



Financial Infrastructure Report

2017

Contents

ABBREVIATIONS 4

SUMMARY 5

RISKS AND VULNERABILITIES 7

Cyberattacks comprise a serious threat to the financial infrastructure 8

Operational risk in the financial system will be heightened until the VPC system has been changed 10

The Swedish securities market needs a long-term strategy 11

Continuity and capacity for recovery need to be strengthened 12

Central counterparties' increased importance means that they need to develop their risk management and preparedness 15

ARTICLE – The board of directors' responsibility in an infrastructure company 17

ARTICLE – New framework for taking care of central counterparties with financial problems 19

APPENDIX 21

The Riksbank's oversight of the financial infrastructure 21

Foreword

The financial infrastructure consists of infrastructural systems through which payments are made and payments and transactions with financial instruments are managed. This infrastructure makes it possible for individual households, companies and authorities to make and receive payments in a safe and efficient manner. It also makes it possible to safely and efficiently pay for and deliver shares, debt securities and other financial instruments traded on the financial markets.¹

The financial infrastructure thereby plays a central role in the financial system and is necessary for its functioning. This means that problems arising in the financial infrastructure can have serious negative consequences for the financial system, with potentially substantial costs to society as a result. It is thus of great importance for the stability of the financial system that the financial infrastructure functions in a safe and efficient way.

The Riksbank oversees the financial infrastructure with the objective of identifying and analysing the sources of risks and efficiency losses, and acts to reduce these. The starting point for this work is the Riksbank's responsibility for safeguarding financial stability.

The Financial Infrastructure Report presents the Riksbank's assessment of the stability and efficiency of Sweden's financial infrastructure. The report also highlights the risks and vulnerabilities that the Riksbank deems may lead to disruptions in the financial system. The report also contains two articles. The first article emphasises that all risk management is ultimately dependent on good governance and management, and illustrates the Riksbank's expectations of management in the infrastructure systems. The second article deals with the growing safety net for the management of serious financial problems in an infrastructure company – so-called recovery and resolution. Above all, it describes the European Commission's proposals for the recovery and resolution of central counterparties.

The report is aimed at infrastructure companies in the financial infrastructure, their participants, authorities in Sweden and abroad, the Riksdag and other interested parties. By publishing its assessments, the Riksbank wishes to encourage continual improvements to benefit the financial infrastructure and thus the financial stability of Sweden. The report is issued once per year and is available from the Riksbank's website, www.riksbank.se. This year's report takes into account data available until 31 March 2017.

Stockholm, 31 March 2017

Kasper Roszbach
Head of Department,
The Riksbank's Financial Stability Department

¹ For more information on the financial infrastructure in Sweden, see *The Swedish Financial Market 2016*. Sveriges Riksbank.

Abbreviations

BIS – Bank for International Settlements

CLS – Continuous Linked Settlement

CPMI – Committee on Payments and Market Infrastructures

CSDR – Central Securities Depositories Regulation

EMIR – European Market Infrastructure Regulation

IOSCO – International Organization of Securities Commissions

LCH. Clearnet – London Clearing House

OTC – Over the Counter

PFMI – Principles for Financial Market Infrastructures

SWIFT – Society for Worldwide Interbank Financial Telecommunication

T2S – Target2-Securities

Summary

On the whole, the Riksbank considers the financial infrastructure in Sweden to be well-functioning.² However, there are risks and vulnerabilities in it that could lead to disruptions in the financial system. The Riksbank would primarily like to emphasise two operational risks:

Cyberattacks comprise a serious threat to the financial infrastructure

A comprehensive attack could result in central financial services, which are a precondition for a smoothly-functioning economy, becoming unavailable. Cyberattacks can be characterised by the attacker, a hacker, is acting with the aim of causing harm, stealing information or conducting extortion. The attacker is often persistent and acts in a changeable manner, making it particularly difficult for the attacked to defend itself. In recent years, serious attacks have been made against financial institutions and cyber threats are therefore receiving increasing attention from authorities and other participants in the financial system, both in Sweden and internationally.

Outsourcing of IT services is present in the financial infrastructure, both externally to other suppliers and within particular corporate groups. This poses special challenges for buyers and their ability to maintain resilience against cyberattacks. A hacker can attack outsourced operations with the aim of thereby accessing core operations. This risk exists regardless of the outsourced operations' significance for core operations in general. Consequently, particularly regarding the outsourcing of IT and data communication services, the starting point should be that all suppliers are to be subject to the same high security requirements. Over the year, all infrastructure systems that the Riksbank oversees have worked on strengthening their resilience against cyberattacks.

The operational risk in the financial system will be increased until Euroclear Sweden has replaced the VPC system

Since 2013, the Riksbank has repeatedly pointed out that Euroclear Sweden needs to replace its IT system for securities settlement, the VPC system. Keeping the outdated system would entail high and rising risks due to the system's age and high level of complexity, which makes it difficult to change. In 2016, Euroclear Sweden started a project aimed at exchanging the VPC system for a completely new system. However, at the end of the year, it became clear that it would not be possible to implement the system changeover in time to allow Euroclear Sweden to comply with the new requirements of the EU regulation CSDR. Euroclear Sweden therefore decided to postpone the system changeover and instead carry out adjustments to CSDR in the old VPC system, despite the risks this would entail. The Riksbank deems that the level of operational risk in the financial system will remain heightened as long as the old VPC system is in use. In addition, making changes to the VPC system increases the risk of disruptions to daily operations. Euroclear Sweden therefore needs to ensure that the adjustment to CSDR does not affect the continuity or reliability of daily operations. In addition to this, the Riksbank considers it important that Euroclear Sweden, together with other market participants, adopts a long-term strategy for the Swedish securities market, so that it can continue to offer relevant services to investors and issuers. As an example, this would include the consequences of a possible future Swedish connection to the European platform for securities settlement in central bank money, TARGET2-Securities (T2S). The Riksbank considers that the Swedish Bankers' Association, as mouthpiece for the Swedish securities market, should urgently examine the question of Sweden joining T2S. If the Swedish market were to advocate a Swedish connection to T2S, the Riksbank would take a stand on whether or not the Swedish krona should be connected to T2S.³

² The infrastructure systems that are included in the Riksbank's oversight are: The Riksbank's payment system for account transfers RIX, Euroclear Sweden AB's settlement system for securities (the VPC system), Nasdaq Clearing AB's central counterparty system for financial derivatives, commodity derivatives and repos and Bankgirocentralen BGC AB's payment system for clearing retail payments.

³ Following recommendations from the Swedish securities market, the Swedish Bankers' Association decided, in December 2011, to not recommend the Swedish krona to be connected to T2S for settlement of securities transactions in Swedish kronor. However, in its

In addition to these risks, the Riksbank also considers that:

The financial market infrastructures need to continue to develop their contingency procedures as well as plans for recovery and orderly wind-down

All systems have contingency solutions in place. For the RIX system, which has a central function in the financial system, these contingency procedures need to be exceptionally robust according to international standards (PFMI).⁴ The work of strengthening the RIX system's contingency procedures therefore needs to be started as planned in 2017.⁵ Nasdaq Clearing has significantly developed its recovery plan. However, the Riksbank considers that this work must continue so that the plan is in line with the international standards which the approaching legislation is based on. These international standards also require that infrastructure companies not run by central banks have plans for how critical services can be wound down with the least possible negative impact on society and have enough capital to carry out their plans. Euroclear Sweden, Nasdaq Clearing and Bankgirot need to develop their plans to ensure that they are able to conduct orderly wind-downs. The Riksbank's calculations show that Bankgirot has significantly less capital in relation to its operational costs than the other systems and can barely cover the minimum requirement of six months' costs. The Riksbank has therefore requested Bankgirot to ensure that it has enough capital to manage an orderly wind-down.

Central counterparties need to develop risk management and improve preparedness, for example by having good liquidity preparedness in minor currencies

Central counterparties enter into their participants' agreements as counterparties and are therefore exposed to major credit and liquidity risks that could affect the stability of the rest of the financial system. Central counterparties have also increased their significance for financial stability as increasing numbers of transactions are going through these. The Riksbank therefore considers it important that the Swedish central counterparty Nasdaq Clearing continues to develop its methods for managing liquidity risks in line with the international guidance currently being developed. In addition, the Riksbank considers it important that foreign central counterparties with operations in Swedish kronor, primarily LCH.Clearnet and EuroCCP, have good liquidity preparedness in Swedish kronor, regardless of the krona's relative importance to these overseas counterparties.

decision, the Association noted that the Swedish banks were fundamentally positive towards T2S and that the question should be examined again at an appropriate future point.

⁴ See CPMI-IOSCO Principles for financial market infrastructures (PFMI), Principle 17.

⁵ In *Financial Infrastructure 2014* and *Financial Infrastructure 2015*, the Riksbank called attention to the importance of RIX starting work on an improved contingency procedure. It remains important to ensure that the risk of an IT incident does not affect the different RIX operating sites. An improved continuity solution would reduce the consequences of potential incidences.

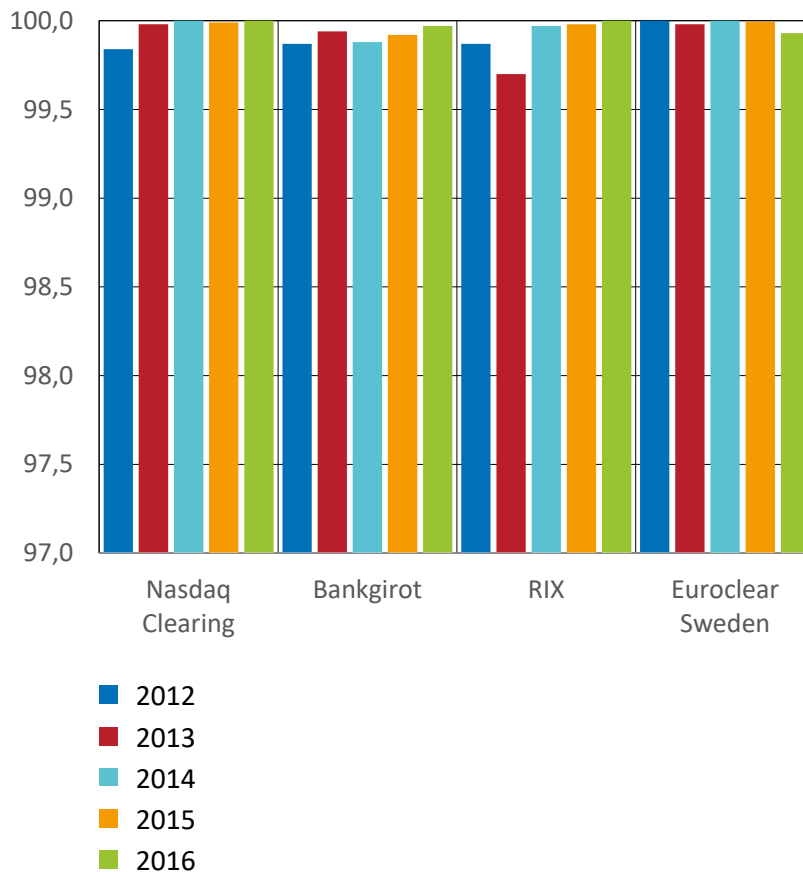
Risks and vulnerabilities

The Riksbank's oversight of the financial infrastructure shows that it works well on the whole, but that operational risk is heightened

The Riksbank's oversight of the financial infrastructure shows that it works well on the whole. All four infrastructure systems that the Riksbank oversees comply to a large extent with CPMI-IOSCO's international standards⁶, which entail high requirements for risk management and resilience to disruptions. All four infrastructure systems have also had good availability over the year (see Chart 1). This means that it has been possible to execute the great majority of all payments and securities transactions on time. The systems have also made several improvements.

Chart 1. Availability of the Swedish systems

Per cent



Sources: Bankgirot, Euroclear Sweden, Nasdaq Clearing and the Riksbank

⁶ The international standards referred to in this report are the CPMI-IOSCO Principles for financial market infrastructures, the CPMI-IOSCO Disclosure Framework and Assessment Methodology as well as further guidance on the principles published by CPMI or CPMI-IOSCO.

Follow-up of issues from Financial Infrastructure 2016

In Financial Infrastructure report 2016, the four Swedish systems were urged to take measures. A brief description of what the systems have done regarding some of these measures is given below.

- All systems have been working actively to complement and strengthen their cybersecurity
- All systems – partly in collaboration with each other – have also started an analysis of the consequences of a bank entering into resolution.
- Nasdaq Clearing, Bankgirot and Euroclear Sweden have developed respective recovery plans.
- RIX has improved its method of monitoring its participants and analysed the risks of indirect participation.

The Riksbank's oversight focuses on identifying risks and vulnerabilities in the financial infrastructure systems (see the appendix *The Riksbank's oversight of the financial infrastructure*). The risks and vulnerabilities that the Riksbank deems are greatest at present are presented below.

Cyberattacks comprise a serious threat to the financial infrastructure

The financial infrastructure consists of IT systems that are becoming increasingly interconnected. This has created new possibilities, such as faster and more efficient mediation of payments, but also means that an attack on a participant's IT system, a so-called cyberattack, can more easily spread to other systems. For example, a cyberattack could involve a stoppage in a bank's operations or that systems enabling payments are put out of action or lose their reliability because information has been manipulated.

Cyberattacks are characterised by a hacker acting deliberately, persistently and with variations, making it particularly difficult for an attacked system to defend itself. In recent years, serious cyberattacks against participants in the financial system have been carried out and cyber threats are therefore receiving increasing attention from authorities and other participants in the financial system, both in Sweden and internationally. For example, in 2016, CPMI-IOSCO prepared supplementary guidance on cybersecurity.⁷ This guidance is an addition to PFMI that the Riksbank uses as a basis for its oversight of the financial infrastructure. The addition describes how financial market infrastructures shall work to maintain their resilience towards cyberattacks. In two reports in 2016, the Riksbank also drew attention to how important it is that financial market infrastructures implement a strategy and a framework to protect themselves from cyberattacks.⁸ Protection from cyberattacks shall be considered by corporate management and the board of directors and in the strategic governance of operations.⁹

Infrastructure companies' work on preventing cyberattacks

Over the year and using CPMI-IOSCO's guidance as a starting point, the Riksbank's system for large-value payments (RIX) has prepared a programme of measures to complement and strengthen work on cybersecurity for the RIX system. Nasdaq Clearing has also prepared such a programme of measures, partly as a consequence of the conclusions that

⁷ Guidance on cyber resilience for financial market infrastructures, Committee on Payments and Market Infrastructures Board of the International Organization of Securities Commissions, 2016.

⁸ See *Financial Infrastructure 2016* and *Financial Stability Report 2016:1*. Sveriges Riksbank.

⁹ Continual training of staff, mandatory tests of new software and hardware before installation, identification of critical information and critical IT systems, continual international monitoring and cooperation with customers, suppliers and authorities are examples of how businesses' preparedness to counteract cyber threats can be strengthened.

Finansinspektionen has drawn from various matters concerning sanctions.¹⁰ Since 2016, Bankgirot has initiated a number of projects for the better management of cyber threats, for example by carrying out special self-assessments and requirements analyses. Euroclear Sweden is also actively conducting work on strengthening its cybersecurity and launched a comprehensive programme in this area in 2016. The programmes and activities initiated by RIX, Nasdaq Clearing, Bankgirot and Euroclear Sweden cover both preventive measures and measures aimed at minimising damage and enabling the recovery of operations.

Another example of work being conducted to counteract and minimise the damage from cyberattacks is the programme of measures¹¹ launched in spring 2016 by SWIFT¹². This programme of measures started as a consequence of the attack on Bangladesh's central bank in early 2016.¹³ The attack was directed against the central bank's internal IT system that sends payment orders on to SWIFT's network and resulted in it being possible to execute unauthorised payments in large amounts. The aim of SWIFT's programme of measures is to increase the security beyond its own network by requiring SWIFT's participants to increase the security of their own IT environments connected to SWIFT's network. The programme consists of several different parts, among others increased requirements for participants' security requirements, increased controls of participants' compliance to SWIFT's rules and regulations and an increased focus on the information sharing requirements in the event of suspected attacks. The Riksbank is positive towards this initiative and assesses that it will contribute towards increased cybersecurity across the entire global financial system. Their participation in the cooperation on the oversight¹⁴ of SWIFT allows the Riksbank and other overseers close monitoring of SWIFT's programme of measures. The Riksbank and Finansinspektionen also jointly follow up the systemically-important infrastructure systems in Sweden through this programme.

Cyberattacks place particular demands on outsourcing

In recent years, the infrastructure companies overseen by the Riksbank have increasingly outsourced their IT operations, either to external suppliers or to internal units providing services within that group. This sets particular challenges regarding the prevention of cyberattacks. For example, a cyberattack against an important external supplier of IT services could put critical IT systems out of action for several banks and infrastructure companies at the same time.

PFMI differentiate between critical suppliers to financial market infrastructures and other suppliers. Critical suppliers supply services and products that are of particular importance to the principal and which must therefore meet special demands for risk control and information security.¹⁵ However, the Riksbank considers that this distinction has limits when it comes to assessing infrastructure companies' resilience to cyber threats.¹⁶ Even an insignificant part of operations that has been outsourced can become a target for cyberattacks, which in turn could threaten the core activities of the infrastructure company. IT and communication services are particularly sensitive to cyberattacks and the basic premise should therefore be that these suppliers must be subject to high security requirements. If infrastructure companies place lower security requirements for some outsourced activities but not others, this should be preceded by a thorough analysis. This analysis should identify the risks and vulnerabilities of outsourcing and make an assessment of the consequences should these risks be realised. Physical security such as fire safety,

¹⁰ See also footnote 41.

¹¹ SWIFT Customer Security Programme, see www.swift.com and *Financial Stability Report 2016:2*. Sveriges Riksbank.

¹² SWIFT (Society for Worldwide Interbank Financial Telecommunication) is a Belgian cooperative company that provides a global network for the secure transfer of financial messages such as payment instructions between financial actors across the world. SWIFT also acts for the standardisation of financial messages. SWIFT has participants in over 200 countries across the entire world and thus plays an important role in the financial markets.

¹³ For more information, see *Financial Stability Report 2016:1*. Sveriges Riksbank.

¹⁴ SWIFT is overseen by the central banks of the G10 countries, under the leadership of the National Bank of Belgium. There also exists an extended forum under the framework for oversight in which representatives from CPMI are represented in addition to G10.

¹⁵ IT services and communication links are two examples of such services. PFMI, principle 17, operational risk and interdependencies, PFMI Annex F; oversight expectations applicable for critical service providers, CPMI-IOSCO; PFMI assessment methodology for the oversight expectation applicable to critical service providers.

¹⁶ This was also brought up in CPMI-IOSCO's guidance on cybersecurity.

perimeter security and access to a reserve energy supply for electricity and telecommunications should also be considered in outsourcing.

The Riksbank investigates resilience to cyberattacks

Under the framework of the continuous oversight, the Riksbank will follow the systems' continued work on cybersecurity in 2017. Specifically, the Riksbank intends to carry out a survey of the Swedish financial market infrastructures being overseen, to further investigate their preparedness to deal with cyberattacks and to find out whether the companies comply with CPMI-IOSCO's guidance on cybersecurity. In conjunction with this, the Riksbank will pay particular attention to outsourcing and its effect on resilience to cyberattacks.

Operational risk in the financial system will be heightened until the VPC system has been changed

A functioning trade in securities requires securities to change ownership – transactions to be settled in a secure and efficient manner. On the Swedish market, the central securities depository Euroclear Sweden alone provides this function through the VPC system.

Since 2013¹⁷, the Riksbank has repeatedly pointed out that Euroclear Sweden should replace the VPC system as soon as possible. The reason for this is that the VPC system is old¹⁸, and inflexible and the risks involved in keeping it increase with each year. The risks are partly due to the VPC system's complex construction. The system is not constructed of modules, like modern systems often are. Instead, there are many interconnections and interdependencies in the system. This makes it difficult to gain an overview of what the consequences may be when changes are made in the system and there is a greater risk that changes may have unintended effects on the system. Another risk arises from the fact that the programming language the VPC system is coded in is old and hardly used any more. This means that there is limited access to programmers with the skills needed for the VPC system. The Riksbank has also earlier pointed out that it is becoming increasingly difficult as time passes to adapt the VPC system to the demands for change due to new laws and other changes in the securities market.¹⁹ In autumn 2015, Euroclear Sweden decided to replace the VPC system and a project for this was initiated at the start of 2016.²⁰ However, by December 2016, it was clear that it would not be possible to implement a system change fast enough to comply with the timetable in the EU regulation CSDR²¹. In practice, no other options remained but for Euroclear Sweden to make the CSDR adjustments in the VPC system, despite the risks this would entail. The board of directors of Euroclear Sweden then decided to pause the system changeover and instead make adjustments to CSDR in the old VPC system.

Keeping the old VPC system in operation means that the operational risk increases every year. Additionally, making changes to the system further increases the operational risk, as described above. Disruptions to the function for securities settlement lasting longer than a day or so could have far-reaching consequences for many participants in the Swedish economy. If a stoppage in the VPC system were to occur at a time of day or on a day of the month when large volumes of transactions are to be settled, for example when large numbers of due loans are to be renewed, this could rapidly lead to significant liquidity disruptions for both banks and other infrastructure companies. This would probably also

¹⁷ *Financial Infrastructure 2016, 2015, 2014 and 2013*. Sveriges Riksbank.

¹⁸ The VPC system has been in use since 1989.

¹⁹ The IT review of the VPC system that the Riksbank commissioned in 2013 showed that the risks involved in implementing changes to the VPC system were high, due to age, complexity and obsolete technology. The IT review also noted that the code used to program the VPC system was obsolete and, consequently, there was limited access to programmers with this skill.

²⁰ There were several reasons for this decision: The VPC system is certainly stable and reliable but it is deemed to have reached the final phase of its expected lifetime. The introduction of the EU regulation CSDR also entails requirements for comprehensive changes, which were intended to be introduced in a new system.

²¹ The timetable for the introduction of CSDR had yet to be completely settled when the decision for the system changeover was taken, but the preliminary timetable at this point suggested that the new regulations could be expected to enter into force in the winter of 2017/2018.

make it difficult for markets for trade in securities and derivatives to function and lead to a marked decline in the possibility of pledging securities. For the Riksbank, this would lead to difficulties in conducting monetary policy as the pledging of securities for monetary policy transactions is carried out in the VPC system.

The Riksbank therefore deems that one consequence of the decision to keep and adjust the VPC system is that operational risk in the financial infrastructure as a whole will be heightened until Euroclear Sweden has exchanged the VPC system, particularly over the period in which the VPC system is to be adjusted to the requirements of CSDR.

To reduce this risk, Euroclear Sweden must safeguard the continuity of the daily operations of the VPC system and ensure that changes to the system in no way disrupt the daily operations and activities or impact the reliability of the system. Euroclear Sweden should implement heightened preparedness for disruptions and stoppages when it starts changeover work so as to avoid problems in the settlement of Swedish securities. Euroclear Sweden must also tangibly ensure that continuity plans are in place to allow it to manage any consequences of the risks identified.

Finally, the Riksbank finds that there is reason, once again, to repeat how important it is that Euroclear Sweden replaces the VPC system as soon as the currently planned CSDR adjustments have been introduced.

Euroclear Sweden needs to manage the project risk of adapting the VPC system

Apart from the risks of stoppages and disruption in daily operations as Euroclear Sweden adjusts the VPC system to CSDR, the project itself also entails risks. These include, for example, the risk that the project will be affected by delays. Euroclear Sweden's paused project on replacing the VPC system was fraught with problems and delays (see the article *The board of directors' responsibility in an infrastructure company*). The Riksbank would therefore like to emphasise a number of aspects that are important to limit the risk that the project for the CSDR adjustment of the VPC system will fail.

One important precondition for success is that Euroclear Sweden ensures that its participants are involved in project planning and specifying requirements at an early stage of the project. It is also important that the functional requirements for the changes to be implemented are developed by Euroclear Sweden and the participants together. This will require clear communication and transparency on Euroclear Sweden's part towards the participants as regards timetables, documentation and planning of the project. Furthermore, both Euroclear Sweden and its participants will be required to devote sufficient time and resources to the project. The Riksbank also expects Euroclear Sweden, where relevant, to apply the recommendations presented in the external quality control²² of the paused system changeover project²³ in the project for the CSDR adjustment of the VPC system. The Riksbank supports Euroclear Sweden's decision to allow this project too to be reviewed by external evaluators, as this will contribute towards the quality assessment of the project. The Riksbank will also itself monitor Euroclear Sweden's project closely.

The Swedish securities market needs a long-term strategy

Over the last few years, major changes have been taking place in the market for securities settlement in the EU. Following CSDR²⁴, new regulations for central securities depositories and their participants are being introduced and Target 2 Securities (T2S)²⁵, a joint platform for

²² In the summer of 2016, Euroclear Sweden commissioned an external review of the paused system changeover project. The reviewer examined the project's planning and governance, among other areas.

²³ Recommendations for improving the governance and planning of the project, among other matters.

²⁴ CSDR will gradually be introduced over several years. The regulation entered into force in September 2014. A number of more detailed regulations (technical standards) entered into force at the end of March 2017. According to the regulation, a central securities depository must apply for authorisation within six months of the entry into force of these detailed regulations, i.e. by no later than 30 September 2017. Other changes, such as the introduction of new regulations to improve the settlement ratio, so-called settlement discipline, will be introduced 24 months after the entry into force of the detailed regulations. Other further requirements will be introduced by 2023.

²⁵ Target 2 Securities is the European Central Bank's platform for securities settlement in central bank money in several currencies. See *Financial Infrastructure 2015* for a description.

securities settlement in central bank money in several currencies, was launched in the summer of 2015. Until recently, central securities depositories have, to a large extent, operated under various national laws and, in many cases, an almost monopolistic position. CSDR and T2S will create conditions for European central securities depositories to conduct cross-border operations, meaning that operations that have, until now, basically been national and monopolistic can now be exposed to competition. The changes will also make it possible to standardise processes, which should benefit the participants on these markets and contribute towards increased efficiency. The changes will thus entail new possibilities, but will also involve new demands on the central securities depositories to adapt their operations and strategies to the new conditions.

Apart from the changes within the EU described above, Euroclear Sweden's future replacement of the VPC system will entail major changes for the Swedish securities market. However, Euroclear Sweden's decision to postpone the system changeover has changed the conditions for a future system changeover in that the time pressure caused by the regulatory requirements²⁶ has been removed. When the system changeover is resumed after a few years, Euroclear Sweden will have the possibility of taking new strategic considerations in the design of its services for the Swedish market, which takes into account the changes that are taking place now. The approaching system changeover and the ongoing transformation of the European market for securities settlement also mean that the Swedish market participants – that is, both Euroclear Sweden and its participants – should formulate a strategy for the Swedish securities market in the longer term. Such a strategy should include a stance on whether the Swedish market should join T2S or not, as this affects which functionality the new system will need. For example, joining T2S will involve the central securities depository moving a number of functions to T2S instead of managing these in its own system. Examples of functions that could be moved to T2S are securities settlement and intraday credit in central bank money.²⁷ A standpoint on Sweden joining T2S is thus highly relevant as a basis for the future exchange of the VPC system as it would affect what the new system should be able to do. The Riksbank therefore finds that there is now reason for the Swedish Bankers' Association, as mouthpiece of the Swedish securities market, again to examine the pros and cons of a Swedish membership of T2S. If the Swedish market advocates Sweden joining, the Riksbank will take a stance on whether or not the Swedish krona should be connected to T2S.

Continuity and capacity for recovery need to be strengthened

Financial market infrastructures provide services that are critical to the functioning of the financial markets. The services are expected to be available without interruption. It is therefore important that all systems have plans and routines for maintaining services in the event of serious problems. To manage purely operational problems, the Swedish systems²⁸ have contingency plans and back-up sites and conduct contingency exercises, among other preparations. To manage financially difficult situations that threaten their viability, the Swedish systems have recovery plans. The systems also have plans for how they should manage any wind-down of an important service. Continuity solutions and plans are thus in place, but need further development. For example, Euroclear Sweden needs to improve its preparedness to manage disruptions to the VPC system (see the section *Operational risk will be heightened until the VPC system has been replaced*). If Euroclear Sweden cannot maintain its critical services, this could lead to operational stoppages in other infrastructure systems, primarily RIX and Nasdaq Clearing.

²⁶ See footnote 24.

²⁷ These functions are handled by Euroclear Sweden in their own system today.

²⁸ All systems except RIX, as systems owned by the central bank need neither recovery plans nor plans for orderly wind-down.

Work on the RIX system's contingency procedures needs to be resumed

All systems have well-established contingency procedures in place. However, for the RIX system, which has a central function in the financial system, these contingency procedures need to be exceptionally robust according to PFMI.²⁹ RIX has good and steadily improving availability (see Chart 1). In previous reports, the Riksbank has emphasised the importance of RIX initiating work on improved contingency procedures.³⁰ It remains important to ensure that the risk of an IT incident does not affect all RIX different operating sites. Work on strengthening the RIX system's contingency procedures has been delayed as other projects³¹ have been considered to be more time-critical. In 2017, the work of strengthening the contingency solutions should be initiated as planned.

All parties need to participate in the systems' contingency exercises

One way of strengthening a system's contingency procedures and ensuring that they function as they should is to test them regularly. The systems are required to regularly conduct contingency exercises, both internally and with the system's participants. So that these tests can serve their purpose, all participants should participate to the greatest possible extent in the contingency exercises arranged by the systems. The Riksbank has pointed out that the participants' interest in participating in Nasdaq Clearing's contingency tests is low. The participants should always strive to participate in Nasdaq Clearing's contingency tests.

The Swedish systems' recovery plans need further development

If a company providing a financial infrastructure system is impacted by serious financial problems, there should be a plan for recovery so that bankruptcy can be avoided. The three Swedish infrastructure companies (Nasdaq Clearing AB, Euroclear Sweden AB and Bankgirot AB) that international standards, PFMI says should have recovery plans all have a plan in place. However, the companies have made varying amounts of progress in the development of their plans. The common factor for them all is that they must continue to work actively with their recovery plans so that these can be useful tools in a financially difficult situation.

In 2016, CPMI-IOSCO published the results of a survey of how counterparties³² have complied with the requirement for recovery plans around the world.³³ It noted that a great deal of development work remains to be done before the plans are in line with the requirements of the PFMI. For example, tools to manage losses and restore liquidity and capital need to be developed. Similarly, tools for managing losses not caused by the failure of a participant need to be developed. The conclusions in CPMI-IOSCO's report are relevant for Nasdaq Clearing and, where applicable, also for Euroclear Sweden and Bankgirot. The systems' plans also need to be developed continually, as their operations develop and the international environment changes.

Some of the shortcomings the CPMI-IOSCO report indicated concerning recovery plans, and which are relevant to Nasdaq Clearing, were previously highlighted by the Riksbank and IMF. The IMF's analysis was made in conjunction with their analysis of the Swedish financial system within the framework of the Financial Sector Assessment Program (FSAP) that was conducted in 2016. Since then, Nasdaq Clearing has developed its recovery plan considerably, which has been received positively by the Riksbank. To prepare for the approaching legal requirement for recovery plans, Nasdaq Clearing should continue to develop its recovery plan in line with the international standards on which the approaching legislation is based (see the article *New framework for taking care of central counterparties with financial problems*).

Bankgirot has continued developing its recovery plan. Some work remains before the plan complies with international guidance and becomes a usable policy document in a difficult

²⁹ See PFMI, Principle 17.

³⁰ See *Financial Infrastructure 2014* and *Financial Infrastructure 2015*. Sveriges Riksbank.

³¹ A project that has been prioritised is the Riksbank's change of collateral management systems.

³² Nasdaq Clearing was not included in this survey.

³³ Implementation monitoring of PFMI: Level 3 assessment – *Report on the financial risk management and recovery practices of 10 derivatives CCPs*. BIS Committee on Payments and Market Infrastructures – International Organization of Securities Commissions. August 2016.

financial situation. It is important that Bankgirot has a well-considered recovery plan, even if the company, unlike Nasdaq Clearing, is not exposed to credit and liquidity risks.

The orderly winding down of critical services requires capital and plans

Financial infrastructure systems contribute to systemic risk and additionally provide critical services to which there are not always alternatives. It is therefore necessary that infrastructure companies, unlike banks, for example, have plans for an orderly wind-down and enough capital to implement such a plan. The objective is for the winding down of infrastructure companies to take place with the least possible negative impact on society. In concrete terms, this means that it must be possible to continue the critical service that the company provides without interruption. In practice, this probably means that operations will have to be continued until another company becomes able to provide a corresponding service. As there is, at present, no legal possibility for the government to intervene to ensure that critical services are maintained, responsibility lies entirely with the infrastructure systems. A resolution procedure for central counterparties is, however, currently being drafted (see the article *New framework for taking care of central counterparties with financial problems*).

Each of the three Swedish systems (Nasdaq Clearing AB, Euroclear Sweden AB and Bankgirot AB) that are to have plans for an orderly wind-down either have a plan in place or are currently developing one. However, all three systems need to develop their plans further to ensure that they are able to wind down a critical service in a way that would have as few negative consequences as possible for the participants in and the functioning of the financial system. That the systems do not yet have sufficient plans for an orderly wind-down is a risk that needs to be limited by the systems and is carefully monitored by the Riksbank.

PFMI includes a requirement for all infrastructure systems to have assets for at least six months' operating expenses so that they are able to carry out an orderly wind-down. However, it is difficult to evaluate how long an orderly wind-down would take. Assuming that it will be possible to wind down a critical operation in six months, which is the minimum requirement, may be excessively optimistic, particularly if there is no established alternative to the critical service. Consequently, it is important that companies providing these services base their assessments of how long an orderly wind-down will take on thorough analyses and adjust their plans accordingly. In this analysis, the company will have to consider matters such as what the participants need to do and how much time it will take for them to find a replacement for the company's critical service. This is to reduce the impact on society as far as is possible.

A system should thus have assets funded by equity that cover the operating expenses over the period it takes to wind down a critical service. At the same time as the Riksbank monitors the systems' work on their plans, it also examines in more depth how the systems have assessed and calculated the capital they must retain to be able to implement these plans. As part of this analysis, the Riksbank has calculated how long a critical service can be maintained with the liquid net assets funded by equity that the system actually holds. This capacity can be summarised with the assistance of what is known as an orderly wind-down ratio (OWD ratio).

The OWD ratio – a complement to the analysis of preparedness for an orderly wind-down

The ratio shows the relationship between total liquid net assets and three years' average operating expenses for six months.

$$OWD - ratio = \frac{\text{Liquid net assets (funded by equity)}}{3 - \text{years' average } 6 - \text{months operating expenses including interest}}$$

According to PFMI, a financial market infrastructures should have liquid net assets³⁴ funded by equity for at least six months' operating expenses.³⁵ The OWD ratio places a system's liquid net assets in relation to average operating expenses instead of the last six months' operating expenses. Using the average for six months over the last three years is considered to provide a better view of the expenses.

A ratio equal to 1 shows that the system has the resources to run operations for six months, assuming that the expenses are the same or lower than they have been over the last three years. A ratio below 1 indicates that there are not sufficient resources, and a ratio higher than 1 indicates that there are more resources.

The ratio only takes account of the operating expenses and liquid net assets. It does not take full account of volatility in expenses caused, for example, by various risks materialising or decreases in the value of the liquid assets.

It is difficult to make direct comparisons of the different systems' OWD ratios, as they have widely-differing operations and conditions for orderly wind-down. On the other hand, the ratio does give an indication of how large margins individual infrastructure systems have in relation to the requirement to maintain enough capital in liquid form to cover at least six months' operating expenses. The figures for the year-end 2015 show that the OWD ratios for two of the Swedish systems are well above 1, while Bankgirot lies just under 1 (see Table 1). A ratio of 1 shows that a system has enough resources to continue operations for six months. This means that, at the start of 2016, Nasdaq Clearing and Euroclear Sweden had enough liquid net assets to cover expenses for almost 3.5 and 2.5 years respectively, independently of how long the systems deem an orderly wind-down would take. In contrast, Bankgirot's liquid net assets only corresponded to just under half a year's operating expenses. The Riksbank has therefore requested Bankgirot to ensure that it has enough capital, under all circumstances, to manage an orderly wind-down.

Table 1. OWD ratios for the Swedish systems

	Nasdaq Clearing	Euroclear Sweden	Bankgirot
OWD-ratio	6,86	4,97	0,95

Note. The Riksbank's estimates are based on the systems' balance sheets and profit and loss accounts.

Sources: Bankgirot, Euroclear Sweden, Nasdaq Clearing and the Riksbank

Central counterparties' increased importance means that they need to develop their risk management and preparedness

Central counterparties contribute to financial stability as they take on a lot of the risks in the financial system and strive to reduce the risk by robust risk management. At the same time, central counterparties' operations give rise to major credit and liquidity risks. These risks arise because a central counterparty commits to supply payment or securities in the place of its participants, even if a participant should default. At the same time as central counterparties are exposed to financial risks, they have also gained increased importance for financial stability around the world. This is because there are regulatory requirements for central

³⁴ Net assets are total assets on the balance sheet minus total liabilities on the balance sheet, which correspond to equity. Liquid assets are only those assets on the balance sheet that are liquid, such as cash balances and short-term investments.

³⁵ PFMI, Principle 15 Key consideration 2.

counterparty clearing and stronger economic incentives than previously for banks to clear centrally. More and more risks are thus being concentrated in central counterparties.

CPMI-IOSCO has assessed financial risk management among a number of central counterparties around the world. The assessment showed that many of them have largely implemented the requirements of PFMI in a consequent manner. However, CPMI-IOSCO points out that the central counterparties must continue to improve their risk management, above all as regards liquidity risks and financial risks connected to a recovery situation (see the section *Continuity and capacity for recovery need to be strengthened*).

CPMI-IOSCO also indicated a number of areas in which more detailed international guidance will be forthcoming. These include, for example, the importance of taking a holistic approach to procyclicality³⁶, replenish financial resources in the so-called waterfall³⁷ as soon as they are consumed, and the design of liquidity stress tests.

Nasdaq Clearing was not included in CPMI-IOSCO's assessment but the results are still relevant for it. The Riksbank therefore considers that Nasdaq Clearing should take notice of the results of CPMI-IOSCO's investigations, above all when Nasdaq Clearing develops its methods for the management of liquidity risk. In addition, Nasdaq Clearing should also take account of local market conditions. As central bank, the Riksbank has particular responsibility for liquidity supply in the economy and can, for example, supply liquidity by various methods to where it may be needed in a crisis situation. It is, however, primarily the individual counterparty's responsibility to ensure it also has enough liquidity to meet its payment commitments in highly stressed situations. In the years ahead, the Riksbank will conduct an updated analysis and assessment of Nasdaq Clearing's management of liquidity risks, based on relevant parts of PFMI.

It is important to have good liquidity preparedness in small currencies too

Apart from the Swedish central counterparties, there are foreign central counterparties that are important to the Swedish market. These are primarily LCH.Clearnet³⁸ and EuroCCP³⁹. Both PFMI and EU legislation make clear that it is important for central counterparties to have good liquidity preparedness in all relevant currencies. For Sweden, the Riksbank considers that it is particularly important for the foreign central counterparties to have good liquidity preparedness in Swedish kronor, even though the krona is often a small currency for foreign central counterparties. Even if the Swedish market is small for foreign central counterparties, they may be major actors on the Swedish market and thereby be important for the stability of the Swedish financial system.

CPMI-IOSCO has also pointed out the need for further international guidance around the standards for liquidity preparedness in relevant currencies, which the Riksbank supports.

³⁶ Procyclicality means that changes in requirements for risk management are positively correlated with movements in financial and economic cycles. This may for example strengthen or create movements in financial markets, which may ultimately jeopardise financial stability.

³⁷ The waterfall is the financial resources a central counterparty has allocated for the management of financial flows in conjunction with participant failures.

³⁸ LCH.Clearnet Ltd is a British central counterparty that both clears various derivative contracts denominated in Swedish kronor and clears shares traded on the stock exchange in Stockholm as well as from other trading platforms. Several Swedish banks are also participants in LCH.Clearnet Ltd.

³⁹ EuroCCP is a Dutch central counterparty that clears equities. EuroCCP clears the majority of shares denominated in Swedish kronor.

ARTICLE – The board of directors’ responsibility in an infrastructure company

Financial market infrastructures play a central and critical role in the financial system. It is therefore important for financial stability that they function well. Ultimately, it is the company’s board of directors that is responsible for ensuring this. This means that the board of directors manage systemic risks on a daily basis, unlike the boards of other companies. The board of directors’ actions or failure to take action can affect the entire financial system. Consequently, particularly high demands are placed on the board of directors of an infrastructure company. In this article, the Riksbank describes its expectations of the boards of directors of infrastructure companies. Apart from the board of director’s general responsibility for all risk management, the Riksbank would particularly like to emphasise the board of director’s responsibility for outsourcing and for complex projects. To be better able to follow up how boards of directors are taking this responsibility, in the period ahead, the Riksbank will expand its dialogue with the boards of directors of the infrastructure companies it monitors.

The board of directors’ responsibility for operations

It is the responsibility and task of the board of directors to ensure that the infrastructure company can provide the services that are critical for financial stability.⁴⁰ It must therefore ensure that the risk of interruption to services is managed well. Good risk management begins and ends with good governance, leadership, control and follow-up at the highest managerial level. The board of directors takes ultimate responsibility for deciding how the company is to be organised and thereby also which and how many resources are to be assigned and which activities are to be prioritised. It is important that the board of directors assigns enough resources, with the right skills and clear responsibility for operations, particularly as regards risk management. Other important components for good risk management are independent functions that report directly to the board of directors, such as a risk function and internal or external auditing. Independence strengthens the prerequisites that these functions are acting independently and with the company’s best interests in mind.

The clear and good governance of the company by the board of directors is fundamental if it is to function well. This can be achieved with the assistance of policy documents specifying the roles and responsibilities of the board of directors and management, but it also requires clear frameworks for risk management and risk tolerance. These must clearly specify how responsibility for risk management is allocated, as well as what kind of risk appetite the company has. In addition to documentation

and independent control functions, it is also important that follow-ups are conducted in the operations to ensure that planned activities have been conducted and adopted risk tolerance levels have been maintained. All in all, the board of directors must manage the infrastructure company in a manner that protects both its own and the financial system’s stability. To be able to discharge this responsibility, it is important that the board of directors possesses competence in risk management and in the operations conducted by the infrastructure company. Independent board members provide balance and contribute objective assessments of risks in the operations.

Infrastructure companies that are part of groups or larger organisations

An infrastructure company that is included in a corporate group or is part of a larger organisation must ensure that it is sufficiently independent to fulfil its obligations as a separate unit and that its independence is not jeopardised by conflicts of interest or outsourcing arrangements within the group or organisational structure.

The boards of directors of Swedish infrastructure companies have a responsibility for limiting the risks of outsourcing

Outsourcing operations can be seen both as a possibility to reduce fixed costs and focus on core activities and as a way of utilising competence that cannot be found within the company. However, outsourcing is accompanied by

⁴⁰ In addition to PFMI, further guidance can be found in various publications from CPMI-IOSCO, which emphasise the importance of governance and control. These

include guidance on cyber threats and the report on central counterparties’ resilience from 2016.

risks in the form of dependence on the supplier, impaired operational control and, in certain cases, a loss of skills. Consequently, outsourcing places high demands on a company's procurement expertise. International standards, as well as legislation, demand that all outsourced operations comply with the same requirements that would apply if the operations were being conducted by the infrastructure company itself.

All infrastructures that the Riksbank monitors have comprehensive outsourcing, both external and internal. In a number of cases, the suppliers are located abroad. For example, Euroclear Sweden's data centre has been outsourced to Paris and is managed by the parent company in Brussels, ESA. Nasdaq Clearing also outsources several functions within its corporate group, for example its IT operations. In an investigation conducted in 2016, Finansinspektionen found shortcomings in Nasdaq Clearing's outsourcing of the company's functions for information security to the group's parent company.⁴¹ Bankgirot has identified three critical service suppliers, Vocalink, CGI and D+H. This means that Bankgirot is strongly dependent on external actors for the continued development and operation of its system platform. The RIX system is dependent on certain other parts of the Riksbank's operations, for example for the management of its IT environment, regulatory framework, analysis and risk management. This dependence displays strong similarities with outsourcing. The IT operations are also, in turn, outsourced to an external supplier. The Riksbank has previously pointed out the problems connected to the RIX system's internal dependencies.⁴² The Riksbank has *inter alia* pointed out that the risks associated with these dependencies should be analysed, as well as the sufficiency of the dedicated resources around the RIX-system.

Since outsourcing also involves risks, it must meet the same high standards as additional operations. It is important that it is clearly documented that the Board is ultimately responsible for all outsourced activities, and that the organization has the right resources and skills in order to make a thorough follow-up of delivered services and to be able to carry out complex orders so that the system receives the services that needed. There should also be documented routines in place to comply with the requirements for the risk management and follow-up of outsourced operations.

Project management and resource allocation are key tools for achieving success

Innovations, new regulations, increased competition and new demands from the market place new demands on the financial infrastructure. These demands mean that more resources are needed to run infrastructure systems and, not infrequently, they also mean that resource-hungry development projects, for example concerning IT, must be implemented. This means that the board of directors must assign sufficient resources and skills to ensure the implementation of the project. Comprehensive projects must be carefully planned in advance and demand thorough documentation.

Over the last year, several projects in certain Swedish infrastructure companies have not been implemented according to plan. The most serious example is Euroclear Sweden, which paused its project for replacing the VPC system. Together with Finansinspektionen, the Riksbank has regularly followed up the project, which has been marked by problems and delays. A number of deficiencies in project management were also observed in the external quality assessment that Euroclear Sweden had conducted in August 2016. The Riksbank is able to note that, in several respects, the project has not been managed well enough by Euroclear Sweden and that there exists reason to be critical of governance and implementation. Another example of a project that has been heavily delayed is the RIX system's ongoing project to replace its collateral management system.

It is worrying that some infrastructure companies have failed in the governance and implementation of certain critical projects. For example, the pausing of Euroclear Sweden's project means, as previously mentioned in this report, that the operational risks across the entire financial system will be heightened for several years.

The Riksbank will extend its dialogue with boards of directors

As a consequence of the Riksbank's observation of various risks and areas for improvement that can all ultimately be traced back to deficiencies in governance and control, the Riksbank intends to open dialogues with the boards of directors of the infrastructure companies. The Riksbank already has, at present, a good dialogue with the infrastructure companies and their managements, but the issue of governance needs to be escalated to the next level, so a dialogue with the boards and, occasionally, with the companies' independent control functions too, has become necessary.

⁴¹ In December 2016, Finansinspektionen decided to issue Nasdaq Clearing with a reprimand and a sanction fee of SEK 25 million for deficiencies in the outsourcing of its information security and elsewhere (FI ref. no. 15-9258). Nasdaq Clearing has appealed against Finansinspektionen's decision.

⁴² *Financial Infrastructure 2016*, pp. 22-23 and *Financial Infrastructure 2015*, p. 24. Sveriges Riksbank.

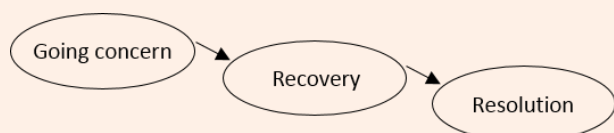
ARTICLE – New framework for taking care of central counterparties with financial problems

The services provided by infrastructure systems in Sweden on the financial markets are of decisive significance for financial stability. If an infrastructure company is facing serious financial problems meaning that it can no longer offer critical services, this would entail a threat to financial stability. Recovery and resolution provide a safety net for managing such a situation. The design of this safety net is specified by both international standards and EU regulations. This article describes the safety net – recovery and resolution – and its functions, as well as the European Commission's proposal for the recovery and resolution of central counterparties.

Recovery is the first step when viability is threatened...

Infrastructure companies must be able to function even when risks impairing their financial position materialise. Consequently, their normal operations have sufficient routines, processes and financial resources to take care of such a situation and its consequences. These routines and processes act as a cushion in the operations. However, it may happen that the cushion is not sufficient. In this case, the infrastructure company will need to adopt measures to recover its financial position. Figure 1 summarises the sequence from normal operations to resolution. The company must be able to manage a recovery on its own without the involvement of central government.

Figure 1 From normal operations to resolution via recovery.



International standards, PFMI, requires all infrastructure companies to have complete recovery plans approved by the board of directors. The board of directors' approval is an important part of supporting the plan. For both central counterparties and central securities depositories, there exist requirements for recovery plans in existing⁴³ or proposed EU regulations⁴⁴, which are in line with the requirements in PFMI.

The plans must describe which tools (see examples below under Tools crucial to both recovery and resolution) and measures that the infrastructure company intends to utilise to maintain its critical services and restore its viability when threatened.

Both the infrastructure companies and the outside world are constantly developing, meaning that the conditions for recovery can change rapidly. After a company has developed a recovery plan, it is therefore important that the plan is regularly updated and adjusted to the prevailing situation.

...if recovery is not enough, resolution awaits

When a company is no longer viable, it normally enters into bankruptcy. However, for an infrastructure company that provides critical services important to financial stability, bankruptcy is not an appropriate alternative. Consequently, there must exist an alternative to bankruptcy for infrastructure companies, just as there is for some banks.

Resolution is such an alternative, meaning that the government takes control over an infrastructure company before bankruptcy and reconstructs it. The aim is to ensure that critical services can be maintained and that financial stability is safeguarded. For central counterparties, the European Commission has proposed a regulation on recovery and resolution. But for other infrastructure systems, such as central securities depositories and payment systems, there is, as of yet, no such proposal.

A recovery and resolution regulation for central counterparties is on the way

The European Commission's proposed regulation on the recovery and resolution of central counterparties is very similar to the corresponding framework for banks⁴⁵ and requires, according to the Riksbank, a number of amendments before it can be fully applied to central

⁴³ Regulation 909/2014 on improving securities settlement in the European Union and on central securities depositories.

⁴⁴ The proposed regulation on a framework for the recovery and resolution of central counterparties.

⁴⁵ Directive 2014/59/EU of the European Parliament and of the Council of 15 May 2014 establishing a framework for the recovery and resolution of credit institutions and investment firms. The directive has been implemented into Swedish law through several acts of parliament, including the Resolution Act.

counterparties. Similarly, the Riksbank considers that the proposal is a good starting point for further work and, as the proposal has not been adopted yet, amendments may still be made. As it is a regulation that is being proposed, it will be directly applicable in Sweden without scope for national deviations.

Supervisory authorities to get an expanded role

According to the proposal, the supervisory authority, together with the supervisory college⁴⁶, will jointly approve the recovery plan prepared by a central counterparty. The supervisory authority will also be given the power to intervene in the central counterparty's activities, so-called *early intervention*. This means that the central counterparty can be forced to take various measures. The measures inherent in early intervention complement the supervisory measures that the supervisory authority has the right to take if a central counterparty violates a regulation.

Early intervention may take place when the central counterparty's financial position is in danger and could result in a crisis situation. The reason that a distinction is made between normal supervisory measures and early intervention is that certain protection mechanisms are triggered under early intervention. For example, contractual parties may not terminate agreements with the central counterparty on the sole grounds that it is subject to early intervention.

Tools crucial to both recovery and resolution

If a central counterparty is to survive serious financial problems, losses need to be covered and financial resources need to be restored. This can take place either via a recovery or, in the worst case, via resolution. It is up to the central counterparty to decide which tools should be used in recovery. In contrast, special resolution tools are described in the regulation. To some extent, these are the same resolution tools existing for banks, but a few of the tools are specific to central counterparties. The tools that can be used in resolution may also be used for recovery. It is therefore likely that there will be a certain overlap between recovery and resolution tools. Two of the proposed resolution tools are:

- Cash calls
- Variation Margin Gains Haircutting (VMGH)

A *cash call* means that the participants must make a cash contributions to the central counterparty. This increases

the amount of money that the central counterparty has at its disposal to manage losses. As a participant must be prepared to pay in the event of a cash call, it is important that the participant is able to predict the amount it may be obliged to pay. The size of a cash call is therefore often set in relation to a participant's contributions to the default fund and the maximum amount is therefore predetermined.⁴⁷ For example, if a participant has contributed SEK 100 million to the default fund, an equivalent amount will be demanded in the event of a cash call.

Variation Margin Gains Haircutting (VMGH) is a tool for write down of debt. It can be likened to a so-called bail-in, which is a tool for write down of debt for banks. When VMGH is initiated, the central counterparty's debts are written down. This is achieved by not paying some or all of the money the central counterparty owes its participants. VMGH has the drawback that it is difficult for a participant to predict how it will be affected by the tool. This is because the size of the debt to be written down is determined by the market value of the cleared contracts in a participant's portfolio unlike the size of a cash call and is therefore not as predictable. A contract that generates a positive cash inflow for a participant, which is to say a liability for the central counterparty, will entail a reduced cash inflow for the participant when that liability is written down.

Resolution colleges proposed for central counterparties

As a complement to supervisory colleges, it is proposed that resolution colleges also be formed. According to the proposal, these would include resolution authorities and supervisory authorities for the central counterparty and its three largest participants as well as central banks. This differs from the banks' resolution colleges, in which central banks are not a self-evident part. The resolution colleges are tasked with drafting resolution plans and making resolvability.

All infrastructure companies need resolution regimes

The Riksbank has previously pointed out how important it is that all types of infrastructure companies can be put into resolution as an alternative to bankruptcy. It is, of course, positive that the European Commission has proposed a resolution scheme for central counterparties. But resolution schemes are also needed for other types of infrastructure companies that are important to financial stability. Consequently, the Riksbank would like for resolution schemes also to be proposed for other types of infrastructure companies than central counterparties.

⁴⁶ According to Article 18 of Regulation 648/2012 of the European Parliament and of the Council of 4 July 2012 on OTC derivatives, central counterparties and trade repositories (EMIR), the supervisory college consists of several different authorities from various member states, including central banks.

⁴⁷ The default fund is a part of a central counterparty's pre-funded financial resources that can be used to cover losses arising from participants defaulting. The financial resources in the default fund are funded by participants and the proportion contributed by a participant depends on its exposure in the central counterparty.

Appendix

The Riksbank's oversight of the financial infrastructure

The Riksbank has the task of promoting a safe and efficient payment system, which in practice means it has a responsibility for promoting stability in the financial system.⁴⁸ Part of this task is analysing and following the development of the financial market infrastructure, i.e. the systems that handle payments and transactions with financial instruments.⁴⁹ In more concrete terms, it is a question of:

- overseeing the central participants in the financial market infrastructure, so that these are safe and efficient,
- promoting market initiatives that can improve and rationalise the financial market infrastructure, and
- influencing international standards, laws and regulations so that they contribute to a safe and efficient financial market infrastructure.

The financial market infrastructure is interconnected. Several banks and other financial institutions are participants in financial infrastructure systems and in many cases these systems also participate in each other's systems. This interconnectedness means that there are many interdependencies between the systems in the financial market infrastructure, banks and the financial markets that need to be considered in the analysis.

Another important task for the Riksbank's oversight and analysis of the financial market infrastructure is, as a result of its analysis work, to have contingency for managing a crisis.⁵⁰

The Riksbank's oversight

In its oversight, the Riksbank applies CPMI-IOSCO's international principles⁵¹ for safe and efficient financial market infrastructures. The aim of the oversight is to identify and analyse sources of risks and efficiency losses in the financial market infrastructure and where necessary to elicit change. For certain types of financial infrastructure systems, many of the international principles have also been incorporated into law. The financial infrastructure systems are subject to continuous supervision as a result of international cooperation arrangements. The Riksbank participates in these arrangements but also monitors to ensure that the systems also comply with those parts of the international principles that are not covered by the law.

Criteria for which financial market infrastructures (FMIs) are to be included in the oversight

The Riksbank oversees the financial infrastructure systems that it has deemed to be important for financial stability. These systems are the Riksbank's payment system for account transfers (RIX)⁵², Euroclear Sweden AB's settlement system for securities (the VPC system), Nasdaq Clearing AB's central counterparty system for financial derivatives, commodity derivatives and repos, Bankgirocentralen BGC AB's payment system for clearing retail payments (Bankgirot) and the foreign systems CLS, SWIFT, EuroCCP and LCH.

The Riksbank applies six criteria to identify the financial infrastructure systems that are to be overseen:

- the number and value of the transactions handled by the system
- the system's market shares
- the markets on which the system is active
- the available alternatives that could be used at short notice
- links with other systems and other financial institutions
- the system's significance for the implementation of monetary policy

⁴⁸ For a description of the Riksbank's tasks, see *The Riksbank and Financial Stability*. 2013. Sveriges Riksbank.

⁴⁹ For a more technical definition of financial market infrastructure, we refer to CPMI-IOSCO, who define it as "a multilateral system among participating institutions, including the operator of the system, used for the purpose of clearing, settling or recording payments, securities, derivatives and other financial transactions".

⁵⁰ *The Riksbank and Financial Stability*. 2013. Sveriges Riksbank.

⁵¹ The international principles referred to are the CPMI-IOSCO Principles for financial market infrastructures, the CPMI-IOSCO Discourse framework and Assessment Methodology as well as further guidance on the principles published by CPMI or CPMI-IOSCO.

⁵² The Riksbank owns and runs the RIX system and is also a participant in it. The part of the Riksbank's operations that runs the RIX system is organisationally separate from the Riksbank's oversight of the financial infrastructure.

The criteria should be seen as assessment areas, meaning that not all the criteria need to be fulfilled before a decision to subject a system to oversight is taken. When applying the criteria, how the system may develop in the future is also to be taken into consideration. Once the Riksbank has taken a decision to oversee a new system, the decision is made public.

What does being subject to oversight involve?

Once the Riksbank has taken a decision to subject a financial infrastructure system to oversight, the Riksbank expects the system to comply with CPMI-IOSCO's international principles. Compliance with the principles involves, for example, publishing information in accordance with CPMI-IOSCO's Disclosure Framework, at least once every two years, or more often if the system has undergone major changes.

The principles are minimum requirements, however. The specific characteristics of the Swedish market may require the Riksbank to impose additional requirements. When the Riksbank adjusts the requirements to Swedish conditions, this is justified in the analysis and in the assessment of the individual systems. Being subject to oversight also involves reporting to the Riksbank and regular meetings.

Risk-based working method

The Riksbank employs a risk-based working method when applying the international principles in order to prioritise risks in and among the financial infrastructure systems that are subject to oversight. For each infrastructure system, the risks are assessed using a template based on the international principles. These system-specific assessments form the basis of an assessment of all the risks based on how great the risks are to financial stability in Sweden. The assessment may also consider whether the Riksbank finds it necessary to perform a more in-depth analysis aimed at ensuring compliance with a specific component in the international principles. Finally, the risk assessment is incorporated into a plan for oversight activities which specifies which risks are to be analysed in more depth and managed in the short term.

Cooperation with Finansinspektionen

Finansinspektionen also has a responsibility for financial stability through its supervision of the individual companies in the financial infrastructure. The remits of the two authorities occasionally overlap. In these cases, the aim is to have efficient forms of contact and cooperation. Formalised cooperation exists between the Riksbank and Finansinspektionen to achieve this. However, the Riksbank does not cooperate with Finansinspektionen as regards the oversight of RIX, as RIX does not fall under the supervision of Finansinspektionen.

Cooperation in the oversight of foreign systems

For the foreign systems that operate in the Swedish infrastructure and that can affect financial stability in Sweden, the Riksbank participates in established cooperation projects with the relevant authorities. The oversight is led by the responsible authorities in each system's home country and follows the guidelines for cooperation in accordance with the international principles.

Communication

The Riksbank communicates its analysis of safety and efficiency in the financial market infrastructure not only in a direct dialogue with the financial infrastructure systems it oversees and other market participants, but also via public statements, speeches and publications. In addition, the Riksbank presents the results of its work on the financial market infrastructure and its view on important financial infrastructure issues in the report "Financial infrastructure".