP may be subject to a different set of requirements than a participant in the auctioning process of the same CCP.

18.5 To help address the balance between open access and risk, an operator should manage the FMI's participant-related risks through the use of risk management controls, risk-sharing arrangements, and other operational arrangements that have the least-restrictive impact on access and competition that circumstances permit. For example, an operator can use credit limits or collateral requirements to help it manage credit exposure to a particular participant. The permitted level of participation may be different for participants maintaining different levels of capital. Where other factors are equal, participants holding greater levels of capital may be permitted less-restrictive risk limits or be able to participate in more functions within the FMI. The effectiveness of such risk management controls may mitigate the need for an operator to impose onerous participation requirements that limit access to the FMI. An operator could also differentiate the FMI's services to provide different levels of access at varying levels of cost and complexity. For example, an operator may want to limit direct participation in the FMI to certain types of entities and provide indirect access to others. Participation requirements (and other risk controls) can be tailored to each tier of participants based on the risks each tier poses to the FMI and its participants.

Monitoring

18.6 An operator should monitor compliance with the FMI's participation requirements on an ongoing basis through the receipt of timely and accurate information. Participants should be obligated to report any developments that may affect their ability to comply with an FMI's participation requirements. An operator should have the authority to impose more-stringent restrictions or other risk controls on an FMI's participant in situations where an operator determines the participant poses

heightened risk to the FMI. For example, if a participant's creditworthiness declines, an operator may require the participant to provide additional collateral or reduce the participant's credit limit. An operator should consider additional reporting requirements for non-regulated participants, and also have clearly defined and publicly disclosed procedures for facilitating the suspension and orderly exit of an FMI's participant that breaches, or no longer meets, the participation requirements of the FMI.

STANDARD 19: TIERED PARTICIPATION ARRANGEMENTS

19.1 Tiered participation arrangements occur when some firms (indirect participants) rely on the services provided by other firms (direct participants) to use the FMI's central payment, clearing, or settlement facilities.

19.2 The dependencies and risk exposures (including credit, liquidity, and operational risks) inherent in these tiered arrangements can present risks to the FMI and its smooth functioning as well as to the participants themselves and the broader financial markets. For example, if an FMI 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 FMI depend on a few direct participants. This will increase the severity of the effect on the FMI 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 FMI. 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, CCPs 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 FMI if there is uncertainty about the liability for indirect participant transactions and how these transactions will be handled in the event of a default.

19.3 The nature of these risks is such that they are most likely to be material where there are indirect participants whose business through the FMI is a significant proportion of the FMI's overall business or is large relative to that of the direct participant through which they access the FMI's services. Normally, 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 an FMI's services. In exceptional cases, however, tiered participation arrangements may involve a complex series of financial intermediaries or agents, which may require an operator to look beyond the direct participant and its immediate customer.

19.4 There are limits on the extent to which an operator, in practice, observe or influence direct participants' commercial relationships with their customers. However, an operator 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 and efficient operation of the FMI. At a minimum, an operator must identify the types of risk that could arise from tiered participation and should monitor concentrations of such risk. If an FMI or its smooth operation is exposed to material risk from tiered participation arrangements, an operator should seek to manage and limit such risk.

Gathering and assessing information on risks arising from tiered participation arrangements

19.5 An operator may be able to obtain information relating to tiered participation through the FMI's own systems or by collecting it from direct participants. An operator must ensure that the FMI's procedures, rules, and contracts with direct participants allow an operator to gather basic information about indirect participants in order to identify, monitor, and manage any material risks to the FMI arising from such tiered

participation arrangements. This information should enable an operator to identify (a) the proportion of activity that direct participants conduct on behalf of indirect participants; (b) direct participants that act on behalf of a material number of indirect participants; (c) indirect participants with significant volumes or values of transactions in the system; and (d) indirect participants whose transaction volumes or values are large relative to those of the direct participants through which they access the FMI.

Understanding material dependencies in tiered participation arrangements

19.6 An operator must identify material dependencies between direct and indirect participants that might affect the FMI. Indirect participants will often have some degree of dependency on the direct participant through which they access the FMI. In the case of an FMI with few direct participants but many indirect participants, it is likely that a large proportion of the transactions processed by the FMI 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. An operator must identify material dependencies of indirect participants on direct participants so that the FMI has readily available information on which significant indirect participants may be affected by problems at a particular direct participant.

19.7 In some cases, issues at an indirect participant could affect the FMI. This is most likely to occur where a large indirect participant accesses an FMI's facilities through a relatively small direct participant. 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 FMI. Operators must therefore identify and monitor the material dependencies of direct participants on indirect participants so that an operator has readily available information on how the FMI may be affected by problems at an indirect participant, including which direct participants may be affected.

Credit and liquidity risks in tiered participation arrangements

19.8 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. An operator is not expected to manage the credit and liquidity exposures between direct and indirect participants, although an operator may have a role in applying credit or position limits in agreement with the direct participant. An operator should, however, have access to information on concentrations of risk arising from tiered participation arrangements that may affect the FMI, allowing an operator to identify indirect participants responsible for a significant proportion of the FMI's transactions or whose transaction volumes or values are large relative to those of the direct participants through which they access the FMI. An operator should identify and monitor such risk concentrations.

19.9 In a CCP, direct participants are responsible for the performance of their customers' financial obligations to the CCP. An operator of the CCP 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 FMI with a potential credit exposure related to an indirect participant's positions, an operator should ensure it understands and manages the exposure the FMI would face. For example, an operator may set participation requirements that require the direct participant, on an operator's request, to demonstrate that it is adequately managing relationships with its customers to the extent that they may affect the FMI. An operator should also consider establishing concentration limits on exposures to indirect participants, where appropriate.

Indirect participation and default scenarios

19.10 Default scenarios can create uncertainty about whether indirect participants' transactions have been settled or will be settled and whether any settled transactions will be unwound. Default scenarios can also raise legal and operational risks for the FMI if there is uncertainty about whether the indirect or direct participant is required to complete the transaction. An operator should ensure that the FMI's rules, procedures, and contracts are clear regarding the status of indirect participants' transactions at each point in the settlement process (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) and whether such transactions would be settled in the event of an indirect or direct participant default. An operator should also ensure that it adequately understands the FMI's direct participants' processes and procedures for managing an indirect participant's default. For example, an operator should know whether the indirect participant's queued payments can be removed or future-dated transactions rescinded and whether such processes and procedures would expose the FMI to operational, reputational, or other risks.

Encouraging direct participation

19.11 Direct participation in an FMI usually provides a number of benefits, some of which may not be available to indirect participants, such as RTGS, exchange-of-value settlement, or settlement in central bank money. Moreover, indirect participants are vulnerable to the risk that their access to an FMI, their ability to make and receive payments and their ability to undertake and settle other transactions is lost if the direct participant, on whom these indirect participants rely, defaults or declines to continue their business relationship. If these indirect participants have large values or volumes of business through the FMI, this may affect the smooth functioning of the FMI. For these reasons, where an indirect participant accounts for a large proportion of the transactions processed by an FMI, an operator should encourage direct participation. For example, an operator may, in some cases, establish objective thresholds above which direct participation would normally be encouraged (provided that the firm satisfies the FMI's access criteria). Setting such thresholds and encouraging direct participation should be based on risk considerations rather than commercial advantage.

Regular review of risks in tiered participation arrangements

19.12 An operator must regularly review risks to which the FMI may be exposed as a result of tiered participation arrangements. If material risks exist, an operator must take mitigating action when appropriate. The results of the review process should be

reported to the board of directors and updated periodically and after substantial amendments to an FMI's rules.

STANDARD 20: FMI LINKS

20.1 A link includes a set of contractual and operational arrangements between two or more FMIs that connect the FMIs directly or through an intermediary. An operator may establish a link between the FMI and a similar type of FMI for the primary purpose of expanding its services to additional financial instruments, markets, or institutions. For example, an investor CSD may be linked to another CSD in which securities are issued or immobilised (referred to as an issuer CSD) to enable a participant in the investor CSD to access the services of the issuer CSD through the participant's existing relationship with the investor CSD. A CCP may be linked to another CCP to enable a participant in the first CCP to clear trades with a participant in the second CCP through the participant's existing relationship with the first CCP. An FMI may also be linked to a different type of FMI. For example, a CCP for securities markets must establish and use a link to a CSD to receive and deliver securities. This standard covers links between CSDs-CSDs, CCPs-CCPs, CSD-CCP links, and links between other classes of FMIs. If an FMI is linked to another FMI, an operator must identify, monitor, and manage its link-related risks. The regulator considers link-related risks to include legal, operational, credit, and liquidity risks. Further, an operator that establishes multiple links should ensure that the risks generated in one link do not affect the soundness of the other links and linked FMIs. Mitigation of such spill-over effects requires the use of effective risk management controls, including additional financial resources or the harmonisation of risk management frameworks across linked FMIs.

Identifying link-related risks

20.2 Before entering into a link arrangement and on an ongoing basis once the link is established, an operator 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 FMIs and the nature of the relationship between them. In a simple case of a vertical link, for example, an FMI may provide basic services to another FMI, such as a CSD that provides securities transfer services to an SSS. Such links typically pose only operational and custody risks. Other links, such as an arrangement in which a CCP provides clearing services to another CCP, may be more complex and may pose additional risk to FMIs, such as credit and liquidity risk. Cross-margining by two or more CCPs may also pose additional risk because the CCPs may rely on each other's risk management systems to measure, monitor, and manage credit and liquidity risk (see Standard 6: 'Margin'). In addition, links between different types of FMIs may pose specific risks to one or all of the FMIs in the link arrangement. For example, a CCP may have a link with a CSD with an SSS for the delivery of securities and settlement of margins. If the CCP poses risks to the CSD, an operator of the CSD should manage those risks. In all cases, an operator must ensure it designs link arrangements such that an operator of each FMI is able to observe the other FMI's compliance with the applicable FMI Standards or relevant overseas standards.

Managing legal risks

20.3 An operator must ensure a link has a well-founded legal basis, in all relevant jurisdictions, that supports the link's design and manages operational, legal, and financial risk to the FMIs involved in the link. 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 Standard 1: 'Legal basis'). For example, this could arise where there is a link between a designated FMI covered by subpart 5 of Part 3 of the Act (providing finality of settlement) and another FMI that is not protected by this subpart. In some jurisdictions, differences in laws may create uncertainties regarding the enforceability of CCP obligations assumed by novation, open offer, or other similar legal device. Differences between New Zealand law and insolvency laws in other jurisdictions may unintentionally give a participant in one CCP a claim on the assets or other resources of the linked CCP in the event of the first CCP's default. To limit these uncertainties, the respective rights and obligations of the linked FMIs and, where necessary, their participants should be clearly defined in the link agreement. The terms of the link agreement should also set out, in cross-jurisdictional contexts, an unambiguous choice of law that will govern each aspect of the link, taking into account the protections for designated FMIs in the Act.

Managing operational risk

20.4 Operators of linked FMIs should provide an appropriate level of information about the FMI's operations to each other in order for each FMI to perform effective periodic assessments of the operational risk associated with the link. In particular, operators 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 Standard 17: 'Operational risk'). Systems and communication arrangements between linked FMIs also should be reliable and secure so that the link does not pose significant operational risk to the linked FMIs. Any reliance by a linked FMI on a critical service provider should be disclosed as appropriate to the other FMI. In addition, an operator of a linked FMI 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 one FMI will not inhibit the smooth functioning of the link, related risk management arrangements, or non-discriminatory access to the link (see Standard 2: 'Governance' and Standard 18: 'Access and participation requirements').

Managing financial risk

20.5 An operator of an FMI that establishes a link with one or more FMIs must identify, monitor, and manage link-related risks, including custody risk. Operators should ensure that they and their participants have adequate protection of assets in the event of the insolvency of a linked FMI or a participant default in a linked FMI. Specific guidance on mitigating and managing these risks in CSD-CSD links and CCP-CCP links is provided below.

CSD-CSD links

20.6 As part of its activities, an operator of an investor CSD may choose to establish a link between that CSD and another CSD. If such a link is improperly designed, the settlement of transactions across the link could subject participants to new or increased risks. In addition to legal and operational risks, linked CSDs and their

participants could also face credit and liquidity risks. For example, an operational failure or default in one CSD may cause settlement failures or defaults in a linked CSD and expose participants in the linked CSD, including participants that did not settle transactions across the link, to unexpected liquidity pressures or outright losses. A CSD's default procedures, for example, could affect a linked CSD through loss-sharing arrangements. Operators of linked CSDs must measure and manage the credit and liquidity risks arising from other linked FMIs. In addition, an operator must ensure any credit extensions between CSDs are covered fully by high-quality collateral and be subject to size limits. Further, some practices deserve particularly rigorous attention and controls. In particular, provisional transfers of securities between linked CSDs should be prohibited.

20.7 An operator must ensure an investor CSD only establishes links with an issuer CSD if the link arrangement provides a high level of protection for the rights of the investor CSD's participants. In particular, the investor CSD should use issuer CSDs that provide adequate protection of assets in the event that the issuer CSD becomes insolvent (see Standard 11: 'Central securities depositories'). In some cases, securities held by an investor CSD can be subject to attachment by the creditors of the CSD or its participants and, as such, can also be subject to freezing or blocking instructions from local courts or other authorities. Further, if an investor CSD maintains securities in an omnibus account at an issuer CSD and a participant at the investor CSD defaults, the investor CSD should not use the securities belonging to other participants to settle subsequent local deliveries of the defaulting participant. An operator should ensure the investor CSD has adequate measures and procedures to avoid affecting the use of securities belonging to non-defaulting participants in a participant-default scenario.

20.8 Furthermore, operators of linked CSDs should have robust reconciliation procedures to ensure that their respective records are accurate and current. Reconciliation is a procedure to verify that the records held by the linked CSDs match for transactions processed across the link. This process is particularly important when three or more CSDs are involved in settling transactions (that is, the securities are held in safekeeping by one CSD or custodian while the seller and the buyer participate in one or more of the linked CSDs) (see also Standard 11: 'Central securities depositories').

Indirect CSD-CSD links

20.9 If an investor CSD uses an intermediary to operate a link with an issuer CSD, an operator of the investor CSD must measure, and manage the additional risks (including custody, credit, legal, and operational risks) arising from the use of the intermediary. In an indirect CSD-CSD link, an investor CSD uses an intermediary (such as a custodian bank) to access the issuer CSD. In such cases, the investor CSD faces the risk that the custodian bank may become insolvent, act negligently, or commit fraud. Although an investor CSD may not face a loss on the value of the securities, the ability of the investor CSD to use its securities might temporarily be impaired. An operator of the investor CSD should measure, monitor, and manage on an ongoing basis its custody risk (see also Standard 16: 'Custody and investment risks') and provide evidence to the regulator when requested that adequate measures have been adopted to mitigate this custody risk. In addition, an operator of the investor CSD must ensure that it has adequate legal, contractual, and operational protections to ensure that its assets held in custody are segregated and transferable (see Standard 11: 'Central securities depositories'). Similarly, an

operator of an investor CSD should ensure that its settlement banks or cash correspondents can perform as expected. In that context, an operator of the investor CSD should have adequate information on the business continuity plans of its intermediary and the issuer CSD to achieve a high degree of confidence that both entities will perform as expected during a disruptive event.

CCP-CCP links

20.10 A CCP may be linked with one or more other CCPs. Although the details of individual link arrangements among CCPs differ significantly because of the varied designs of CCPs and the markets they serve, there are currently two basic types of CCP links: peer-to-peer links and participant links.

20.11 In a peer-to-peer link, a CCP maintains special arrangements with another CCP and is not subject to normal participant rules. Typically, however, the CCPs exchange margin and other financial resources on a reciprocal basis. The linked CCPs 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 CCPs. Risk management between the CCPs is based on a bilaterally approved framework, which is different from that applied to a normal participant.

20.12 In a participant link, one CCP (the participant CCP) is a participant in another CCP (the host CCP) and is subject to the host CCP's normal participant rules. In such cases, the host CCP maintains an account for the participant CCP and would typically require the participant CCP to provide margin, as would be the case for a participant that is not a CCP. An operator of a participant CCP 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 CCP defaults, the participant CCP may not have adequate protection because the participant CCP does not hold collateral from the host CCP to mitigate the counterparty risk posed to it by the host CCP. Risk protection in a participant link is one-way, unlike in a peer-to-peer link. An operator of the participant CCP that provides margin but does not collect margin from another linked CCP should therefore hold additional financial resources to protect its participant CCP against the default of the host CCP.

20.13 Both types of links – peer-to-peer and participant links – may present new or increased risks that should be measured, monitored, and managed by an operator of the CCPs involved in the link. The most challenging issue with respect to CCP links is the risk management of the financial exposures that potentially arise from the link arrangement. Before entering into a link with another CCP, an operator of a CCP must identify and manage the potential spill-over effects from the default of the linked CCP. If a link has three or more CCPs, an operator of each CCP should identify and assess the risks of the collective link arrangement. A network of links between CCPs that does not properly acknowledge and address the inherent complexity of multi-CCP links could have significant implications for systemic risk.

20.14 Exposures faced by one CCP from a linked CCP should be identified, monitored, and managed by an operator with the same rigour as exposures from a CCP's participants to prevent a default at one CCP from triggering a default at a linked CCP. Such exposures should be covered fully, primarily through the use of margin or other equivalent financial resources. In particular, an operator in each CCP in a CCP link arrangement must be able to cover, at least on a daily basis, its current and potential future exposures to the linked CCP and its participants, if any, fully

with a high degree of confidence without reducing the CCP's ability to fulfil its obligations to its own participants at any time (see Standard 6: 'Margin'). Financial resources used to cover inter-CCP current exposures should be prefunded with highly liquid assets that exhibit low credit risk. Best practice is for CCPs to have near real time inter-CCP risk management. However, at a minimum, financial exposures among linked CCPs should be marked to market and covered on a daily basis. Operators also need to consider and address the risks arising from links in designing the CCP's stress tests and calibrating their prefunded default arrangements. Operators of linked CCPs should also take into account the effects that possible contributions to each other's prefunded default arrangements, exchange of margin, common participants, major differences in their risk management tools, and other relevant features may have on their risk management frameworks, especially in relation to the legal, credit, liquidity, and operational risks they face.

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

20.16 An operator of a CCP (the first CCP) will usually have to provide margin to an operator of a linked CCP for open positions. In some cases, an operator of the first CCP may not be able to provide margin collected from its participants to the linked CCP because the first CCP's rules may prohibit the use of its participants' margin for any purpose other than to cover losses from a default of a participant in the first CCP. Alternatively, the first CCP's legal or regulatory requirements may not permit such reuse of its participants' collateral. As such, an operator of the first CCP would need to use alternative financial resources to cover its counterparty risk to the linked CCP, which would be normally covered by margin. If a CCP is allowed to reuse its participants' collateral to meet an inter-CCP margin requirement, such collateral provided by the first CCP must be unencumbered and its use by the linked CCP in the event of the default of the first CCP should not be constrainable by actions taken by the participants of the first CCP. The credit and liquidity risk arising from the reuse of margin should be adequately mitigated by the CCPs. This can be achieved through segregation, protection, and custody of margin exchanged between CCPs in a manner that allows for its swift and timely return to the CCP in case of a decrease in the exposures and that allows for supplemental margin (and, if necessary, supplemental default fund contributions) needed to cover the counterparty risk between the linked CCPs to be charged directly to the participants who use the link service, if applicable.

20.17 Operators of linked CCPs 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 CCP holds to address other risks. The most direct way to achieve this outcome is for CCPs not to participate in each other's default funds, which may in turn mean that the CCP will need to provide additional margin. However, in arrangements in which CCPs have

agreed, consistent with their regulatory framework, to contribute to each other's default funds, the linked CCPs should assess and mitigate the risks of making such contributions via specific conditions. In particular, funds used by a CCP to contribute to another CCP's default fund must represent prefunded additional financial resources and must not include resources used by the CCP 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 CCP to mitigate the counterparty risk presented by its participants. An operator of the contributing CCP should further ensure that any consequent exposure of its own participants to the risk of a participant default in the linked CCP is fully transparent to and understood by its participants. The contributing CCPs may, for example, consider it appropriate to ensure the default fund contribution is made only by those of its participants that use the link, if applicable. Moreover, we expect that the resources provided by one CCP to another are held in such a way that they are ring-fenced from other resources provided to that CCP. 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 as acceptable collateral in this case. Finally, in case of a participant default in the first CCP, the use of the linked CCP's contribution to the default fund of the first CCP could be restricted or limited. For example, the linked CCP's contribution to the default fund could be put at the bottom of the first CCP's default waterfall.

20.18 Link arrangements between CCPs will expose each CCP to sharing in potentially uncovered credit losses if the linked CCP's default waterfall has been exhausted. For example, a CCP may be exposed to loss mutualisation from defaults of a linked CCP's participants. This risk will be greater to the extent that the first CCP is unable directly to monitor or control the other CCP's participants. Such contagion risks can be even more serious in cases where more than two CCPs are linked, directly or indirectly, and a CCP considering such a link should satisfy itself that it can manage such risks adequately. An operator of each CCP 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. CCPs 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, operators may need to increase financial resources to address this risk.

20.19 Any default fund contributions or allocation of uncovered losses should be structured to ensure that (a) no linked CCP is treated less favourably than the participants of the other CCP; and (b) each CCP's contribution to the loss sharing arrangements of the other is no more than proportionate to the risk the first CCP poses to the linked CCP.

STANDARD 21: EFFICIENCY AND EFFECTIVENESS

21.1 An operator must ensure an FMI is operated efficiently and effectively in meeting the requirements of the FMI's participants and the markets it serves, while also maintaining appropriate standards of safety and security as outlined in the applicable FMI standards or relevant overseas standards. "Efficiency" refers generally to the resources required by the FMI to perform its functions, while "effectiveness" refers to whether the FMI is meeting its intended goals and objectives. An FMI that operates inefficiently or functions ineffectively may distort financial activity and the market structure, increasing not only the financial and other risks of an FMI's participants, but also the risks of their customers and end users. If an FMI is inefficient, a participant may choose to use an alternate arrangement that poses increased risks to the financial system and the broader economy. The primary responsibility for promoting the efficiency and effectiveness of an FMI belongs to its owners and operators.

Efficiency

21.2 Efficiency is a broad concept that encompasses what an operator decides the FMI will do, how it does it, and the resources required. An FMI's efficiency depends partly on an operator's choice of a clearing and settlement arrangement (for example, gross, net, or hybrid settlement; real time or batch processing; and novation or guarantee scheme); operating structure (for example, links with multiple trading venues or service providers); scope of products cleared, settled, or recorded; and use of technology and procedures (for example, communication procedures and standards). In designing an efficient FMI, an operator should also consider the practicality and costs for the FMI's participants, their customers, and other relevant parties (including other FMIs and service providers). Furthermore, an operator should ensure the FMI's technical arrangements are sufficiently flexible to respond to changing demand and new technologies. Fundamentally, an FMI should be designed and operated to meet the needs of its participants and the markets it serves. An FMI's efficiency will ultimately affect the use of the FMI by its participants and their customers as well as these entities' ability to conduct robust risk management, which may affect the broader efficiency of financial markets.

21.3 Efficiency also involves cost control. An operator of an FMI should establish mechanisms for the regular review of the FMI's efficiency, including its costs and pricing structure. An operator should control the FMI's direct costs, such as those stemming from transaction processing, money settlement, and settlement-entry preparation and execution. An operator also should consider and control its indirect costs. These include infrastructure, administrative, and other types of costs associated with operating the FMI. Some indirect costs (and risks) may be less apparent. For example, an operator may need to consider the FMI's participants' liquidity costs, which include the amount of cash or other financial instruments that a participant must provide to the FMI, or other parties, in order to process its transactions, and the opportunity cost of providing such assets. An FMI's design has a significant impact on the liquidity costs borne by participants, which, in turn, affect the FMI's costs and risks. Cost considerations, however, should always be balanced against appropriate standards of safety and security as outlined in the standards. An operator should control the FMI's direct costs, such as those stemming from transaction processing, money settlement, and settlement-entry preparation and execution. An operator also should consider and control its indirect costs. These include infrastructure, administrative, and other types of costs associated with

operating the FMI. Some indirect costs (and risks) may be less apparent. For example, an operator may need to consider the FMI's participants' liquidity costs, which include the amount of cash or other financial instruments that a participant must provide to the FMI, or other parties, in order to process its transactions, and the opportunity cost of providing such assets. An FMI's design has a significant impact on the liquidity costs borne by participants, which, in turn, affect the FMI's costs and risks. Cost considerations, however, should always be balanced against appropriate standards of safety and security as outlined in applicable FMI standards or relevant overseas standards.

21.4 Competition can be an important mechanism for promoting efficiency. Where there is effective competition and participants have meaningful choices among FMIs, such competition may help to ensure that FMIs are efficient. Operators should ensure, however, that they adhere to appropriate standards of safety and security as outlined in applicable FMI standards or relevant overseas standards. Both private and central bank operators of FMIs should make use of market disciplines, as appropriate, to promote efficiency in the FMI's operations. For example, an operator could use competitive tendering to select service providers. Where competition may be difficult to maintain because of economies of scale or scope, and an FMI therefore enjoys some form of market power over the service it provides, the regulator or other relevant agencies (such as the Commerce Commission) may monitor the costs imposed on the FMI's participants and the markets it serves.

Effectiveness

21.5 An FMI is effective when it reliably meets its obligations in a timely manner and achieves the public policy goals of safety and efficiency for participants and the markets it serves. In the context of oversight and auditing, an FMI's effectiveness may also involve meeting service and security requirements. To facilitate assessments of effectiveness, an operator must have clearly defined goals and objectives for the FMI that are measurable and achievable. For example, an operator should set minimum service-level targets (such as the time it takes to process a transaction), risk management expectations (such as the level of financial resources it should hold), and business priorities (such as the development of new services). An operator should establish mechanisms for the regular review of the FMI's effectiveness, such as periodic measurement of its progress against its goals and objectives.

STANDARD 22: COMMUNICATION PROCEDURES AND STANDARDS

22.1 The ability of participants to communicate with an FMI in a timely, reliable, and accurate manner is key to achieving efficient payment, clearing, and settlement. An FMI's adoption of internationally accepted communication procedures and standards for its core functions can facilitate the elimination of manual intervention in clearing and settlement processing, reduce risks and transaction costs, improve efficiency, and reduce barriers to entry into a market. Therefore, an operator must ensure the FMI uses relevant internationally accepted communication procedures and standards to ensure effective communication between the FMI and its participants, their customers, and others that connect to the FMI.

Communication procedures

22.2 An operator must ensure the FMI uses internationally accepted communication procedures. These procedures should facilitate effective communication between the FMI's information systems, and those of its participants, their customers, and others that connect to the FMI (such as third-party service providers and other FMIs). Standardised communication procedures (or protocols) provide a common set of rules across FMIs and other systems for exchanging messages. These rules allow for a broad set of systems and institutions in various locations to communicate efficiently and effectively. Reducing the need for intervention and technical complexity when processing transactions can help to reduce the number of errors, avoid information losses, and ultimately reduce the resources needed for data processing by the FMI, its participants, and markets generally.

Communication standards

22.3 An operator must ensure the FMI uses internationally accepted communication standards. These can include standardised messaging formats and reference data standards for identifying financial instruments and counterparties. The use of internationally accepted standards for message formats and data representation will generally improve the quality and efficiency of the clearing and settlement of financial transactions.

Cross-border considerations

22.4 An operator must ensure that an FMI conducting payment, clearing or settlement activities across borders uses internationally accepted communication procedures and standards. An FMI that, for example, settles a chain of transactions processed through multiple FMIs or provides services to users in multiple jurisdictions should use internationally accepted communication procedures and standards to achieve efficient and effective cross-border financial communication. Furthermore, adopting these communication procedures can facilitate interoperability between the information systems or operating platforms of FMIs in different jurisdictions, which allows market participants to obtain access to multiple FMIs without facing technical hurdles (such as having to implement or support multiple local networks with different characteristics). An FMI that operates across borders should also be able to support and use well-established communication procedures, messaging standards, and reference data standards relating to counterparty identification and

securities numbering processes. For example, relevant standards promulgated by the International Organization for Standardization should be carefully considered and adopted by an FMI.

STANDARD 23: DISCLOSURE OF RULES, KEY PROCEDURES, AND MARKET DATA

23.1 An operator must provide sufficient information to the FMI's participants and prospective participants to enable them to identify clearly and understand fully the risks of participating in the FMI. This disclosure is in addition to disclosure that is required under Standard 23B: 'Notifying the regulator'. To achieve the above objective, an operator should adopt and disclose written rules and procedures that are clear and comprehensive and that include explanatory material written in plain language so that participants can fully understand the FMI's design and operations, their rights and obligations, and the risks of participating in the FMI. An FMI's rules, procedures, and explanatory material need to be accurate, up-to-date, and readily available to all current and prospective participants. Moreover, an operator must disclose to the FMI's participants and the public information on its fee schedule and basic operational information.

Rules and procedures

23.2 An operator must adopt clear and comprehensive rules and procedures that are publicly disclosed. An FMI's rules and procedures are typically the foundation of the FMI and provide the basis for participants' understanding of the risks they incur by participating in the FMI. As such, an operator must ensure relevant rules and procedures include clear descriptions of the FMI's design and operations, as well as the FMI's and participants' rights and obligations, so that participants can assess the risk they would incur by participating in the FMI. They must clearly outline the respective roles of participants and the FMI as well as the rules and procedures that will be followed in routine operations and non-routine, though foreseeable, events, such as a participant default (see Standard 13: 'Participant-default rules and procedures').

23.3 In addition to disclosing all relevant rules and key procedures, an operator should have a clear and fully disclosed process for proposing and implementing changes to its rules and procedures, and for informing participants and the regulator of these changes. Similarly, the rules and procedures must clearly disclose the degree of discretion that an operator can exercise over key decisions that directly affect the operation of the FMI, including in crises and emergencies (see also Standard 1: 'Legal basis', Standard 2: 'Governance', and Standard 17A: 'Contingency planning'). For example, an FMI's procedures may provide for discretion regarding the extension of operating hours to accommodate unforeseen market or operational problems. An operator should also have appropriate procedures to minimise any conflict-of-interest issues that may arise when an operator is authorised to exercise its discretion.

Participants' understanding of rules, procedures, and risks

23.4 Participants bear primary responsibility for understanding the rules, procedures, and risks of participating in an FMI as well as the risks they may incur when the FMI has links with other FMIs. An operator, however, must provide all documentation, training, and information necessary to facilitate participants' understanding of the FMI's rules and procedures and the risks they face from participating in the FMI. New participants must receive training before using the FMI, and existing

participants should receive, as needed, additional periodic training. An operator should disclose to each individual participant the 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 FMI. Other relevant information that should be disclosed to participants, but typically not to the public, includes key highlights of the FMI's business continuity arrangements.

23.5 An FMI 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, procedures, and risks of participation. In such cases, an operator should take steps to rectify any perceived lack of understanding by the participant and take other remedial action necessary to protect the FMI 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, an operator should notify the appropriate regulatory, supervisory, and oversight authorities.

Fees and other material costs to participants

23.6 An operator must disclose the FMI's fees at the level of the individual services it offers as well as its policies on any available discounts to the public. An operator must provide clear descriptions of priced services for comparability purposes. In addition, an operator should disclose information on the system design, as well as technology and communication procedures that affect the costs of operating the FMI to the public. These disclosures collectively help participants evaluate the total cost of using a particular service, compare these costs to those of alternative arrangements, and select only the services that they wish to use. For example, HVPSs typically have higher values and lower volumes than retail payment systems, and, as a result, processing costs can be less important to participants than the costs of providing liquidity to fund payments throughout the day. The FMI's design will influence not only how much liquidity participants need to hold in order to process payments but also opportunity costs of holding such liquidity. An operator should provide timely notice to participants and the public of any changes to services and fees.

23.7 Other relevant information that could be disclosed to participants and, more generally, the public could include general information on the FMI's full range of activities and operations, such as the names of direct participants in the FMI, key times and dates in FMI operations, and its overall risk management framework (including its margin methodology and assumptions). An operator also should disclose the FMI's financial condition, financial resources to withstand potential losses, timeliness of settlements, and other performance statistics to participants and more generally to the public. With respect to data, an operator must disclose basic data on transaction volumes and values. This should be updated at least annually or more often if the basic data is not representative of the FMI's current position.

Forms of disclosure

23.8 An operator should make the relevant information and data it discloses as set forth in Standard 23: 'Disclosure of rules, key procedures, and market data' (and this guidance) readily available through generally accessible media, such as the internet, in a language commonly used in financial markets in addition to the

domestic language(s) of the jurisdiction in which the FMI is located. The data should be accompanied by robust explanatory documentation that enables users to understand and interpret the data correctly.

STANDARD 23A: DISCLOSING COMPLIANCE WITH THE FMI STANDARDS

23A.1 An operator should provide a comprehensive narrative disclosure for each relevant standard, including the key elements listed in the assessment methodology provided at Annex A under each requirement. The purpose of this disclosure is to provide transparency over an FMI's arrangements to allow a broad audience, including participants, prospective participants, the market and other relevant stakeholders to understand an operator's compliance with each relevant standard, and in doing so, promote a sound and efficient financial system. This disclosure includes an overview of an operator's and FMI's governance, operations, and risk management framework.

23A.2 We expect that charts and diagrams are included wherever they aid the public's understanding of the information provided in the disclosure. All charts and diagrams should be accompanied by a description that enables them to be easily understood.

23A.3 An operator should not refer to or quote rules or regulations as its substantive response to the disclosure framework. As a supplement to a response, however, an FMI may indicate where relevant rules or regulations may be found.

23A.4 When addressing the timing of events, an operator should disclose relative to the local time zone(s) where the FMI is located and New Zealand Daylight Time or New Zealand Standard Time as applicable.

23A.5 The narrative should provide sufficient detail and context to enable the public to understand the FMI's approach to compliance with each standard.

23A.6 For the disclosure to correctly reflect the FMI's current rules, procedures, and operations, an operator must update its disclosure following material changes to the FMI or operating environment.

23A.7 In addition to updating the disclosure for any material changes, an operator must perform a comprehensive review of its responses at least every two years to ensure that the disclosure remains up to date.

23A.8 An operator should make sure its responses in the disclosure are easily available online.

STANDARD 23B: NOTIFYING THE REGULATOR

23B.1 Standard 23B is largely based on section 412 of the Financial Markets Conduct Act 2013 and is also intended to mirror equivalent breach reporting guidance for banks issued by the RBNZ.

Contravention or potential contravention of the Act

When an FMI 'may have contravened'

23B.2 In some situations, an operator may become aware of facts suggesting a contravention may have, or may be, occurring. An operator may not be able to make a determination with sufficient certainty that this contravention has occurred, or is occurring. An operator is expected to treat, and report, a possible contravention in the same way as it would an actual contravention. Incomplete knowledge around the potential contravention is not a reason to delay reporting to the regulator.

When an FMI is 'likely to contravene'

23B.3 The word 'likely' is expected to be interpreted broadly, in line with its usual meaning. If a contravention is expected, or considered probable, it should be reported under the 'likely to contravene' criterion. These considerations should be based on the facts available to an operator as it becomes aware of the potential contravention.

23B.4 An operator may consider any remedial action that it can take to reduce the likelihood of the potential contravention. If an operator is confident that it can take remedial action that will entirely avoid the contravention, then an operator does not have to report it as a likely contravention.

Assessing a 'material contravention'

23B.5 A material contravention includes (but is not limited to) a contravention that raises substantive concerns around risk management or governance, or any contravention that substantively increases the risks to the operation of the FMI.

23B.6 In particular, a contravention that is symptomatic of a serious control weakness, even if it has not resulted in actual adverse outcomes, should be considered a material contravention.

23B.7 Factors impacting on the materiality of contraventions include:

a) the impact of the contravention on the FMI's essential services; and

b) the extent to which the contravention could result in financial consequences to the New Zealand financial system or to participants; and

c) whether the contravention was negligent, reckless, or intentional; and

d) the extent to which any matter may mislead or deceive the regulator; and

e) the extent to which any matter could have a significant adverse impact on an operator's or the FMI's reputation; and

f) how long the contravention lasted or is expected to continue; and

g) whether the contravention is an isolated incident, or part of a recurring pattern of breaches in relation to a matter that is of the same nature; and

h) the extent to which the contravention or likely contravention indicates that the FMI's internal control and compliance frameworks are inadequate.

23B.8 Where a contravention is an isolated incident that neither impairs an operator's ability to provide essential services nor is of interest to an FMI's participants or the wider public, it should not be considered as material. However, in cases of doubt an operator should err on the side of caution and report the contravention.

Timing of reporting to the regulator

23B.9 The standard requires an operator to notify the regulator as soon as possible if there has been, or is likely to be, an outage. 'As soon as possible' means immediately or without delay, ideally as an operator and/or FMI becomes aware of the outage and, at a maximum, within two hours after the occurrence of the outage. This allows the regulator to take action or respond to media or participant enquiries as appropriate.

23B.10 The regulator does not expect the initial notification to contain details about the cause and consequences of the event if they are not known at the time. An operator will likely need to engage with the regulator multiple times as an operator becomes aware of more details about the cause and consequences of the event. An operator should not wait until the cause or consequence to become apparent before notifying the regulator.

23B.11 Following resolution of the outage, the regulator should be informed of how and when the event was resolved. The regulator should also be informed of the results of any post-event analysis such as identification of any root causes or systemic changes necessary to prevent recurrences.