Timo Iivarinen – Harry Leinonen –
Matti Lukka – Veikko Saarinen

Regulation and control of payment system risks – a Finnish perspective

Bank of Finland Studies
A:106 • 2003

Regulation and control of payment system risks – a Finnish perspective

SUOMEN PANKKI
BANK OF FINLAND
PO Box 160
FIN – 00101 HELSINKI
FINLAND

Phone: +358 9 1831
Fax: +358 9 174 872
Email: publications@bof.fi

Subscriptions to the A series of the Bank of Finland's research publications and changes in address details

Old address details

Company .....

.....

Name .....

Address .....

.....

New address details/subscriptions

Company .....

.....

Name .....

Address .....

.....

☐ New subscription ☐ Cancellation ☐ Number of copies

Timo Iivarinen – Harry Leinonen –
Matti Lukka – Veikko Saarinen

Regulation and control of payment system risks – a Finnish perspective

Bank of Finland Studies
A:106 • 2003

The views expressed in this study are those of the authors and do not necessarily reflect the views of the Bank of Finland.

ISBN 952-462-104-5
ISSN 1238-1683
(print)

ISBN 952-462-105-3
ISSN 1456-5943
(online)

Vammalan Kirjapaino Oy
Vammala 2003

Abstract

This report begins by scrutinising regulation, supervision and risk management of payment systems, as well as risk analysis at a more general level. This is followed by an introduction to payment system supervision and regulation at the international level, with emphasis on the Bank for International Settlements (BIS), European Central Bank (ECB) and International Monetary Fund (IMF). Also included is a discussion of the proper role of national bodies, approached from the Finnish perspective. Payment system risks are discussed in terms of the writers' conceptions of the key risks involved and their classification and measurement.

The payment system risk classifications and framework presented in this report can be systematically examined in terms of either specific types of systems and instruments or as an integrated whole. This framework is used to evaluate the risks of Finnish payment systems. A product-specific risk model is also introduced, which can be used for example by banks to evaluate the risks of specific payment transfer products and their importance. The model development was a joint project of the banks and public authorities.

The report also presents means by which risks can be eliminated or reduced and explains how they have been alleviated in the Finnish payment systems. In this connection, the book describes – again in terms of the risks involved – Finnish interbank payment systems and how Finnish banks are linked to international payment systems. According to evaluations by the ECB and IMF, Finnish payment systems meet international standards and are relatively free of risks.

Finally, a view is presented of the overall course of future developments in payment transfers. The primary trends cited are globalisation, electronification and integration of systems.

Key words: payment systems, payments, regulation, supervision, risks

Tiivistelmä

Tässä julkaisussa tarkastellaan aluksi maksujärjestelmien sääntelyä, valvontaa ja riskienhallintaa sekä riskianalyysiä yleisellä tasolla. Sen jälkeen esitellään maksujärjestelmien kansainvälistä valvontaa ja sääntelyä painottaen Kansainvälisen järjestelypankin (BIS), Euroopan keskuspankin (EKP) ja Kansainvälisen valuuttarahaston (IMF) sekä kansallisten elimien roolia. Kansallisten maksujärjestelmien valvontaa ja sääntelyä tarkastellaan Suomen näkökulmasta. Maksujärjestelmäriskien hahmottamiseksi esitetään kirjoittajien käsitys keskeisistä maksujärjestelmäriskeistä sekä niiden luokittelusta ja arvioinnista.

Esitetyn järjestelmäkohtaisen riskiluokittelun ja -kehikon perusteella voidaan systemaattisesti tarkastella erityyppisiin maksujärjestelmiin ja -välineisiin liittyviä riskejä erikseen ja kokonaisuutena. Riskikehikkoa käyttäen julkaisussa esitetään arvio suomalaisten järjestelmien riskeistä. Lisäksi esitetään tuotekohtainen riskimalli. Sitä voidaan käyttää esimerkiksi pankeissa arvioitaessa yksittäisten maksujenvälitystuotteiden riskejä ja niiden merkittävyyttä. Malli on kehitetty yhteistyössä pankkien ja viranomaisten kesken.

Julkaisussa esitellään keinoja, joilla riskejä voidaan poistaa tai supistaa, sekä kerrotaan, miten riskejä on vähennetty suomalaisissa maksujärjestelmissä. Siinä kuvaillaan myös riskinäkökulmasta pankkien väliset maksujärjestelmät Suomessa sekä suomalaisten pankkien liittymät kansainvälisiin maksujärjestelmiin. EKP:n ja IMF:n arviointien mukaan suomalaiset maksujärjestelmät täyttävät kansainväliset standardit ja systems risks ovat vähäiset.

Maksujenvälityksen tuleviin kehitysnäkymiin luodaan julkaisun lopussa yleiskatsaus. Keskeisiä muutostrendejä ovat globaalistuminen, elektronisoituminen ja järjestelmien integroituminen.

Asiasanat: maksujärjestelmät, maksuliike, sääntely, valvonta, riskit

Preface

Good payment systems are an integral part of a modern efficient economy. With continuous progress in globalisation and rapid technological advance, payment systems as also in a state of transition. International interdependencies are increasing and real time implementation of payments is becoming commonplace. These changes mean higher quality payment transmission and less risk, but they also bring new challenges. The spread of real time processing reduces the timeframe for correcting errors. Problems are discovered more swiftly than before, which underlines the importance of system reliability.

This book, *Regulation and control of payment system risks – a Finnish perspective*, which is included in the Bank of Finland's Series A publications, is a completely revised and updated version of a 1998 publication. The new material includes a description of developments in international regulation and supervision, an evaluation of the risks associated with interbank payment systems, and a presentation of the proposed new capital adequacy requirements. We also use a new approach for analysing payment system risks. The chapter on the challenges of payment system regulation and supervision has been completely rewritten. The Annexes are updated to reflect the current situation and material has been added on the Finnish Bankers' Association's guideline for risk surveys and descriptions of Finland's key payment systems.

A key finding of this study is that presently the risks associated with Finnish payment systems are relatively minor. This echoes a finding of the IMF's Financial Sector Assessment Programme (FSAP). Behind this good situation are the active developmental work of financial market participants and measures taken by the authorities.

These good marks should not lull us into complacency; rather, the systems need to be further developed to meet the needs of technological advance and an otherwise changing environment. This means taking into account the needs of the institutions that maintain the systems as well as those of consumers, companies and investors. Operability of payment systems must be guaranteed even in extraordinary conditions. International cooperation in respect of payment systems needs further improvement, as we strive for a consensus on the basis for developing international standards.

This publication has been updated with the joint efforts of the Bank of Finland and the Financial Supervision Authority (FSA). The writers are Harry Leinonen, Adviser to the Board, and Timo Iivarinen,

Economist, from the Bank of Finland, and Veikko Saarinen, Payments Systems Expert, and Matti Lukka, Banking Supervisor, from the FSA.

Helsinki, September 2003
Matti Louekoski

Contents

1 Introduction

The purpose of this book is to describe the risks associated with Finnish payment systems and clarify the need for their regulation and supervision. The book is a completely updated version of a 1998 publication on the risks of Finnish payment systems[1]. During the intervening four years, payment systems and related risks, and especially risk control, have changed a great deal. For the most part, the changes have been positive in that payment system risks have been reduced.

Payment systems are part of the foundation of a monetary economy. Virtually every business transaction leads to a payment and the use of payment systems. Modern society is highly dependent on the smooth functioning of payment systems. The importance of payment systems and control of the risks involved has increased greatly in recent years because of remarkable growth in trading volumes in currency, money and securities markets. Payment systems have also become increasingly technically sophisticated and faster operating. Their management requires higher-level expertise than before, as well as preparedness for disturbances.

In recent years increasing attention has been paid to the systemic risks of payment systems and their prevention. Wide-ranging payment system disturbances can paralyse large parts of society and cause considerable costs to payment system users. An economic crisis can spread via payment systems from bank to bank or even country to country if the systems do not include effective firewalls.

Payment systems have become increasingly internationalised, in keeping with the globalisation process. At the same time, the authorities have tightened their cooperation. In Finland as well, regulation and supervision must be closely aligned with internationally agreed frameworks and operating principles. With financial markets opening up and the cross-border payments on the increase, more and more attention must be paid to the international dimension of payment system risks.

In Finland, regulation and supervision of payment systems is entrusted largely to three authorities – Bank of Finland, FSA and Ministry of Finance – but the competition office and consumer ombudsman also handle payment matters within their own remits. In this book we pay particular attention to the payment system tasks of

[1] Leinonen – Saarinen (1998) Payment system risks in Finland and the need for regulation and supervision. Bank of Finland A:101. Helsinki.

the Bank of Finland and FSA and the need for their cooperation, and we explain the foundations and operating methods of payment system regulation and supervision. We also examine Finnish payment systems, the associated risks, and the supervisory methods used by the authorities.

The book is organised as follows. First, the objectives of payment system regulation and supervision are broadly described. The 1990s were a decade of highly significant developments in international payment systems, which have had notable effects on tasks, division of labour, and cooperation also at the national level. This is followed by an introduction to the various risks generally associated with payment systems and instruments, as well as to the risk-based model used here to conduct both system-specific and product-specific analyses. We then proceed to describe the Finnish payment systems and their risk-control principles and to evaluate the systems' risk levels. This is followed by an examination of the proposals for new capital adequacy requirements, which would for the first time include capital requirements to cover payment system risks. The book ends with a broad look at possible future developments in payment systems. Annex 6 contains a list of abbreviations used in the book and other key terms.

2 Payment system regulation and supervision – challenges and goals

Payment systems constitute a fundamental part of a modern economy and are of particular importance to the financial sector. As a way of ensuring society's continuing ability to function, promotion of stable and reliable payment systems has become one of the primary goals of payment system supervision. The financial sector as a whole, as well as payment systems as an integral part of the sector, are seen to require public regulation and supervision in order to ensure their adequate stability. Long experience has shown that market mechanisms alone do not generate sufficiently reliable payment system solutions.

A growing share of payments travel through the banks' account systems and so become exposed to the risks of the financial and payment systems. The views of private banks' owners and management – regarding risks, advantages and disadvantages – differ from the views of banks' depositors and customers and society as a whole. Payment systems and their parts are tightly integrated, so that risk realisations can spread quickly within these systems. This underlines the importance of assessment of the whole and of the interdependencies. Because of the large amounts of money involved, payment systems are tempting targets for criminals and others who would misuse these systems. Customers find it difficult to obtain sufficient information for independent assessment of the reliability of financial institutions and payment systems, nor is it a reasonable and practical prospect that such assessments be done privately and continuously.

Public regulation determines the operative framework within which all payment systems are free to pursue maximum efficiency. The payment system infrastructure often takes the form of a monopoly, due to external effects connected with networks. This is another reason why it may be important for the authorities to initiate measures that promote efficiency.

Supervision is necessary for ensuring adherence to regulations. Although self-regulation-based supervision of payment systems has developed and grown in importance, the implementation of such supervision is largely in the hands of authorities. During the last ten years, for example, the BIS, ECB, European Commission, the G10

central banks, and the IMF have drawn up a significant collection of international principles for regulation and supervision. The aim is to create uniform minimal criteria for international application.

Realised payment system risks fall mainly on entities other than system operators and those who determine risk levels. In order to narrow the gaps between different concerned parties' views on risk, it is necessary to use regulation and sanctions to build mechanisms that enable a sufficient portion of risks to be channelled to entities that determine risk levels. Sufficiently strong sanctions are needed to combat avoidance of regulations and rules set by authorities and the distortion of information.

Financial and payment systems are undergoing continual change. It must be possible to quickly adapt regulation and supervision to changing conditions. However, rapid change is itself a risk factor, since adaptation necessarily involves a certain lag. The adaptation process often resembles a pendulum: initial reactions to risk realisations are often excessive and marked by over-regulation; later on, there is too much deregulation and de-supervision. In theory, the optimal level of regulation and supervision is clear, because a single measure is efficient if the additional costs involved are less than the losses that would ensue in its absence. In practice, the matter is less clear because losses are almost always very difficult to estimate precisely, retrospectively. Estimates must be done under conditions of ignorance, and the actual losses must be resigned to afterward. It is not efficient to remove all risks because the costs of regulation and supervision would then greatly exceed the benefits obtained.

Authorities must have sufficient power to regulate and supervise, ie regulatory power for implementing measures and ensuring proper disclosure (eg laws, decrees, orders, operating licences etc). On the other hand, to ensure the efficiency of regulation and supervision, authorities should be accountable and should submit regular reports and evaluations of the effects and costs of regulation and supervision. It should also be possible for external entities to evaluate the efficiency of regulation and supervision.

3 International developments in regulation and supervision

Recent decades have witnessed extensive international cooperation in developing payment systems and reducing the related risks. The need for cooperation has been underlined by the explosive growth of payment flows, especially international transfers, in the last twenty years, as a result of the dismantlement of foreign exchange regulation, globalisation of financial markets, growth of world trade, and technological innovation. These changes have brought notable challenges for practices and procedures of banks involved in payment intermediation, as well as to the central banks and banking supervisors charged with overseeing payment transmission and systems. Some international institutions, for example IMF and World Bank, have added payment and settlement systems to their assessment agenda. These assessments, based on international recommendations, have aimed at determining the systems' possible developmental needs.

In the EU responsibilities for payment system supervision are divided, as agreed, into the broad oversight function and prudential supervision of individual institutions. In Finland, the FSA (Financial Supervision Authority) is responsible for supervising payment system institutions while the Bank of Finland (central bank) handles payment system oversight.

3.1 International cooperation in payment systems

3.1.1 Worldwide cooperation

Under the aegis of the BIS, the G10 central banks meet to discuss, study and agree on payment system risks and control, with the BIS Committee on Payment and Settlement Systems (CPSS) playing a central role. In recent years, countries outside the G10 have increasingly participated in the work of the BIS, and several countries in Asia and Central and South America have joined the BIS. The BIS provides a global forum for cooperation in payment system supervision and management as well as facilities for study and research. As banks have increasingly operated in several continents and some crises have quickly spread across continents, it has become

evident that cooperation in payment system development, regulation, and supervision must also have a global dimension.

Cooperation on payment system development among central banks began as early as 1980, when the BIS established its Group of Experts on Payment Systems. However, it was not until 1989 that the G10 countries published their first report on payment systems (Report on Netting Schemes), which dealt with the risk implications of netting. The Report on Interbank Netting Schemes (Lamfalussy Report), published in the following year, contains the well-known Lamfalussy minimum standards for design and operation of cross-border and multicurrency netting and settlement schemes, and gives several recommended principles for cooperative central bank oversight of these.

In 1992 the BIS Group of Experts became the G10 central banks' CPSS. The CPSS, in cooperation with the G10 countries, has prepared numerous highly regarded reports on mitigating payment and settlement system risks. The most important of these, from the international perspective, is the Core Principles for Systemically Important Payment Systems, published in 1999. Representatives of non-G10 countries were also involved in drawing up the principles, which constitute a minimum requirement for these systems. The IMF adopted the recommendations as basic requirements in its assessments of different countries' payment systems.

BIS analyses and related published reports have also dealt with major risks associated with payments and settlements in securities and FX trading and means of controlling these risks. Some private organisations, eg large banks of the G20 and G30 countries, IOSCO, FIBV, and ISSA[2], have also issued recommendations for reducing payment and settlement risks involved in FX, securities, and derivatives trading.

3.1.2 Cooperation in Europe

Within the European Union, central bank cooperation in respect of payment systems began in 1991 with the establishment of the ad hoc working group on payment systems under the aegis of EU central bank governors. After the EMI was founded, the effort continued in the Working Group on EU Payment Systems (WGPS). In the process of preparing for stage 3 of EMU, the WGPS took up four key matters

[2] Annex 6 contains many of the abbreviations used in this book.

of concern: monitoring of the ECU Clearing system, harmonisation of the main features of EU-country payment systems, central bank cooperation in the oversight of cross-border payments, and payment system planning for the needs of the single monetary policy.

The EU adopted the real time gross settlement (RTGS) principle as a model for risk reduction in European payment systems. This means that netting is not used in interbank payments; instead, each payment is settled via a gross transfer of funds to the receiving bank, which pays the payee. All EU countries were required to implement an RTGS system by the end of 1997. Linking together the national RTGS systems via central banks afforded a way of creating a secure EU-wide real time gross settlement system (TARGET) for payments related to the single monetary policy and other large payments.

The commencement of operations of the ECB and ESCB on 1 January 1999 enabled the realisation of these plans. The TARGET payment system covering the whole EU area was immediately up and running. ECU Clearing, a bank-administered system for ECU-denominated payments, was replaced by Euro1, the EBA clearing system for euro payments. At the same time, responsibility for monitoring the system passed from EMI to ECB (lead overseer).

In the area of payment system regulation, the ECB Statute empowers the ECB to issue regulations that promote the efficiency and soundness of EU area payment systems. To deal with issues of oversight and development of payment systems, the ESCB set up the Payment and Settlement Systems Committee (PSSC). Besides the ECB, PSSC participants include experts from the national central banks. In order to hone the concept of payment system oversight and facilitate cooperation in the EU area, the ECB drafted a set of core principles for national central banks' oversight activities (see section 3.2).

The work of drawing up directives in the area of payment systems is handled by the EU Commission in cooperation with the member states. The Commission has issued directives on small-value cross-border payments, payment finality and collateral, and issuance of e-money. Work is underway on directives on reorganisation and closing of credit institutions and on transfer of collateral between EU countries. The Commission has also issued regulations for example the on introduction of the euro and pricing of cross-border euro-denominated payments. The Commission has also been active in consumer protection regarding payment services and has made recommendations in this area as well as in the provision of remote services.

3.1.3 Cooperation – committees and documents

Banking supervision in the EU area is based on the principle of 'home country control'. A supervised institution's competent supervisor is its home country supervisor. As regards banks and payment systems operating in several countries, this requires cooperation and exchange of information between supervisory authorities of different countries. Otherwise, the organisation as a whole will not be properly supervised.

In Europe there are three bodies for cooperation in supervision of banking and payments systems, which focus on exchange of information and experiences and promotion of cooperation and regulation. These are the ESCB's Banking Supervision Committee (BSC), European Commission's Banking Advisory Committee (BAC), and the EEC countries' unofficial bank supervisors' cooperative body, Groupe de Contact (GdC). All of these bodies deal with payment system issues as one area within the full range of banking activities.

The BSC assists the ESCB in tasks related to supervision of credit institutions and maintenance of financial stability. The BSC for instance studies trends in European banking, financial and payment systems, and the effects of the macroeconomy on the banking sector. It also assists the ECB in drafting opinions on legislative proposals concerning financial activities – including payment systems – of institutions or member states, when requested by the EU Council, Commission, or a member state. Another BSC task is to promote broad information exchange between banking supervisors and central banks, as pertains to financial stability or cooperation in oversight of payment and settlement systems or supervision of institutions.

The primary task of the BAC is to assist the Commission in drafting legislation on EU financial institutions as well as in other matters concerning banking regulation and supervision. The BAC also aids the Commission in the practical implementation of EU banking directives.

The purpose of the Groupe de Contact – the cooperative body for European banking supervisors – is to promote practical cooperation and information exchange among banking supervisors. The GdC is comprised of EEA member countries' banking supervisors and is the only extensive European forum for exchanging information on individual supervised entities involved in banking. This information exchange is confidential and limited to GdC members. The GdC also makes comparisons and works for harmonisation of banking supervision practices, exchanges up-to-date information on member

states' banking supervision, and conducts studies on various banking activities.

Besides the efforts of committees and working groups, international cooperation in supervision is realised by means of memoranda of understanding (MoU). These enable two or more countries' financial market supervisors to agree on practical principles and modes of exchanging confidential information. It is particularly important to agree on cooperation principles in respect of financial companies that operate in areas within the remit of several supervisors since, generally speaking, a supervisor's competence is limited to supervised entities within its own country. The Finnish FSA has signed an MoU with twelve EEA countries, and the Nordic supervisors have one in effect covering that area.

Alliances, such as financial conglomerates, that are involved in several business lines – eg banking, insurance and securities – also require supervisory cooperation. The scope of cooperation may be within or across national borders, depending on whether the alliance and its operations are domestic or international.

3.1.4 Information exchange on payment systems – EU general principles

The ECB and national central banks of the EU, which oversee payment systems in the EU area, have an MoU with the member states' banking supervisory authorities on information exchange. The MoU, which entered into effect on 1 January 2001, serves primarily as a basis for cooperation and information exchange in respect of large-value payment systems in the EU area. The agreed arrangements superseded those in effect from 1994.

The MoU became a necessity because the establishment of the monetary union has had an impact on the division of tasks and cooperation in the oversight of payment systems and prudential supervision of credit institutions. Under the ESCB statute, oversight of payment systems is one of the primary tasks of the Eurosystem, while supervision of credit institution activities is the responsibility of national supervisory authorities.

The MoU points out that cooperation among payment system overseers and banking supervisors is essential because financial stability may be affected by the risks borne by credit institutions arising from their participation in payment systems or their provision

of settlement services and by the risks arising in payment systems as a result of participation by credit institutions.

The main purpose of the MoU is to promote cooperation between EU states' central banks and supervisory authorities in respect of large-value payment systems. But the MoU can also serve as a starting point for cooperative efforts in small-value payment systems and e-money schemes. The general principles presented in the MoU are aimed at promoting the stable development of payment systems and the participating credit institutions. The MoU also applies to investment firms that participate in payment systems and whose domestic supervisors have so agreed.

Signatories of the MoU have agreed that the focal points of cooperation and information exchange are 1) situations in which a new participant joins an existing payment system or a new system is established, 2) as an ongoing basis 3) crisis management situations.

The Signatories have agreed to reassess the arrangements set out in the MoU after the elapse of three years. This will enable taking account of experiences gained in the meantime as well as market developments.

3.2 Eurosystem policy on oversight of payment systems

The aim of oversight in the Eurosystem is to guarantee the smooth operation of payment systems by containing systemic risks, promoting system efficiency and ensuring adequate security of payment instruments used by the public. Central banks use payment systems in the implementation of monetary policy. Oversight is a means of ensuring the smooth functioning of the monetary policy transmission mechanism. Its focus is on risk control and efficiency vis-à-vis private-sector payment systems.

The tasks of payment system oversight in the Eurosystem[3] are divided into four main groups:

a. Formulation of oversight policy is the responsibility of the ECB Governing Council. This includes the determination of core principles for oversight. At national level, the central banks can

[3] For more details on Eurosystem oversight policy, visit the ECB's website (http://www.ecb.int/pub/pdf/paysysover.pdf).

supplement these principles according to local needs. The principles include the minimal requirements and standards for sound payment systems. The central banks are most concerned about large-value and high-volume payment systems.

b. Enforcement of oversight policy is mainly entrusted to the national central banks. The aim is to ensure that all essential systems meet the minimal requirements entailed in oversight policy. In enforcing policy, the national central banks can utilise the different levels of regulation (eg official regulations) or more ad hoc means (eg discussions).
c. Another task area is monitoring payment system developments so as to enable assessment of risks and system efficiency, as well as preventing excessive risk taking. Changes in the operating environment have a continuing impact on payment systems and call for their continual development. One task of oversight is to monitor developments and ensure that payment systems, at both national and international level, take sufficient account of these changes.
d. Management of an emergency situation is primarily the responsibility of the national central bank in whose area the problem originates. Cooperation between central banks is especially important when a problem extends across the areas of several central banks.

Central banks have harmonised and filled out the minimal requirements for payment systems in phases. The core principles for systemically important payment systems, which were formulated jointly by the central banks of the G10 countries, also serve as the basis for Eurosystem oversight.[4] These principles are presented in the next section and form the basis for central bank assessment of Europe's large-value payment systems.

The intention is to apply an abridged version of these standards to important retail payment systems in Europe. The Eurosystem considers it essential to promote the efficiency of retail payment systems and to make the EMU area a common payment area, It has published surveys of the situation and formulated related objectives. The Eurosystem has also worked on security issues regarding electronic payment systems.

[4] The large-value payment systems are the EBA's Europe-wide Euro 1 system, Servicio de Pagos Interbancarios (SEPI) in Spain, Paris Net Settlement (PNS) in France, and the banks' online express transfer and cheque system (POPS) in Finland.

3.3 Results of international cooperation in payment systems

3.3.1 G10 central banks' international recommendations for payments systems

The G10 central banks have agreed on core principles[5] for systemically important payment systems. The aim is to use these in formulating common arrangements and standards for ensuring the soundness and efficiency of payment systems. While the principles are intended for worldwide application particularly in respect of systemically important systems, they can be applied more widely. The Eurosystem is also committed to operationalising the principles. They are treated as minimal requirements, and the aim is to do even better in critical areas.

The recommendations are timely because of the ongoing integration of financial markets and payment systems, and the aim is to ensure that payment system structures and operating modes are such that risks do not spread via payment systems from country to country. Systems that are important in terms of systemic risk generally handle large-value payments and often reach into several countries. Thus the risks must be effectively limited, both domestically and in foreign countries.

The recommendations are distilled into ten Core Principles and four central bank responsibilities.

Ten core principles for systemically important payment systems

I *Legal basis.* The system should have a well-founded legal basis in all concerned member states. Participants may be subjected to financial risks if system rules and procedures are unclear or unenforceable.

[5] The principles were formulated by the BIS Committee on Payment and Settlement Systems (CPSS) and have been published in the BIS publications series (no. 43): Core Principles for Systemically Important Payment Systems. They are also available on the website http://www.bis.org/publ/cpss43.htm.

II *Clear understanding of financial risks.* Rules and procedures should give participants a clear picture of the system's impact on each of the risks incurred through participation. This information should be presented mainly in system rules and operating instructions, which define involved parties' rights and obligations.

III *Management of financial risks.* The system should have clearly defined procedures for managing credit and liquidity risks. The procedures should specify responsibilities of system operator and participants and provide appropriate incentives to manage and contain such risks.

IV *Prompt and final settlement.* Payment covering funds should be transferred by the end of the value day but preferably earlier in the day.

V *Settlement in systems with multilateral netting.* The system should at least ensure timely completion of daily settlements in the event of an inability to settle by the participant with the largest single settlement obligation.

VI *Assets used for settlement.* Central bank money is the preferred asset for settlement[6]. If other assets are used, they should carry little or no credit or liquidity risk. Use of central bank money means that system participants are able to avoid the credit risk of a bank's possible inability to meet its obligation to transfer covering funds. Thus central bank money is the safest settlement asset.

VII *Security and operational reliability.* The system should operate with very high degrees of security and reliability, and there must be backup systems that guarantee that daily operations can be handled in a timely manner even in disturbance situations.

VIII *Efficiency.* The system should enable making payments in a manner that is practical for users and efficient for the economy. Resources should be used efficiently, despite the existence for example of a trade-off between cost minimisation and the safety objective. System designers need to find a solution that takes account of both users' needs and macroeconomic effects.

[6] Here, 'central bank money' consists of system-participant banks' balances in settlement accounts at the central bank.

IX *Criteria for system participation.* The criteria should be objective, publicly disclosed, and fair. Membership should be open to all entities that meet the criteria. The criteria should encourage competition among participants and promote efficient and low-cost payment services. This means that, generally speaking, membership should be voluntary and open. It may nonetheless be necessary to restrict membership in order to protect the system and participants from excessive risks.

X *Governance.* Governance arrangements should be effective, accountable, and transparent. They should enable setting and achieving the system's overall objectives and operations monitoring and should provide proper incentives for management to pursue objectives that are in the interests of system, participants, and the general public. The governance arrangements should also ensure that concerned entities are held accountable and should be sufficiently open so as to provide all concerned parties with access to pertinent information.

Four central bank responsibilities in applying core principles

1. To clearly define its payment system objectives and publicly disclose its role and major policies vis-à-vis systemically important payment systems.

2. To ensure that the systems it operates comply with the Core Principles.

3. To oversee compliance with Core Principles by systems it does not operate and of which it should have the ability to carry out the oversight.

4. To cooperate with other central banks and other relevant domestic and foreign authorities in promoting payment system safety and efficiency through the Core Principles.

3.3.2 IMF-World Bank Financial Sector Assessment Programme (FSAP)

Flexible and well-regulated financial systems are key to a stable domestic economy and international financial system. In 1999 the IMF and World Bank initiated a joint effort to develop the FSAP. The IMF's aim is to promote cooperation in international financial matters, economic growth, good employment conditions, and to assist countries that encounter financial difficulties. The World Bank focuses on lending to the poorer countries. The purpose of the FSAP is to assist countries in their efforts to increase the soundness and flexibility of financial systems and to promote the development of these systems. It identifies financial system strengths and vulnerabilities for the countries studied and makes recommendations to their authorities regarding developmental efforts and so aims to reduce the likelihood of crises.

Country-specific assessment programme are carried out in cooperation with central banks and financial supervisors. So far, programmes have been completed for about 60 countries – some industrialised (eg Canada, Ireland, Finland) and some developing (eg Cameroon and El Salvador). The FSAP was initiated first on a trial basis. The results have proved to be very useful, so that the FSAP is now an established part of the work of the IMF and World Bank.

An assessment looks at the country's financial institutions, such as banks and insurance corporations, and financial markets (for example securities and FX markets). Because payment systems are key to economic performance, their regulation, supervision and legal bases are also examined. The bases for the assessments are the above-listed core principles of the G10 central banks.

An FSAP assessment of Finland was carried out in spring 2001. The team of international experts assessed the stability of the Finnish financial system; the observance of international standards, codes and practices; and financial sector reforms and developmental needs. Finland's key payment systems – BoF-RTGS, POPS and PMJ – were also assessed. The team did not find any noteworthy deficiencies in the Finnish payment systems and considered these to be in compliance with international core principles.

Based on the FSAP assessment for Finland, the IMF published a Financial System Stability Assessment for Finland in September

2001.[7] This dealt with risks of the financial sector that could affect the macroeconomy, as well as the financial sector's vulnerability to macroeconomic shocks.

3.4 Prospects for international cooperation

The onset of stage 3 of the EMU at the start of 1999 and the euro cash changeover at the start of 2002 marked the formation of a common cash and payments area in Europe. In this connection, the present national payment systems and modes are gradually converging. The changes that are occurring derive largely from market forces. The prime means by which different countries' supervisors and central banks and the EU bodies, working together, can affect these developments is by creating common developmental frameworks.

The common currency and payments area have formed a new supranational level of euro cooperation for regulators and supervisors of European payment systems. This requires close cooperation among all the member states, which in turn underlines the importance of the key bodies, such as the ECB, European Commission and European Parliament. In the future, the development and adaptation of regulation and supervision to the new euro area environment will fall to committees and working groups comprised of representatives of these bodies and the individual countries.

Globally, the development of payment systems has been guided by various international recommendations and major (for example G10) countries' public pronouncements. At the global level, the BIS, IMF and World Bank will assume larger roles than earlier in cooperating with individual countries' supervisors and other authorities in assessing the state of payment and settlement systems and the degree to which they meet international recommendations.

Internet and other networks will further promote innovation in payment systems and transfers, as well as improve their efficiency, nationally and internationally. Secure transmission of information requires adoption and understanding of the new technologies of electronic agreement, identification and encryption. Because of its worldwide nature, Internet is difficult to regulate and supervise solely at national level. Internet-based payment systems will in future require

[7] More details on different country assessments are available on the IMF website (http://www.imf.org/external/np/fsap/fsap.asp).

wide cooperation among supervisors and possibly development and adoption of completely new supervisory methods.

The internationalisation of payment systems and transfers is more problematic as regards the EU's practice of home country control. Especially in connection with multinational systems, the need for euro area and global supervision will be underlined. The course of development will necessarily lead to more highly centralised systems.

4 Regulation and supervision of payment systems of Finland

4.1 Oversight of payment systems in Finland

International cooperation between central banks and particularly among Eurosystem central banks has intensified in respect of oversight of payment systems. As part of the European system of central banks, the Bank of Finland is committed to conducting the common Eurosystem oversight policy in Finland.

The powers and tasks of the national central banks are laid down in the Treaty establishing the European Community (Treaty) and the Statute of the European System of Central Banks and of the European Central Bank (Statute). According to Article 105(2) of the Treaty, one of the basic tasks to be carried out by the ESCB is 'to promote the smooth operation of payment systems'. Smooth operation entails both sufficient stability and efficiency. According to Article 22 of the Statute, the ECB and national central banks may provide facilities, and the ECB may make regulations, to ensure efficient and sound clearing and payment systems within the Community and with other countries. Cooperation within the Eurosystem will be emphasised in the common financial markets and the consolidating payment systems. In accordance with Article 105(4) of the Treaty, the ECB shall be consulted on issues relating to eg payment systems.

Central banks' tasks in relation to payment systems are also governed by national legislation. In Finland, the Act on the Bank of Finland, section 3, provides that 'The Bank of Finland shall also […] participate in maintaining the reliability and efficiency of the payment system and overall financial system and participate in their development'.

In practice, oversight in each EU member state is handled by the national central bank. In recent years, the Bank of Finland has, in cooperation with commercial banks, reduced the risks pertaining to domestic payment systems, thus promoting the stability of domestic payment systems. Both POPS and PMJ systems[8] meet the recommendations established by the central banks of the G10 countries for payment systems significant with respect to systemic

[8] See Chapter 6 and Annex 5.

risk[9]. As part of the cooperative efforts within the Eurosystem, the Finnish systems have been evaluated against these recommendations. Possible future changes of these systems will be evaluated rapidly using these criteria as well. With regard to oversight, the systemic risk of the Finnish interbank payment transfers system has been substantially reduced in the past five years.

The efficiency of domestic payment systems in Finland has traditionally ranked very high by international standards, so there has been no special need for supervision of efficiency in Finland. The efficiency of international bank transfers has been weak around the world and Finnish banks alone cannot improve it. Indeed, the efficiency of international transfers will be one of the focal areas in payment system development in the next few years. Finnish banks need to ensure that this development leads to international standards that enable economical and efficient linkages also for the payment systems and banks of small countries.

4.2 Bank-specific payment system supervision in Finland

In Finland, payment transfers by banks participating in common payment systems are supervised by the Financial Supervision Authority (FSA) as part of banks' risk management by virtue of the Act on the Financial Supervision Authority and the Credit Institutions Act. This supervision is mainly based on inspection visits conducted at regular intervals. Supervision based on reporting plays a secondary role. On the other hand, new payment system products offered to the public are inspected before they are launched on the market.

Legal basis of supervision

The legal basis of payment system supervision and related inspection visits is the Act on Credit Institutions, section 68, providing the general rules for risk management in a credit institution. It states as follows:

[9] See Chapter 6.

‘A credit institution and an undertaking belonging to its consolidation group may not, in the course of their operations, incur a risk that fundamentally endangers the solvency or consolidated solvency of the credit institution. A credit institution and an undertaking belonging to its consolidation group shall have adequate internal control and adequate risk management systems vis-à-vis its operations. The Financial Supervision Authority shall issue further regulations on the arrangement of risk management and internal control systems as well as on the requirements to be set for reliable administration.’

In accordance with this section, the FSA has issued a binding regulation and more specific application instructions. These provide the minimum requirements for risk management and other aspects of internal control. The rationale of the regulation is that risk management and other internal control exercised by a credit institution and corporations within its consolidation group should be of adequate standard with regard to the nature and scale of the business. The credit institution and corporations within its consolidation group may not take excessive risks in their business operations. Its internal control methods must enable the recognition, assessment and limitation of risks involved in the business. The regulation comprises the following topics:

– definition of internal control
– risk management as part of internal control
– main elements of internal control
– responsibility for risk management and other internal control
– general principles of internal control
– management policy and control culture
– risk identification, assessment, containment and control
– daily control activities and segregation of duties
– reporting and communication
– monitoring procedures and corrective actions.

The FSA has also given instructions to augment the regulation. In these, it gives recommendations on implementing the risk management and other internal control defined in its regulation 108.1. The principles of reporting and communication are discussed in more detail than the other principles in the instructions. The instructions also reflect on the tasks and status of the internal control of a credit institution.

Payment transfer functions (for example ICT processing of transactions) outsourced by supervised entities are covered by the

FSA *Statement on outsourcing*. According to the statement, a general prerequisite for outsourcing is that if internal functions be delegated to external parties, FSA supervision may not be impaired. Hence, an outsourcing contract made with a service provider must include a proviso on access to information and the right of the FSA to conduct inspections.

Principles of inspection

Payment transfer is one of the main functions of a bank. Interruptions and disturbances in the functioning of payment systems may be fatal for the entire national economy, as payment systems are presently used to transfer a significant share of all the payments made in society. Banks should function so that as few disturbances as possible occur in payment transfer. They should safeguard payment transfer under any circumstances for example by various backup arrangements and contingency plans.

One aim of the Financial Supervision Authority is to promote the stability of financial markets and trust in the functioning of the markets and supervised entities. Therefore, the FSA must ensure that payment systems of major banks function reliably. Furthermore, the FSA must be knowledgeable of the main threats and risks of the payment systems of the entities it supervises and of the practises employed by the supervised entity to manage such threats and risks. The FSA insists on the correction of any shortcomings it detects in the systems and operations of supervised entities.

The objective of FSA payment system inspections is to assess the strategy and goals of the payment intermediation of the supervised entity, the organisation and activities of the payment function, and the control of related risks. Inspections are not typically extended to the level of individual products; rather the starting point is 'process thinking'. The inspections aim to sort out and understand the entire payment transfer process of the supervised entity and its control mechanisms. First an inspection plan is made for the inspections. It is in line with the main groupings of the areas of inspection. As an example, such a plan for payment transfer process can be stated as follows:

- strategy and goals of supervised entity's payment intermediation
- commercial importance of payment services for the entity
- management, organisation and instructions on payment processing
- payment flows and means of payment

– internal control of the main departments involved in payment processing
– payment transfer risks and precautions taken
– payment services/products and their control
– payment systems and applications and the management of related risks
– reconciliations of payment transfer, processing of errors and implementation of corrections
– legal aspects of payment transfer
– administration of users' rights
– recoverability and contingency planning
– payment service contracts between supervised entity and customers
– payment clearing and settlement and cash management
– prevention of money laundering in payment systems.

The key areas of inspection in the supervised entity are risks related to payment systems, risk surveys made, and the analyses and risk management based on these. Also the organisation, functionality and instructions of internal control, and the control mechanisms related to internal control are important. These should enable management to gain awareness of everything exceptional and unusual. The focus of management control is mainly on supervision and the control of mistakes. Control as well as the procedures for recording and reconciling payment accounts must be clearly organised and functional. The aim is to preclude risky task combinations and loopholes in supervision, as these may lead to misuse and losses.

To manage the legal risk related to payment systems, the supervised entity should have the related risk survey results. The legal risk is mainly related to payment contracts made with customers and legislation and regulation on payment systems. The supervised entity should have backup systems and contingency plans in place for disturbances and interruptions. Business contingency plans should be made in sufficient detail, kept up to date, and tested for operability at regular intervals. It is particularly important that the units and divisions crucial for payments have contingenly plans and backup facilities and equipment to cover for a break in electricity supply, data communication failure, fire or water damage or bomb threat etc. The plans should also be tested regularly and reports made documenting possible shortcomings and necessary corrective actions.

4.3 Payment systems regulation in Finland

In Finland, the regulation and supervision of payment systems is decentralised to several authorities. Previously the Ministry of Finance decided on granting licenses to credit institutions, but according to a new law, the granting and revoking of licences was shifted to the FSA as of 1 July 2003.

The Ministry of Finance is responsible for preparing amendments to financial markets legislation. Entirely new legislation is mainly drafted by the Ministry of Justice. The Finnish Competition Authority is accountable for competition matters related to payment systems and related exceptions. Consumer protection matters related to the payment transfers of individual consumers fall in the scope of the Ombudsman, while matters of data protection are attended to by the Data Protection Ombudsman.

In Finland, there is no framework legislation covering payment systems as a whole. However, there is specific legislation on means of payment, such as the laws on bills and cheques. In Finland, the legal relations pertaining to payment systems are still primarily based on contract law and hence on contracts between various parties. The major contract parties are banks engaging in professional payment transfer and the central bank.

Following its accession to the EU, Finland has enacted two specific Acts on payments. They are based on the EU Credit Transfers Directive[10] and the Settlement Finality Directive.[11] The Act on credit transfers based on the first of these, entered into force in August 1999. In addition to small payments (up to EUR 50,000) between EU countries, it also applies, in contrast to the Directive, to domestic credit transfers without any maximum amount. The Act on Certain Conditions of Trading on Securities and Currencies and of the Settlement System, based on the other directive, entered into force in December 1999. It decreased the risk related to the finality and netting of payments and the use of collateral in payment and settlement systems. Based on the Act, the rules of major payment systems were revised. These rules, adopted by domestic authorities, were submitted to the European Commission by the Ministry of Finance, and the

[10] Directive 97/5/EC of the European Parliament and of the Council of 27 January 1997 on cross-border credit transfers.

[11] Directive 98/26/EC of the European Parliament and the Council on Settlement Finality in Payment and Securities Settlement Systems.

systems became designated EU systems in the scope of the Directive and the Act.

In September 2000, the EU issued a *Directive on the taking up, pursuit of and prudential supervision of the business of electronic money institutions*[12]. The directive was to be enforced nationally in EU countries on 27 April 2002 at the latest. In Finland, the provisions of the Directive were included in the revision of the Credit Institutions Act, which entered into force on 15 February 2003.

[12] Directive 2000/46/EC of the European Parliament and of the Council.

5 Analysis of payment system risks

Payment system risks are risks associated with the structures and operations of payment systems, as well as with those who participate in payment systems and transmission of payments.

Payment system risks affect both 'customer payment systems', in which banks act as professional service providers in effecting payments on behalf of customers, and 'interbank payment systems', which are developed by banks and used primarily for effecting banks' own-account payments.

A payment system can also generate risks itself, for instance because of inadequate risk controls or faulty organisation of the system itself. These systems can also spread risks that originate elsewhere, from bank to bank or country to country, if a key system participant has trouble meeting payment obligations and problems are shifted to other participants. In this way payment systems can become a channel for spreading systemic risk, nationally or even worldwide, if disturbances or losses move in a chain reaction throughout the different systems.

A special characteristic of payment system risks is their short duration and continuous recurrence, compared eg to credit risks associated with bank lending. When a payment is irrevocably transferred to the control of the proper payee, the related payment transmission risks cease to exist. On the other hand, since payment orders are sent continuously day after day, there are always payment-related risk positions.

5.1 Challenges of risk definition and evaluation

Defining and assessing payment system risks, like other risks, generally requires the following:

- a clear risk classification scheme
- estimations of risk realisation probabilities
- prior quantification of possible losses.

Since payment system risks can be classified from various perspectives, it is difficult to avoid overlapping and borderline cases. The most demanding task is to identify individual risk events as – specifically – payment system risks. Most risks change over time and

their effects shift from one area to another. An agreement with a corporate customer on non-verification of covering funds illustrates well the difficulty of classification. Under such an agreement, the customer can make payments from its account without verification of covering funds, subject to a de facto overdraft limit amounting at maximum to the total of the same day's outgoing payments. With respect to the possibility of a company going bankrupt and a bank being liable for an intraday overdraft, it is a question of whether the risk is a payment system or credit risk (ie extended overdraft facility).

For frequently occurring events (eg counterfeit payment instruments), for which there are sufficient statistical data, it is fairly easy to estimate realisation probabilities – albeit there is always a danger that unusual changes will go unnoticed. However, it is very difficult to estimate realisation probabilities for unusual events such as a big explosion near a computer centre, an earthquake, a nuclear catastrophe, a terrorist attack, etc.

Measuring the consequences of a risk always entails the danger of over- or underestimation. For example, overestimation is possible if one cannot foresee the possibilities of substituting for a payment system when operations are interrupted. In an actual emergency, the society and concerned parties will adapt to the situation and seek alternative payment systems. If cash were to lose the trust of the public in an exceptionally difficult situation, alternative payment means would probably be put to use. These might be commodity-type media such as gold or other precious metals, or bartering on goods and services. Consequences may also be underestimated if some risks or connections between risks go unnoticed, as in a sophisticated integrated system.

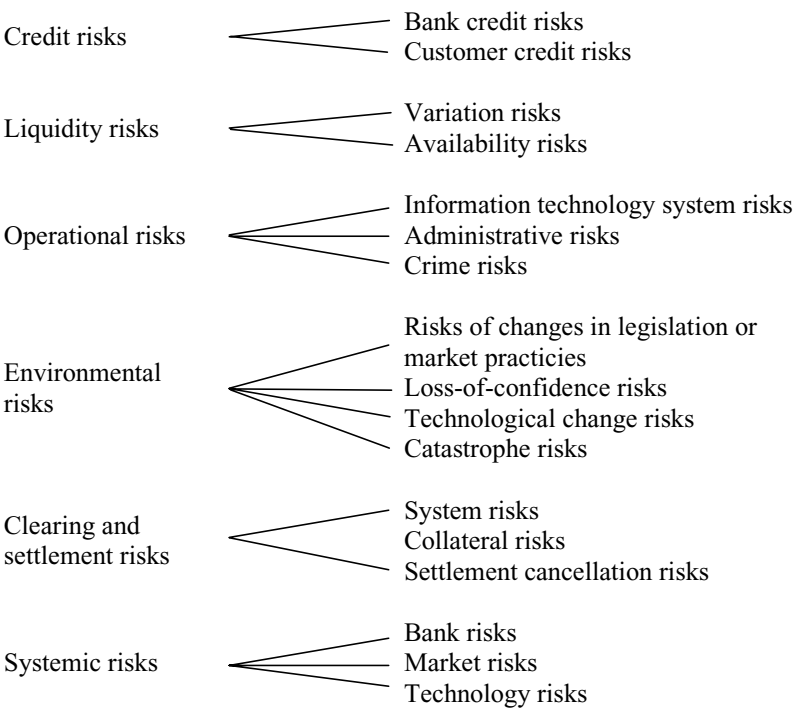
Once accurate estimates of probabilities and consequences of risk realisations have been obtained, as has been done in respect of payment card misuse, one will naturally want to apply risk reducing measures for which the savings will exceed the costs. In difficult-to-estimate cases, decisions are based on subjective views of corporate management and authorities, which generally reflect decision-makers' attitudes toward risk avoidance or risk management policy. Even though risk measurement always entails inaccuracy, outlining and analysing risks helps in understanding of the nature of risks and in finding means to mitigate and control them. Next, we present breakdown of risks, emphasising its utility in analysis and supervision.

5.2 Risk classification

Payment system risks can be classified in several different ways. Generally, a risk realisation results in either a credit loss or a liquidity problem. The ultimate outcome may be the realisation of a systemic risk that threatens the operability of the whole network of payment systems.

In order to classify risks in a manner that is useful for supervision, we begin by listing the basic risk categories and subcategories, as shown in figure 1.

Figure 1. **Classification of payment system**



In academic publications, the classification of risks is usually less extensive. Here, we have aimed at fairly detailed classification, taking into account different specific risk types and means of protection from risk. The scheme can be expanded or contracted as necessary. In the following, each risk category is explained in detail.

Credit risks

Credit risk is the risk of loss that arises when a bank transfers a payment to the payee before receiving covering funds from another bank.

A bank credit risk arises between two banks when the payee's bank assumes an irrevocable liability for the payment but the payer's bank is to settle later, so that there is a risk that the payer's bank may not, for example due to bankruptcy, be able to pay. Bank credit risk is a common aspect of interbank payments, which give rise to open credit positions between banks.

The payer's bank faces a customer risk when it transfers a payment despite a lack of covering funds, at the moment, in the customer's account. Competitive conditions often induce banks to take on customer credit risks, especially as regards large corporate customers.

Liquidity risks

Liquidity risk is the risk of loss that arises when a bank's liquid assets or immediate assess to credit are insufficient to cover its payment obligations.

Variation risk is due to wide variations in a bank's liquidity, which means that the bank is unable at times to forward payments it has undertaken and must temporarily postpone payments execution.

Availability risk arises when a bank's impaired financial condition reduces the amount of liquidity it can obtain from the market to the point that it cannot make payments for which it is irrevocably committed.

Operational risks

Operational risk refers to the risk of costly errors in the information system, administration or organisation of a payment transfer system, or when such a system is misused or accessed by outsiders without authorisation. Information system risks are associated with ICT systems and their manual support operations and with manual payment transfer processes. In the present stage of development, payment transfers are largely information transfers, as the volumes of physical cash payments and cash deliveries are continuously declining. The heavy dependence on ICT systems underlines the importance of these risks.

Administrative risks are generally associated with banks' operating methods, division of responsibilities, functionality of internal risk management processes, employees' expertise, backup systems, problem-handling preparedness, etc. Increasingly more complex and continuously changing systems require far more expertise than before. Increased mobility of key employees and diminished numbers of backup persons create risks of lack of expertise in managing special situations.

Crime risks change as systems develop. Criminals learn about system weaknesses and how to exploit them. In terms of numbers of crimes, most realised risks involve fairly small losses. Organised crime is on the increase, which may portend larger losses to banks. Increasing electronification of services means that criminals often need insider assistance from a bank's present or former employees in order to bypass the systems' security features.

Environmental risks

Environmental risks are risks of loss due to profound changes in the operating environment. The ever-increasing pace of change in society increases these risks. The main environmental risks are associated with changes in legislation and market practices, loss of confidence, technological change and catastrophes.

The frequency of changes in legislation and market practices has increased and may give rise to the emergence of new and unforeseen risks. Laws vary from country to country and are continuously changing. New issues concerning consumer protection, product safety and liability may lead to unforeseen liabilities and damages and thus to unexpected losses, unless there is timely preparation.

Reputation risks associated with loss of confidence can in extreme cases cause customers to avoid a certain service or bank group. A loss of confidence may arise from a single limited problem and spread widely. Customer confidence is key in making payments and using payment instruments.

Risks associated with technological change have increased as the pace of change has increased. This may result in rapid disappearance of certain types of services that are no longer competitive. Dependence on technology can also lead to expensive and unforeseen service maintenance needs. Technical protection of many bank information systems is based on passwords, encryption, control and supervision of user rights, etc. The danger of hacking, ie unauthorised entry into information systems, is on the increase, as criminals obtain

more sophisticated tools and gain access to more powerful hardware and software. This means that banks must continuously upgrade their systems. Because it is easy to make an identical copy of an electronic transaction, it is difficult to ascertain the genuineness of a transaction.

Certain catastrophe risks, such as those associated with natural forces or societal changes, are rarely realised. The deep integration and centralisation of payment systems, and their dependence on high technology, mean increased vulnerability to various large-scale catastrophes.

Clearing and settlement risks

Clearing and settlement risks arise in connection with clearing and fund transfers between banks. These risks are characteristic of interbank payment transfers.

Differences between banks' incoming and outgoing payments vis-à-vis other banks are settled in the central bank's daily clearing. A settlement is a transaction by which a bank transfers funds from its own to another bank's settlement account at the central bank, in the net amount owed as per the clearing calculation. By means of such settlements, sending banks transfer funds to cover the payment needs of receiving banks.

Clearing and settlement systems risks are associated with information systems used by banks and central banks in clearing and settlement, specifically with their credibility, reliability, and backup systems.

Clearing and settlement risks involve the safety, adequacy and custodial care of collateral for clearing and settlement.

Settlement cancellation risks concern the certainty of the irrevocability and finality of clearing and settlement. These depend on the underlying domestic and foreign legislation, interbank agreements, and possible special arrangements for dealing with disturbances. The main problems here are the legal validity of netting in netting-based settlement systems; the timing of customer payment and settlement finality; and (if the parties are from different countries) the applicable legislation.

Systemic risks

In connection with payment systems, systemic risk refers to the risk of loss that would ensue in the event that the whole payment system or a

substantial part of it ceases to function and society's payment services are significantly impaired. Such a disturbance may spread to the extent that it poses a threat to the whole payment system, in which case the operability of the entire financial system and real economy could be at risk.

Systemic risk may be caused by the failure of a critical part of the payment system, such as the information systems; insolvency of a major participant bank; or a crash in a market affected by the settlement of transactions. By these criteria, systemic risks can be classified according to their origins, as technology-, bank- or market-based. With system volumes and degrees of integration increasing, payment transactions becoming more centralised and international linkages increasing, the threat posed by systemic risks is growing. Systemic risk can also arise if one or more of the above-mentioned basic risks of payment systems are realised or spread so widely as to jeopardise the operability of the whole system.

5.3 Classification of payment systems

Payment systems can be classified according to numerous criteria: usage, transaction size, transfer speed, currency, etc. From the standpoint of supervision, an appropriate criterion is associated risks.

In the following, payment systems are categorised on the basis of payment method or instrument, so that risk profiles for each category are as uniform as possible:

- cash payment instruments (cash withdrawals from branches, ATMs or shops)
- payment ATMs
- e-money (on networks and cards)
- debit payment instruments (debit cards)
- credit transfers (including recurring payments and direct debiting), cheques and bank drafts
- express transfers (online payments via POPS).

We focus on issues of risk in respect of the last four payment methods in the above list. Cash payment risks are not covered here because they have been discussed extensively elsewhere. E-money without account keeping is also excluded because detailed coverage is already

available[13]. Payment ATMs per se are excluded because the associated risks are largely the same as for credit transfers. This report is further limited to deposit banks and so excludes payment card companies and finance companies, for example.

Analysis of payment system risks can be system-specific, bank-specific or product-specific. Central banks are generally interested in system-specific risks because they are responsible for oversight of payment systems and for preventing systemic risk. Bank supervisory authorities are more concerned with bank-specific and product-specific payment system risks and banks' internal monitoring of these.

5.4 Payment system-specific risks and their overall evaluation

Classification of system-specific risks

An overall risk classification scheme for payment system-specific risks can be set up by cross-tabulating the above-mentioned basic payment system risks with payment system types (Table 1). Each row in Table 1 contains an individual risk type and each column a payment system with a risk profile that is as uniform as possible. When filled in with grades for each risk/system, such a table provides an encapsulation for example of a particular country's payment system risks. Systems that are as unified as possible with respect to risks (eg debit payment instruments, credit transfers, cheques, and express transfers) can be evaluated as regards different risk types (for example credit, liquidity, operating, environment, clearing and settlement, and general systemic risks).

Table 1. **Grading of payment system-specific risks**

Risk type/system	System 1	System 2	System 3
Risk A	Grade	Grade	Grade
Risk B	Grade	Grade	
Risk C	Grade		
…	…		

[13] For example the ECB's (1998) Report on Electronic Money and the BIS annual Survey of Electronic Money Developments.

The scheme provides for the evaluation of risks and their importance in different payment systems. In its various versions and applications, the scheme can be used as a tool for analysis and supervision.

Risk concepts

Different grades of risk are associated with payment systems. The bank-specific and system-specific as well as systemic grades are defined as follows:

- Bank-specific risks, when realised, cause losses to individual banks, and may even lead to bank crises.
- System-specific risks arise when a particular segment of the payment systems (eg use of payment cards) breaks down and poses a significant threat to the stability and reliability of the payment systems.
- Systemic risk arises in extreme situations in which the system's ability to provide payment services to the society becomes seriously weakened because of a breakdown of a payment system or an essential part thereof.

It is characteristic of payment system-specific risks that realisation losses are huge but realisation probabilities are very small. Reliable and cost-effective operation of a payment system requires the elimination of small but frequently occurring risks.

Risk measurement

In order to evaluate the risks of different payment systems, it is necessary to define the probabilities and possible losses in the systems, broken down into bank-specific and system-specific risks as well as systemic risks. These risks and their importance can be graded as follows:

Minor = Realisation probability negligible; potential realisation losses are not very large and would not generally lead to crisis situation for individual system or bank

Medium = Realisation probability very small; potential realisation losses are large and could lead to crisis situation for individual system or bank

Major = Realisation probability small; potential realisation losses are of major magnitude and could readily lead to crisis situation for individual system or bank.

Risk grading scheme applied to credit transfer system

Table 2 illustrates how the scheme could be used to analyse risks associated with a credit transfer system. Each row corresponds to a basic risk type (see 5.2) and each column to a level of risk (bank- or system-specific or systemic risk, as in the section *Definitions of risk concepts*). Hence each table entry is the grade for the indicated combination of basic risk and risk level.

Table 2. **Risk grading of credit transfer system**

Risk level/ Risk type	System-specific	Bank-specific	Systemic
Credit risks			
Bank credit risks	None	None	None
Customer credit risks	None	None	None
Liquidity risks	None	Minor	Minor
Operational risks			
Information system risks	Minor	Minor	Minor
Administrative risks	None	Minor	Minor
Crime risks	Minor	Minor	None
Environmental risks			
Risks of changes in legislation or market practices	None	None	None
Loss-of-confidence risks	Minor	Minor	Minor
Technological change risks	Minor	None	None
Catastrophe risks	Minor	Minor	Minor
Clearing and settlement risks			
System risks	Ei	Minor	Minor
Collateral risks	None	None	None
Settlement cancellation risks	None	None	None
Systemic risk	None	None	None

Detailed descriptions of payment system risks, in accord with the basic grading scheme of payment systems and their risks, are given in Annex 1. Also included are grades for current Finnish payment systems.

The risks associated with payments transmission vary by bank, in accord with the scope of the payments transmission and the different types of payment systems involved. For this reason, it is difficult to make an overall evaluation of the risks of banks' payment systems on the basis of a particular payment service or system. Banks need to do this themselves, possibly making use of the risk-grading scheme presented above. Based on its own history, a bank could, to the context of entering grades into a table, examine the frequency of various risk realisations (ie yearly, once in 5 or 20 years) and the magnitude of the financial losses. This would shed light on the bank's realised losses in different payment systems. The table would also enable the bank to evaluate the maximum possible loss associated with each risk and thus give an indication of the maximum loss that could ensue from its participation in these payment systems.

The most difficult – but also most useful – task here is to estimate the probable losses associated with payment systems in which the bank participates over the next few (or 5–10) years. If the bank's management considers the risks to be excessive, the evaluation should also take into account proposed risk mitigation measures.

Overall evaluation of system-specific risks

Risks associated with debit payment instruments generally involve small monetary values. Crime-related and information system and administrative risks have been the most visible of these. We have not witnessed any realisations of system-specific risks that could undermine the use specific debit payment instruments. An extensive wave of counterfeiting could initiate an erosion of public confidence in a specific debit payment instrument, but these instruments do not entail systemic risk.

While the risks associated with an individual credit transfer are small, the cumulation of bank credit risks over a large number of transactions could pose a serious threat. In addition to highly visible crime-related and information system and administrative risks, there are risks that are rarely realised, such as environmental and clearing and settlement risks. The latter risks concern legal validity of netting in the context of a disturbance. It is highly unlikely that credit transfer risks would spiral into system-specific or systemic risks.

Cheques entail bank credit risk, especially if coverage is not verified and interbank risk positions are not controlled by limits or collateral. The most visible risks associated with cheques have been crime-related and administrative risks. Other significant risks associated with cheques are clearing and settlement risks connected with advance crediting of netted transactions and legal validity of netting. In disturbance situations, cheques do not generally give rise to systemic risk.

In a disturbance situation, large-value express transfers may involve significant bank credit risks if interbank risk positions are not controlled by limits or collateral. Even with backup arrangements, operational risks may exist eg because of a high degree of electronification. Other important risks here are environmental and especially clearing and settlement risks – albeit, with today's systems, the realisation probabilities are very small. Systemic risk may arise in a disturbance situation.

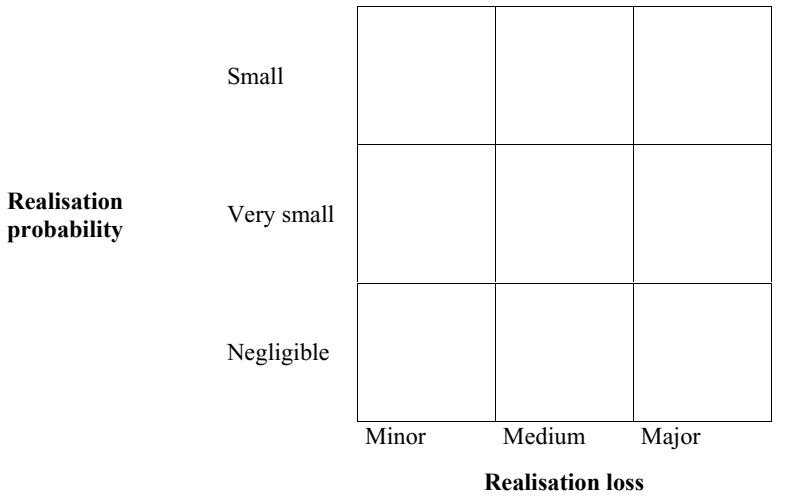
5.5 Evaluation of product-specific payment transfer risks

Classification of product-specific risks

An essential part of banks' risk control is careful analysis and evaluation of risks associated with each product. Such evaluation should, if possible, be done before the product or service is offered to customers.

A bank could for example use the risk classifications presented in Table 3 for evaluating its product-specific or payment instrument-specific risks. The bank would evaluate risks associated with individual services or systems in terms of both realisation probability and realisation loss. Each bank can devise its own grading system. Here, realisation probability ranges from small to negligible and realisation loss from minor to major.

Table 3. **Risk classification of payment services/ products**



By systematically evaluating risks, a bank can get a consistent picture, accumulating over time, of the risks associated with its payment transfer products. This can be useful in controlling product-specific risks and in training employees to recognise these risks.

Banks need to regularly monitor the risks connected with their payment transfer products and for example annually update the grading of realisation probabilities and losses as well as necessary mitigation measures. Historical data on risks are useful in undertaking evaluations, provided they cover a period of several years.

International and national recommendations regarding payment systems call on banks to be cognizant of the risks associated with payment transfer products and systems and to analyse and limit these to appropriate levels. The Bank of Finland and FSA oversee compliance with these recommendations.

A scheme for mitigating product-specific risks

In order to obtain an overall picture of risk control vis-à-vis payment systems, the FSA in 2000 conducted a number of examinations of Finnish banks' payment systems. Weaknesses were exposed in the analysis and control of risks associated with payments systems and services.

In order to correct the weaknesses in risk mitigation, and at the banks' initiative, a working group on risk control was formed in spring 2001. The members were from banks, the Finnish Bankers' Association, the FSA and the Bank of Finland. The group's task was to produce a jointly-acceptable normative model to assist banks in analysing risks associated with payment systems and services. The results were the *Guideline for survey of payment system risks* and *Guideline for survey of legal risks* (Annex 4), which are recommended for banks' use in carrying out risk analyses.

Problems in risk measurement and monitoring

A common problem in measuring payment system risks is a lack of systematic collection of data on risks that could form a basis for calculating realisation probabilities from previous experience. Moreover, some risks pertain to extremely rare events, for which it is virtually impossible to obtain statistical estimates of realisation probabilities because of a lack of observations.

One special problem in monitoring payment system risks is that, for many important risks, the realisation probability is very small but were a realisation to occur the losses to banks and to the whole economy would be huge. Such risks are comparable to those associated with a disaster at a nuclear energy facility or a natural catastrophe. Although the most serious payment system risk is systemic risk, realisations of other risks, especially in respect of large-value payment systems, can also cause enormous losses. Such risks have now been virtually eliminated.

Another characteristic of Finnish payment systems in particular is the high degree of electronification (over 90%) and dependence on ICT-based infrastructure. Misuse of ICT linkages can quickly enable the movement of funds for criminal purposes. Ensuring adequate security for payment transmissions that use the newer payment channels poses a variety of challenges for banks, supervisors and supervisory methods.

A third special characteristic of payment systems is the constantly changing operating environment, which renders difficult the detection, evaluation and monitoring of risks. For example, Internet developments have brought totally new types of payment systems and channels, some of which operate outside traditional banking systems.

5.6 Mitigating payment system risks

Controlling risks

Effective control, reduction or elimination of payment system risks requires a variety of means of payment transfer, procedural rules, risk limits, instructions, and recommendations. In the following, we examine the possibilities for reducing payment system risks by main risk category. Banks that participate in payment systems can use these methods at their own discretion, a financial sector or its interest groups can recommend them to members, or supervisory authorities can require compliance. Methods of mitigating payment system risks are detailed in Annex 2.

Methods of controlling credit risks

Bank credit risk can be eliminated from a payment system by always transferring covering funds for interbank payments before final crediting of customer accounts or by using gross settlement (RTGS). Risks in netting-based systems can be limited by applying bank-specific counterparty credit limits, collateral, legally irrevocable netting, or payment finality rules. The best means of controlling risks is a real time system for execution and monitoring of transactions.

Customer credit risks can be reduced by analysis and rating of customers, transaction- and customer-specific limits and collateral requirements, having persons responsible for specific customers and (preferably real time) monitoring of limits.

Methods of controlling liquidity risks

Liquidity risks in a payment system can be reduced by netting, well-planned payment schedules, and flexible use of limits and collateral. In order to plan for intraday liquidity needs, banks need adequate forecasting systems, and forecasted liquidity positions must cover payment obligations.

Methods of controlling operational risks

Information system risks can be reduced by coordinating decisions concerning these systems, applying common standards, reducing errors and operational disturbances through planning and regular system maintenance. Good ICT system architecture, skilled personnel, continuous training, and written operating instructions will reduce the possibility of errors associated with complex systems and changing conditions. Internal monitoring, a set format for controlling change, security enhancing systems, effective backup systems, and continuity planning all help to prevent realisations of system risks.

Methods of reducing administrative risks include good payment transfer practices; clear division of duties and responsibilities also for senior management; effective use of internal control and risk management methods; and hiring and adequately training skilled employees and continuously upgrading their skills. Also important are care in the maintenance and organisation of system usage; effective backup systems; instructions for handling problems and disturbance situations; and comprehensive agreements covering damages for errors and delays.

Crime risks can be reduced through the application of written security policies and procedures pertaining to crime; integrating security planning into systems planning; adequate monitoring; and separating tasks that are dangerous in combination. Security is further promoted by sufficient physical security; control of access to information systems; observation of secure operating procedures; training employees to recognise crime risks; and sharing experiences with other bodies regarding criminal methods and means of protection.

Methods of controlling environmental risks

The risks associated with changes in legislation and market practices are difficult to avoid, but they can be anticipated by obtaining information from various (domestic and international) sources on applicable laws and planned amendments. Active lobbying of legislators and authorities may also be possible. Corresponding methods can be used in respect of risks associated with market practices, albeit it may be possible to have a more direct impact on authorities through discussions, statements of opinion, etc.

Reputation risks connected with loss of confidence can be avoided by means of proper and swift communication when problems arise,

regular advance dissemination of information, and effective organisation of communications and crisis management. Moreover, anticipating situations that may lead to loss of confidence enables their prevention.

Risks associated with technological change can be identified by monitoring developmental trends in the field. Since the major risks in this category relate to the possibility of breaching existing security barriers, it is prudent to invest beforehand in new security systems and to employ parallel means of protection. Ensuring adaptability requires that systems have sufficient possibilities for extension.

Catastrophe risks can be reduced or alleviated through the application of advance planning and developing and testing recovery capabilities. Security arrangements, such as access control and fire extinguishing equipment, reduce the probability of a catastrophe. Decentralisation of systems reduces vulnerability and enables partial operation during disturbances. Written instructions on the limiting of services or changeover to manual services will improve crisis management.

Methods of controlling clearing and settlement risks

The means of reducing clearing settlement risks include effective and operational backup systems, adequate collateral arrangements, legislation guaranteeing the security of pledged collateral, and settlement finality.

Methods of controlling systemic risk

A key method of controlling systemic risk is to create payment system structures and procedures that reduce the likelihood of both systemic risk realisation and contagion among banks or systems. Internationally recognised methods include real time gross settlement (RTGS), ie immediate transfer of payment cover, along with the other payment information; delivery versus payment (DVP) in securities trading; and payment versus payment (PVP) in currency trading.

Other methods of controlling systemic risk involve the central bank (liquidity provision) or payment/settlement in advance in clearing houses. These alleviate market participants' liquidity problems in the event of a market crash or interruption of the settlement process due to a technical malfunction. Operational backup

systems are also important means of preventing or constraining disturbances.

5.7 Risk mitigation in Finland

In Finland payment system risks have been constrained or eliminated for example by the practice of transferring cover for interbank payments via the central bank before making related entries in customer accounts. New laws and official regulations pertaining to payments have been put in place, and there is a long history of banks' self-regulation aimed at reducing risks. Security enhancing features have also been added to the interbank retail payment system.

Settlement

Finnish domestic payment systems operate in accord with international principles for systems that are important in terms of systemic risk. Payment cover is generally transferred between banks before payments are credited to customer accounts. An exception is the transfer of funds to cover net balances in the POPS system. The receiving bank obtains up-to-date information on a payment transaction and credits the payee customer's account before cover moves between banks. Even here, the banks constrain their risks by means of bilateral limits.

Legislation

The first Finnish law pertaining to payments was a law on credit transfers that entered into effect in 1999 and was followed by the 'netting law'. These first two laws have reduced the juridical uncertainty regarding payment transmission and clarified the underlying legal principles. The netting law makes it clear that netting in the POPS and PMJ systems is legally binding and eliminates systemic and credit risks associated with the possible cancelling of a netting outcome.

Rules

The rules of the PMJ and POPS systems have been approved by the Ministry of Finance, and the EU has been notified that these systems are subject to the netting law. The rules specify when payments become binding and irrevocable. These changes have also reduced credit risks.

Self-regulation

The banks have long cooperated in their self-regulation efforts vis-à-vis payment transmission under the aegis of the Finnish Bankers' Association. By means of various mutual agreements, rules, and standards, and a common delineation of services, the banks have succeeded in giving Finland a speedy and reliable system for payment transmissions. One example of self-regulation is the list of general conditions for domestic payment transfers, which set time limits for the transfer of funds from payer to payee. This was accomplished before the relevant legislation was passed.

For years, the described measures above have been used to control of information system and administrative risks in Finnish payment systems.

Data communication security

In transmitting payment information, the banks use the protected secure information networks in both the POPS and PMJ systems. Since the late 1980s, the 'Sinetti' (electronic seal) procedure has been used to detect information tampering in the PMJ network. And since 1994 the PATU security procedure – developed by the banks themselves – has been helped to safeguard the integrity of transmitted information. It is not possible to change information transmitted in the network without the receiver being aware of the change. Tailored versions of PATU have been used to ensure security in the POPS network from its start, in 1996.

6 Evaluation of interbank payment system risk

6.1 Bank of Finland's RTGS system

BoF-RTGS is the Bank's real time gross settlement system. In such a system, payments are executed one at a time with simultaneous transfer of covering funds and payment information. Participating banks can send payments to each other in real time via their settlement accounts at the Bank of Finland. The system is also the conduit for funds transfers of other interbank systems (PMJ and POPS). BoF-RTGS is also part of the TARGET system, which includes euro area central banks and the ECB.

See Annex 5 for details on BoF-RTGS operations.

Settlements

In the BoF-RTGS, funds are transferred between banks to cover interbank payments. One of the aims in the process is to minimise risks associated with settlement. Account holders' payment orders are entered in real time, provided the payment is valid and the payer's account has sufficient funds. This procedure eliminates bank credit risk. A payment is irrevocable and final when the payer's account is so debited. After this, the payment can be cancelled only via the payee's cancellation or correction transaction.

If there are not sufficient funds in a sending bank's account at the Bank of Finland, the payment order is put in the system's payment queue. The system, at defined intervals, automatically attempts to execute all account holders' queued valid payment orders as a combined entry. A combined entry is made if the funds available in the settlement accounts cover all of the valid queued orders. This means that each account holder must have sufficient available funds, ie amounting at least to the net amount of its outgoing and incoming payments.

In general, account holders' liquidity positions have been good, so that system queues rarely occur and are generally brief.

PMJ settlements

The PMJ system handles mainly small value customer payments between banks. Interbank settlement transfers in this connection are executed twice daily in the BoF-RTGS, at 3.45 pm (afternoon run) and 1.00 am (night run). There is a special morning run whenever a bank is left out of the night run.

In PMJ settlements, fund transfers between individual banks are handled in a combined entry, so that a participating bank needs only enough funds to cover its net position. This procedure reduces banks' liquidity needs and liquidity risks.

Credit and settlement risk

Because payment transactions in BoF-RTGS are not executed until covering funds are debited to the payer's account, interbank credit risks are avoided. A payment is irrevocable and final immediately upon execution. Account holders have access to intraday credit provided by the Bank of Finland, and they can also obtain overnight liquidity via the Bank's marginal lending facility. Intraday and overnight credits are granted against approved collateral.

The BoF-RTGS has been found to meet all of the BIS criteria as set out in 'Core Principles for systematically important payment systems'.

BoF-RTGS backup systems

Because the BoF-RTGS and (linked) TARGET system handle mainly large-value and urgent payments, they must meet demanding requirements. For this reason, the central banks have developed various backup systems that help ensure the smooth flow of daily payments. One requirement is that it must be possible to shift the operations of any parts of TARGET to backup systems within four hours. It is intended that backup systems will be able to handle all critical payments. The Bank of Finland has a separately located facility with backup equipment and a centre that houses a complete set of fully maintained backup hardware and software (including databases). The Bank also has in place a specific plan for operating in exceptional situations, and system participants are informed on what to do in such situations.

Damages and conflict situations

Covering the whole TARGET system is an arrangement for paying damages for financial losses due to system malfunctions. The arrangement applies to both domestic and cross-border payments and covers parties that are forced to resort to the marginal lending facility because of disturbances. Indirect system participants are not covered unless they have used the marginal lending facility.

Final determination of the amount of damages payable is the remit of the ECB Council, which liases closely with the central bank in which the RTGS system disturbance occurred.

An account holder that deems that it has suffered a financial loss due to a TARGET malfunction is required to file for damages within four weeks of the transaction date. Filing is done with the central bank to which it sent a payment order or from which it should have received a payment.

6.2 POPS system

POPS – an online system for large-value payments

POPS is a modern decentralised system for executing mainly large-value and urgent payments. The system is developed, operated and owned by participating banks that are members of the Finnish Bankers' Association. The banks send payment information directly to each other via their own ICT network. Payment funds are transferred via settlement accounts at the Bank of Finland. See Annex 5 for system details.

Gross and net settlements in POPS

In POPS, transfers of payment funds to receiving banks are carried out in both gross and net settlements. Gross settlement is applied when a payment's value exceeds the banks' agreed gross limit, in which case covering funds are transferred immediately from sending to receiving bank's settlement account at the Bank of Finland. Only after this can the receiving bank pay the payee.

Smaller payments are handled by netting, based on bilateral net positions. As regards such a payment, the receiving bank pays the payees immediately but does not obtain funds from the sending bank

until the bilateral net position exceeds the 'warning trigger', which is equal to the gross limit. Both banks calculate and monitor the two-way payment flows and bilateral net position, which must be equal in magnitude but of opposite sign.

Risk mitigation in POPS – gross settlement and limits

In POPS, bank credit risk between banks is controlled via net limits, as regards individual payments that are smaller than the gross limit. The net limit, which is twice the gross limit, is also the maximum allowable bilateral risk. System participants agree on bilateral limits, which cannot exceed the maximum set by the Bank of Finland.

The maximum total credit risk of a single bank in the POPS system is the sum of net limits it has granted to counterparty banks. The risk is virtually never that large, since banks transfer covering funds to each other throughout the day and two-way bilateral payment flows are typical.

As regards payments that exceed the gross limit, credit risk does not occur in the POPS system, as covering funds move between banks prior to entries in customers' accounts.

Clearing and settlement risk is mitigated in POPS by means of the rules on settlement finality and irrevocability.

The technical operability and reliability of the system also helps to mitigate clearing and settlement risks, as do the pre-agreed backup systems. Since collateral is not used in the POPS system, there are no risks associated with collateral.

6.3 PMJ – interbank payment system

Retail payment system based on batch transfers

PMJ is an interbank retail payment system, based on batched transfers, in which transaction details move from bank to bank via the banks' own information transfer network. The banks themselves created and continue to operate the system.

In PMJ clearing, the difference between system outgoing and incoming payments is calculated daily for each bank vis-à-vis each of the other banks. For each pair of banks, the one with the net debt transfers funds in that amount to the other one across accounts at the Bank of Finland. Clearing and settlement take place twice daily. In

Finland there is no separate clearing house for such bank fund transfers. Details on PMJ are given in Annex 5.

PMJ risks have been reduced

In PMJ, the banks no longer have credit risks vis-à-vis other banks, because payment funds are always transferred between banks before corresponding entries are made to customers' accounts. If the sending bank's account at the Bank of Finland does not have sufficient funds to cover a payment, corresponding customer-account entries are not made at the receiving bank.

Because of the PMJ's technical reliability and agreed backup systems, clearing and settlement risks are minor. Risks are also reduced by system rules that ensure that settlements are final and irrevocable. Because collateral is not used in the PMJ, there are no corresponding risks.

6.4 POPS and PMJ meet central banks' requirements

The Bank of Finland has designated POPS and PMJ as systems that must meet the basic requirements of G10 central banks for payment systems that are significant for systemic risk (section 3.3.1). In its spring-2001 evaluation of the two systems, the Bank of Finland determined that both systems met the above-mentioned basic requirements. IMF experts came to the same conclusion in their spring-2001 systems evaluation within the Financial Sector Assessment Programme (section 3.3.2). As part of its overseer function, the Bank of Finland continuously monitors these systems for compliance with the basic requirements.

6.5 Banks' links with international payment systems

Banks' links with international payment systems have changed greatly in recent years. In Europe, the traditional means of transferring payments abroad, via correspondent banks, has been joined by important new euro area payment systems since the introduction of the

euro. EU area central banks created the TARGET system and the bank-administered Euro Banking Association developed the Euro1 and STEP1 systems. Interbank currency trading was also revamped when the Continuous Linked Settlement (CLS) Bank commenced operations in September 2002. International payment systems are still undergoing significant changes, and it is clear that, at least in the euro area, more new systems are on the way.

6.5.1 Correspondent banking system

The traditional way of handling foreign payments is to use a network of foreign correspondent banks. Establishment of new payment systems, especially in the euro area, has led to a decline in the use of correspondent banks, albeit such networks are still necessary. The correspondent banking system is based on payment transfer services rendered by banks in one country to banks in another country. The terms and conditions of the arrangements are agreed beforehand by the participating banks.

There are two levels of correspondent banking relationships. In the broad arrangement, banks open accounts in their correspondent banks, and payments are forwarded via these accounts. In the narrow arrangement, correspondent banks exchange SWIFT[14] keys, which enable interbank transfers of payment messages. Here, covering funds are transferred across accounts at settlement banks. Use of correspondent banking relationships is declining in the EU area, in connection with the introduction of the common currency and development of new euro payment systems.

Credit and liquidity risks are associated with the use of correspondent banks because payment-covering funds move through settlement banks chosen by the sending bank. Each bank must itself assess and evaluate the settlement bank's financial condition.

Besides bilateral correspondent banking relationships, there are also multicentred systems for cross-border payments, mainly for banks operating in Europe. One example is the Eurogiro system for postal banks, which includes the Finnish Sampo Bank. Banks in the Eurogiro system have agreed on timing and other conditions for payment transfers. Customers in all countries receive the same level of services.

[14] Society for Worldwide Interbank Financial Telecommunication.

6.5.2 TARGET system

The TARGET (Trans-European Automated Real-Time Gross Settlement Express Transfer) system is an RTGS system for payments between EU-area central banks. It comprises 15 national RTGS systems and the ECB's payment mechanism, which are interlinked to form a single system covering the EU area. In the TARGET system, more than 5,000 credit institutions in the EU area are able to make euro-denominated payments to each other via their own national RTGS systems. The Finnish part of the system is the BoF-RTGS, which is maintained by the Bank of Finland.

In TARGET all payments are processed in the same way regardless of size. To effect a cross-border credit transfer via TARGET, the participating bank sends a payment order (per national standards) to the respective RTGS system; the TARGET system handles the rest. The receiving bank receives the payment information in accord with its own national standards.

TARGET is used for conducting monetary policy operations and executing international payments related to Eurosystem currency operations, as well as for executing settlements for large-value cross-border payment systems that operate on the netting principle. A small number of international customer payments for banks of different countries are also handled via TARGET.

All TARGET payments are irrevocable. Because the sending bank's account at the central bank is debited before the receiving bank's account is credited, the receiving bank is always certain to get the funds. Thus there are no credit or liquidity risks for the receiving bank.

6.5.3 EBA payment systems

When the euro became the common currency of the euro area, a process of rapid development of new EU-wide payment systems was set in motion. The Euro Banking Association (EBA) has been active in developing and offering services related to euro-denominated payments. Its Euro1 system commenced operations immediately after euro introduction, and its STEP1 system was launched in November 2000.

6.5.3.1 Euro1 payment system

Euro1, operated by the EBA, is an interlinked EU-wide system for European banks' large and medium-size euro-denominated net payments. It is one of two (with TARGET) centralised cross-border payment systems operating in the EU area. Euro1 is the successor to the ECU Clearing system, which commenced operations at the start of 1999. At the start of 2003 there were 73 members of Euro1, including three Finnish banks and three foreign banks operating in Finland.

Euro1 operations utilise the SWIFT network used by international banks. System members can send payment orders via Euro1:n directly to payees' settlement banks. Euro1 calculates participating banks' net positions in real time. In order to reduce risks, there is a position limit for each bank, which cannot be breached during the day. At the end of the day, banks with negative positions send covering funds through their national central banks and TARGET to Euro1 accounts at the ECB. Following this, the banks with positive positions correspondingly receive funds via TARGET.

Euro1 is based on the Single Obligation Structure. This means that at any moment each participating bank has only one position (positive or negative) vis-à-vis all other participating banks. That position changes in real time with every payment received or sent. Payments are final and irrevocable as soon as they are processed.

As a means of reducing credit and liquidity risks, each bank sets a bank-specific credit limit (EUR 5–30 m) for each of the other banks. Each bank then has two total limits: the sum of all credit limits granted to and by it, vis-à-vis all the other banks. Neither limit can exceed EUR 1 billion.

In order to ensure success of end-of-day settlements even when some banks lack sufficient liquidity, the ECB maintains a liquidity pool (EUR 1 bn), to which all the banks contribute equal amounts. If the pool proves to be insufficient, the participating banks are obliged to cover the shortfall.

6.5.3.2 STEP1 payment system

STEP1, which is similar to but smaller than Euro1, is also used for transferring euro-denominated payments. The EBA initiated this service in November 2000. STEP1 provides EU area banks with a simple and fast means of transferring small cross-border euro-denominated payments. Some 50 banks participate in STEP1, but all

banks that use Euro1 have access to STEP1 services. Three Finnish banks are regular members of STEP1. So far, STEP1 has not handled very large numbers of payment transfers.

STEP1 is for payments of up to EUR 50,000 euro. Payment delivery time is two banking days. Membership requires that the bank have a branch in the EU area and an agreement with a Euro1 system bank on transferring covering funds.

STEP1 enables payment connections between all EU area banks that are members of Euro1 or STEP1. However, Euro1 banks do not generally use STEP1 services if the receiving bank is a Euro1 bank since the Euro1 system is faster.

Covering funds are netted, and the net debts are guaranteed by the STEP1 bank's settlement bank in the Euro1 system. To avoid credit and liquidity risks, STEP1 banks cannot credit customers' accounts for incoming STEP1 payments before covering funds are transferred via the Euro1 system. Covering funds are transferred immediately after 4 pm. STEP1 banks cannot cancel a payment order after 6 pm on the day preceding the value date.

6.5.4 CLS system

Settlement risk in foreign exchange transactions[15] and stability of international currency markets are of major concern to central banks because of the large and continually growing trade volumes involved. According to a report published in 1996 by the Bank for International Settlements,[16] settlement risk positions of large international banks in respect of foreign exchange transactions could increase to many times their equity capital. In Finland too, these risks have been estimated as being at a level that could exceed the banks' capacity to bear such risks.

In order to reduce currency settlement risks, the large international banks jointly established the CLS (continuous linked settlement) Bank. Its purpose is to eliminate settlement risk for currency transactions handled within the system. The CLS Bank, which commenced operations in September 2003, provides banks with

[15] Per BIS definition, a bank's settlement risk in an FX transaction, ie settlement risk position, equals the amount of foreign currency purchased. The period of risk begins when the bank can no longer on its own initiative cancel the payment order for its sale of currency and ends when the bank is finally determined to have received its purchased currency.

[16] Settlement risk in foreign exchange transactions. BIS, March 1996.

services connected with settlement of foreign exchange transactions. These services help to eliminate this type of settlement risk because the currencies involved in a trade are transferred simultaneously according to the payment versus payment (PVP) principle. Finnish banks also intend to use the services of CLS Bank.

The service began with seven currencies: US dollar, Japanese yen, euro, UK pound sterling, Swiss franc, Canadian dollar and Australian dollar. Banks can join the CLS Bank's settlement system directly as a shareholder by opening an account at CLS Bank, or by enlisting the services of a settlement/clearing bank.

7 Capital requirements and payment system risks

According to planned changes in international capital adequacy requirements, banks' equity capital will for the first time, also have to cover payment system risks. In practice, this will be accomplished by means of equity requirements for operating risks, one component of which is payment system risks. A brief description follows of the new capital requirements, calculation of the equity requirements for operational risks, and their relation to payment system risks.

7.1 Proposed new capital requirements

In an effort to internationally unify requirements for bank capital, which had long existed at national level, the BIS in 1988 introduced the Basel Capital Accord, which provided a general framework for capital adequacy requirements. The Accord, which was drawn up by the Basel Committee on Banking Supervision under the aegis of the BIS, defined a method of calculating capital adequacy using fixed credit risk weights and set a standard minimum requirement for all banks at 8% of weighted capital. The capital requirements were recommended for application not only to international banks but also generally to all banks in industrial countries. The 1988 Accord represented an attempt to prevent unhealthy competition between countries – based on bank capital requirements - and to ensure a minimum capital level and thus increase the stability of the international financial system.

Further development of the capital requirements ensued in 1999-2001 with the Basel Committee's reform proposal.[17] The aim of the effort was to put in place requirements that would better reflect risks associated with banking and to offer banks and bank supervisors several alternative ways of defining capital adequacy. The reform was divided into three pillars. Pillar 1 deals with minimum capital requirements for credit risks, market risks, and operational risks, pillar 2 with supervisory review of institutions' assessment of these risks,

[17] See FSA statement T/37/2001/TTO, 17 Jan 2001, and A Proposal for a New Basel Capital Accord. Basel Committee on Banking Supervision. Bank for International Settlements, 16 Jan 2001.

and pillar 3 with increasing market discipline through effective disclosure.

It has been intended to include banks' operational risks in the scope of capital adequacy regulation so that these would be subject to quantitative capital requirements. The reform will enter into effect in 2006 at the earliest.

While the Basel Committee was working on the new capital accord, the European Commission published a proposal in February 2001 on reform of the capital adequacy framework for EU credit institutions and investments firms.[18] The Commission's proposal observes the main principles of – and is complementary to – the Basel Committee's proposal for reform of the international capital adequacy framework. The Commission's proposal includes the same three main principles, as does the Basel proposal. The capital adequacy directive drafted by the Commission on the basis of the new framework is scheduled to enter into effect in the member states at the start of 2006, along with the Basel Committee's reforms.

7.2 Operational risks – concept and calculation methods

In a working paper[19] published in September 2001 the Basel Committee defined operational risk as 'the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events'. Systemic risk was not to be included in operational risk but rather to be treated separately in setting capital standards. A key issue in measuring and setting institution-specific standards for operational risk is the collection of loss data. Another problem is that there are no bank standards for operational risk, so that the scope of operational risk may vary from bank to bank.

Under the new capital rules regarding payment and securities settlement systems, a large part of the associated risks are also operational risks. For this reason, these – along with banks' other operational risks – fall within the scope of the capital requirements.

[18] European Commission discussion paper on the reform of the capital adequacy framework. See also FSA statement T/39/2001/TTO, 7 Feb 2001, and Comission Services' Second Document on Review of Regulatory Capital for Credit Institutions and Investment Firms. European Commission, 5 Feb 2001.

[19] Working Paper on the Regulatory Treatment of Operational Risk. Basel Committee on Banking Supervision, Bank for International Settlements. Sep 2001.

The greater risk orientation of the new rules underlines the importance of recognition, control and limiting of these risks. In order to identify and take account of the average risk level in the rules, it is important to obtain reliable data on realisations of payment and settlement system risks, as well as other operational risks.

Below, we introduce the Basel Committee's three alternative approaches for taking account of operational risk within the new capital adequacy framework. These are the basic indicator, standardised and advanced methods approaches.

7.2.1 Basic indicator approach

The basic indicator approach gives the bank a simple way of taking account of operational risk in capital requirements. Banks using this approach must hold capital for operational risk equal to a fixed percentage (a), as determined by the Basel Committee, of a single indicator (I), provisionally gross income.

Under this approach, payment and settlement risks are an undifferentiated part of operational risks. The capital requirement for operational risks depends on the values of a and I. The basic indicator approach is a rough and simple way of taking account of operational risk. It does not measure a bank's true operational risk but instead relies on an average capital requirement based on the risk indicator.

The basic indicator approach is intended for use by any banking organisation, regardless of its complexity or sophistication of risk measurement. However, it is presumed by the Basel Committee that supervisors will not permit use of this approach by internationally active banks nor banks subject to notable levels of operational risk. Banks using the approach will be obliged to observe the Committee's recommendations on control and monitoring of operational risks.

7.2.2 Standardised approach

In the standardised approach, banks' activities are divided into eight business lines (L), each represented by its own indicator (I), which proxies the scale of operations in that business line. The idea is that the indicator will also reflect the likely scale of operational risk exposure within the business line. The chosen business lines, one of which is payment and settlement, are as follows.

Business line (L)	Indicator (I)	Coefficient (b)
Corporate finance	Gross income	b1
Trading and sales	Gross income	b2
Retail banking	Av. receivables	b3
Commercial banking	Av. receivables	b4
Payment and settlement	Total turnover	b5
Agency services and custody	Asset value	b6
Asset management	Gross income	b7
Retail brokerage	Gross income	b8

The capital requirement for operational risk in each business line (L) is found by multiplying the corresponding risk indicator (I) by the coefficient (b). The coefficients will be set by the Basel Committee so as to reflect the importance of operational risk to the corresponding business line in banking as a whole. As of now, the provisional risk indicator for all business lines is gross income, which is easy to calculate, comparable across banks, and not easily manipulated. However, other risk indicators could be used – such as average receivables, total turnover, and value of assets managed – which may reflect activity level in certain business lines better than gross income. Final decisions on the indicators have not yet been made.

In this approach, total capital required for operational risk can be found by adding the requirements for each business line. The importance of each business line can also be accounted for through the previously defined weights. For the bank as a whole, this procedure does not measure the true operational risk but instead relies on values calculated on the basis of risk indicators for each business line.

In the standardised approach, payment and settlement systems are treated as a separate business line and the associated risks and capital requirements are calculated separately. This enables assessment of the importance of payment and settlement system risks relative to operational risks of other business lines.

In order for a bank to use the standardised approach, it must have effective methods for controlling, monitoring, measuring, reporting, and assessing operational risks. It must, moreover, observe the Basel Committee's recommendations on sound practices for the management and supervision of operational risk.

7.2.3 Advanced measurement approaches

It is the Basel committee's view that banks and other companies have long experience using highly developed and risk-sensitive methods of measuring operational risk. In these, risk is mathematically derived from internal and external loss data. The Committee is also prepared to accept such values of operational risk as are derived from a bank's own internal measurement systems and models. The Committee is likely to set floor-values based on the capital charge for operational risk derived from the standardised approach.

Several criteria will be set beforehand for banks intending to use advanced measurement approaches. The criteria have not yet been finalised, but the following have been proposed. 1) Supervisory authorities must approve use of the method, 2) operational risk control and monitoring will be subject to certain qualitative standards, 3) the estimation of operational risk must meet certain quantitative requirements 4) there must be a critical mass of banks using the method. An illustration of these criteria is presented in Annex 1 of the Basel Committee's working paper on operational risk.

7.3 Size of capital requirement for operational risk

The Basel Committee initially estimated the average capital charge for operational risk at 20% of the total capital requirement. In light of comments from banks, the Committee was prepared to reduce it to 12% on average, which is more in line with large banks' overall level of operational risks. Moreover, other risk reduction means such as insurance are also to be taken into account.

In order to encourage banks' use of advanced methods and their own models in assessing operational risks, the Committee has considered reducing the related capital charges. The Committee's initial proposal is that the capital requirement applicable to the advanced measurement approach would be 75% of that for the standardised approach. Assuming an average requirement of at least 12% for the standardised approach, this would imply an average requirement of 9% for the advanced approach. The Committee and the banking supervisors are however apparently assuming that banks which use complicated methods and models will generally also use advanced approaches in measuring operational risk in connection with capital adequacy requirement.

The basic and standardised approaches are fairly rough and inflexible means of defining capital requirements in connection with payment and settlement systems. Neither affords a way of precisely calculating banks' capital requirements for operational risk, albeit the latter approach is somewhat more accurate than the other is. Banks that specialise in certain activities could be put at a disadvantage if they use the basic or standardised approach and so they may be forced to resort to advanced approaches.

In the banks' view, a notable problem in this connection is the lack of compensation for investments that reduce operational risk. Nor do these approaches observe true operational risk exposures or changes therein. So far, insurance is the only risk reducing method that the Basel Committee is prepared to take into account.

8 Future developments

Both national and multinational payment systems are entering a phase of significant change. Today's means of payment transfer have been developing in stages over a long period of time. The changes have been marginal; often new solutions are initially effected on a small and limited scale.

A number of signs now suggest a kind of revolution in the offing concerning payment services and standards for payment systems. The major trends affecting regulation and supervision are

- globalisation
- electronification and integration
- increasing speed (complete switch to real time)
- consolidation
- growing payment volumes
- new market participants.

Globalisation means that in the long run payment systems cannot be regulated and supervised at national level. Systems are really international, and national borders become blurred in the new information networks such as Internet. National authorities' remits and tools cannot cope with international provision of services; and customers become less able to comprehend the risks associated with such services. The importance of international cooperation among authorities is growing, as is the need to establish an international authority for regulation-supervision or a cooperative body.

The general trend toward electronification means that supervision is becoming increasingly computer oriented. Supervision of information system structures and security features of systems is a growing part of the supervisory task. Increasing processing speeds and the trend to 100% real time payment processing require supervision and monitoring that are faster and integral to the systems. Authorities must react more quickly to risk situations so as to limit losses and resolve problems. As the degree of electronification increases, the systems become closely integrated and increasingly interdependent. Even a small isolated problem can expand quickly via ICT systems into a worldwide problem, as we have seen in connection with some of the computer viruses. A major challenge now facing regulators and supervisors is how to control an increasingly complex international entity.

The markets and related systems are being linked up to form an ever-expanding entity. As we become increasingly dependent on individual and nearly worldwide systems, the probability of realisation of system risks grows, as does overall vulnerability. For example, huge numbers of the world's large-value payments are transferred via the SWIFT network. Computer problems, labour disputes, terrorist attacks and other similar events have serious consequences in such a consolidated environment. Parallel systems are often so small, in terms of numbers and capacity, that they cannot completely replace the bigger systems in a disruptive situation. Consolidation increases the need for intervention by authorities in order to prevent a too-big-to-fail situation from being realised. The ability to do this requires that various plans for handling emergencies be put in place beforehand.

Payment volumes are partly determined by budget constraints (eg private consumption must correspond on average to private incomes). Organisational combining of companies reduces payment flows between companies. Economic growth, on the other hand, moderately spurs payment flows, but the growth is due mainly to increases in transaction sizes and turnover rates in the currency, money and stock markets. The same types of foreign exchange and money market instruments and shares now change hands more rapidly than before. The transfers often involve huge monetary values, which means the risks arising in a problem situation can be significant, even for the whole financial system. For this reason, authorities are nowadays especially apt to require better control of these risks, which will continue in the future to be a key aspect of supervision.

So far, payment traffic has been generally been considered a segment of banking, and hence oversight and regulation of banks have substantially increased the stability of payment systems. Banks have been slow to create new effective electronic payment services at the international level. Customers' payment habits also evolve slowly. One obstacle to international development has been the pronounced differences across countries in payment modes and services. Here, Finnish banks are an encouraging exception. Nonetheless, the sluggishness of the international banks has led to sector crossovers, ie newcomers bring new services to international markets (for example data transmission firms, retailers, electronic service providers). Most of these companies currently lie beyond the reach of traditional financial supervision and oversight.

On the other hand, banks have also been expanding beyond the range of traditional payment services. These new services are provided by making use of systems developed in connection with traditional payment systems such as third-party customer recognition,

electronic marketplaces, net-based invoicing, invoice information systems, etc. Such developments also require new expertise and capabilities in risk assessment on the part of regulators and supervisors.

A formidable challenge facing authorities responsible for financial stability is to find international supervisory solutions that promote innovation and progress while obviating increased risks and possibilities for regulatory arbitrage. The tools and operating modes for this must be developed so to meet the needs of the electronic and real time operating environment. The risk of regulatory arbitrage increases also if it is possible to avoid regulation and supervision through non-banking services.

International cooperation between authorities has increased continually, and thus regulatory and supervisory structures have become more unified and standardised (examples of cooperation: Basel banking supervision, G10 central banks and the ESCB). Increased openness has facilitated international comparisons in the area of regulation and supervision. A common problem in reforming regulatory-supervisory structures is internal inflexibility, which slows the process of change. If regulation and supervision fall too far behind advancements in payments transmission, payment system risks increase and may be realised in certain subsectors. Control of the change process is one of the major challenges in the offing.

9 A general assessment of Finnish payment system risks

Overall, payment system risks in Finland are quite small and well controlled. Reduction of these risks is due not only to measures taken by the Bank of Finland and FSA. Banks' self-regulation, international recommendations, improvements in the security of data transfer etc have also contributed to the reduction of payment system risks. Moreover, Finnish domestic payment systems now observe the international core principles for systemically important payment systems.

Even though the risks of domestic payment systems are presently minor, the continuously changing economic and technological environment means that payment systems must be continually developed to meet new needs and demands. There is thus good reason for regular examinations and assessments of payment system risks. Over the next few years, the biggest challenges for Finnish payment systems are connected with the adjustment to the Single Euro Payments Area (SEPA). Moreover, expanded use of Internet and other electronic service channels in payment transfers will also demand knowledge and effective use of new recognition and risk control methods.

References

Leinonen, H. – Saarinen, V. (1998) Suomalaiset maksujärjestelmäriskit ja niiden sääntely- ja valvontatarpeet. Suomen Pankki A:100. Helsinki.

Leinonen, H. – Saarinen, V. (1998) Payment system risks in Finland and the need for regulation and supervision. Bank of Finland Studies A:101. Helsinki.

Mayes, D.G. – Halme, L. – Liuksila, A. (2001) Improving Banking Supervision. Palgrave. Hound Mills, Basingstoke.

BIS publications

Report on Netting Schemes (1989). Basel.

Report of the Committee on Interbank Netting Schemes of the Central Banks of the Group of Ten Countries (Lamfalussy Standards) (1990). Basel.

Delivery versus Payment in Securities Settlement Systems (1992). CPSS Publication No. 5. Basel.

Central Bank Payment and Settlement Services with Respect to Cross-Border and Multicurrency Transactions (1993). CPSS Publications No. 7. Basel.

Cross-Border Securities Settlements (1995). CPSS Publications No. 12. Basel.

Settlement Risk in Foreign Exchange Transactions (1996). CPSS Publications No. 17. Basel.

Survey of Electronic Money Development (2000). CPSS Publications No. 38. Basel.

Core Principles for Systemically Important Payment Systems (2001). CPSS Publications No. 43. Basel.

Recommendations for Securities Settlement Systems (2001). CPSS Publications No. 42. Basel.

A proposal for a New Basel Capital Accord. Basel Committee on Banking Supervision. 16 Jan 2001.

Working Paper on the Regulatory Treatment of Operational Risk. Basel Committee on Banking Supervision. September 2001.

ECB and EMI background papers

Minimum Common Features for Domestic Payment Systems (1993). Working Group on EC Payment Systems. Publication series. Frankfurt.

Report to the Council of the European Monetary Institute on Prepaid Cards (1994). Working Group on EU Payment Systems. European Monetary Institute. Frankfurt.

Standards for the Use of EU Securities Settlement Systems in ESCB Credit Operations (1998). European Monetary Institute. Publication series. Frankfurt.

Improving cross-border retail payment services in the euro area – the Eurosystem's view (1999). Publication series. Frankfurt.

Improving Cross-Border Retail Payment Services (2000). Progress Report. Frankfurt.

Role of the Eurosystem in the Field of Payment Systems Oversight (2000). European Central Bank press release. Frankfurt.

Memorandum of Understanding on Cooperation Between Payment Systems Overseers and Banking Supervisors in Stage Three of Economic and Monetary Union (2001). Frankfurt.

Payment and Securities Settlement Systems in the European Union (2001). Blue Book.

ISO publications

Banking, securities and other financial services – information security guidelines (1996). ISO/TR 13569.

FSA notifications

Baselin komitean ehdotus vakavaraisuuskehikon uudistamisesta (2001). Ratan tiedote T/37/2001/TTO, 17 Jan 2001.

Euroopan komission keskustelupaperi vakavaraisuuskehikon uudistamisesta (2001). Ratan tiedote T/39/2001/TTO, 7 Feb 2001.

European Commission publications

Commission Services' Second Document on Review of Regulatory Capital for Credit Institutions and Investment Firms. European Commission, 5 Feb 2001.

Annex 1

Payment system risks

This Annex describes the risks associated with different kinds of payment systems (debit payment instruments, credit transfers, cheques and express transfers) according to the risk classification presented in figure 1. Assessments are also made of Finnish systems in terms of current system-specific (j), bank-specific (p) and systemic (s) risks, using the grading system described above in the section 'Risk measurement'. 'None' indicates the system is judged to be free of the risk in question.

1 Risks associated with debit payment instruments

Risks associated with debit payment instruments are mainly domestic since banks' debit payment instruments are still relatively seldom used abroad. It is likely that foreign risks will increase in the future. In Finland debit payment instruments, especially debit cards, have largely replaced cash as a payment instrument.

1.1 Credit risks

1.1.1 Bank credit risks

Banks engage in short-term financing of transactions initiated with debit payment instruments since an interbank settlement is generally executed only after the receiving customer's account is credited. Debit cards carry a guarantee of EUR 150. In this regard, there is a difficult legal question: In case of insolvency of the card-issuing bank, is it or the redeeming bank responsible for the seller's guarantee?

Electronic cash may replace a portion of debit card payments and correspondingly alter banks' credit risks.

Use of debit payment instruments may give rise to a degree of bank risk if payments credited to customers' accounts involve a large number of large-value payment instruments certified by other banks, such as cheques and debit card payments.

(Risk grades: j = none, p = none, s = none)

1.1.2 Customer credit risks

A guarantee on a debit card entails risk for the card-issuing bank. If the issuing bank credits the merchant's account for transactions beyond the value of the card guarantee especially when there is no verification of covering funds, the bank bears a credit risk in case claims are filed. Quick crediting of merchants' accounts for card payments is a competitive tool that is difficult to abandon. However, the credit risks involved are not significant except in situations where the bank does not verify unusually large transactions or turnovers.

(Risk grades: j = none, p = none, s = none)

1.2 Liquidity risks

Transactions in debit payment instruments rarely entail liquidity risk because their total monetary value is a small share of that for all payment transfers. These transactions are processed in the PMJ clearing system and are relatively well in balance among banks and predictable.

(Risk grades: j = none, p = none, s = none)

1.3 Operational risks

1.3.1 Information system risks

The processing of transactions in debit payment instruments can be characterised as decentralised, batch, non-urgent, and off-line. For this reason, they are secured by manual backup systems. The risks involved are thus due mainly to traditional possibilities for errors, such as multiplication, destruction, or distortion of transaction data, which can be corrected fairly quickly after detection. The only critical areas are bank-specific online authorisation systems and PIN code control systems.

(Risk grades: p = minor, j = none, s = none)

1.3.2 Administrative risks

Administrative risks are connected with safe custody of payment instruments and timely updating and accuracy of the contents of information systems. Electronification is increasing the need for secure and effective controls for card systems. Loss or the falling into criminal hands of PIN code keys create substantial risks. Switching to smart cards expands the possibilities for protection but also introduces a new potential source of administrative risks. A wide disruption of security systems may cause a system-specific crisis, which can lead to a temporary shutdown – for example of a debit card system – for repairs or changes in security arrangements.

(Risk grades: j = minor, p = none, s = none)

1.3.3 Crime risks

Debit cards can be used to obtain cash and other items of value. Card payment transactions are partially protected by personal identification numbers (PIN codes). If bank employees work with crime organisations, fairly large losses can result. While the smallness of the transactions helps to contain losses, organised crime is nonetheless becoming increasingly active in this area. These risks are being reduced by the introduction of smart cards, increasing emphasis on online transactions, and the use of statistical verification methods.

Debit payment instruments always entail various risks of misuse, albeit the situation in Finland is fairly good by international standards. Because these risks are increasing, prudence argues for replacing magnetic-strip cards with more secure smart cards within the next few years. Wide use of off-line EFTPOS systems and slow updating of 'hot card files' enable misuse eg using stolen or found payment cards. However, realisation of these risks has not yet destabilised payment card services. Investments in this area can be partially based on statistical methods. For example, a wide wave of organised counterfeiting could trigger temporary restrictions on use of debit cards in order to enable improvement or revamping of the security systems.

(Risk grades: j = minor, p = none, s = none)

1.4 Environmental risks

1.4.1 Risks of change in legislation or market practices

As regards debit payment instruments, consumer protection and other authorities have continually reduced customer risks at the expense of the banks. Banks cannot expect customers to bear unreasonably large risks, which are – from the banks' perspective – relatively small.

(Risk grades: j = none, p = none, s = none)

1.4.2 Loss-of-confidence risks

Debit payment instruments entail significant risks of loss of confidence (as in the effect of genuine-looking counterfeit banknotes on the confidence in cash). A massive and successful counterfeiting operation could cause loss of confidence in a debit card system. A wave of bank insolvencies in which merchants suffer financial losses could also cause a serious loss of confidence.

(Risk grades: j = minor, p = none, s = none)

1.4.3 Technological change risks

The introduction of the microchip-based smart card has an impact on the technology and use of debit cards. Popularisation of supranational smart card systems or e-money issued by the central bank can considerably reduce the use of debit cards. New systems may in certain circumstances quickly displace old practices. Electronification also increases dependence on technology and its specialised suppliers. Failure of the electronics or system obsolescence may force a rapid modification of the system and hence greater investment costs.

(Risk grades: j = minor, p = none, s = none)

1.4.4 Catastrophe risks

Catastrophe risks are associated mainly with the use of electronic debit payment instruments, ie magnetic cards and (in future) smart cards. If a malfunction occurs in a key ICT system, these payment

instruments become difficult to use. The high degree of concentration in the Finnish banking sector means that if a catastrophe were to render dysfunctional the ICT equipment or systems of two large banks for a fairly long time, it would become difficult to use electronic debit payment instruments in Finland. On the other hand, the banks' ICT systems are relatively secure.

(Risk grades: j = minor, p = none, s = none)

1.5 Clearing and settlement risks

1.5.1 Systems risks

Settlement of transactions in debit payment instruments is done in the BoF-RTGS in connection with PMJ clearing. The timing of these settlement transactions is not critical, and the associated clearing risks are not significant.

(Risk grades: j = none, p = none, s = none)

1.5.2 Collateral risks

In Finland collateral is not used in the settlement of debit payment transactions. The sending bank can simply charge the account holder's bank. The account holder's bank can verify the authenticity of the transaction only ex post and then, if the transaction is faulty, revoke it. The rules and participation criteria for settlement must permit stoppage of faulty transactions in all situations.

(Risk grades: j = none, p = none, s = none)

1.5.3 Settlement cancellation risks

Settlement of transactions in debit payment instruments is based on multilateral netting. Under current law, a netting cannot be unwound, even in the event of bank failure. Compared to other instruments, debit payment instruments account for a small share of total settlements.

(Risk grades: j = none, p = none, s = none)

1.6 Systemic risk

Apparently realisation of systemic risk specifically in connection with debit payment instruments would be a rarity, except in the case of a massive counterfeiting operation. While the use of cash is on the decline, these instruments are gaining importance. In the long run, dependence on electronic debit payment instruments will increase the danger of technology-related systemic risk in this subsector of payment transfers.

(Risk grades: j = none, p = none, s = none)

1.7 Summary of risks associated with debit payment instruments

The risks associated with debit payment instruments are fairly small. The more important ones are information system risks, administrative risks, crime risks, loss-of-confidence risks, technological change risks, and catastrophe risks.

Debit payment instruments do not entail bank-specific risk nor systemic risk.

2 Risks associated with credit transfers

Credit transfers are the main payment instruments in Finland. Volumes are large, and customers depend heavily on reliable operation of the credit transfer system, which is almost completely electronified.

2.1 Credit risks

2.1.1 Bank credit risks

These risks have been eliminated, as covering funds move between banks before entries are made to customer accounts.

(Risk grades: j = none, p = none, s = none)

2.1.2 Customer credit risks

Banks do not encounter customer credit risk in connection with credit transfers. Covering funds are verified and reserved in the payer's account before the payment is executed. If funds are insufficient, the payment order is held up until sufficient funds arrive. Cover verification is one of the basic requirements of risk management. In a few Finnish banks, certain large customers' cover is checked against 'technical limits' or such a cover check is not made at all if there is in effect an agreement on non-verification of cover.

The bank is responsible for a funds transfer it has accepted and must refund diverted or lost funds according to its agreement with the customer, the principles of contract law, and the general terms and conditions of domestic payment transfers.

(Risk grades: j = none, p = none, s = none)

2.2 Liquidity risks

Net clearing and settlement of credit transfers in the BoF-RTGS, which takes place at the end of the day and in the night clearing, reduces banks' liquidity needs compared to the gross payments involved. Netting also reduces the potential realisation loss but shifts the timing to the following morning.

If all the credit transfers of a single large bank to other banks fail because covering funds are not transferred, whether due to the bank's lack of liquidity or insolvency, liquidity problems could spread to other banks, which would entail a degree of systemic risk.

(Risk grades: j = none, p = minor, s = minor)

2.3 Operational risks

2.3.1 Information system risks

In Finland the processing of credit transfers is decentralised; there are no clearing houses. Payment information is exchanged bilaterally between banks several times a day on a batch basis, but clearing and settlement are handled centrally at the Bank of Finland. The advantage of a decentralised versus a completely centralised system is less vulnerability. Because daily transaction volumes are large, it is crucial

the banks' information systems and transmission links function reliably.

The risks of brief disruptions, however, are not large since relatively small monetary values are at stake because the transactions are small and value dates lagged.

If the credit transfer system of a bank is paralysed for an extended period, a bank-specific risk may arise as customers shift their credit transfer business to other banks. It is also possible that the large number of small-value transactions in the information system will increase manifold or melt away, which could give rise to a big risk despite the smallness of the individual transactions.

Payments executed via terminals located in companies, homes etc are particularly dependent on the smooth functioning of ICT and security systems.

(Risk grades: j = minor, p = minor, s = minor)

2.3.2 Administrative risks

The manual phases of payment transfers are especially vulnerable to errors and misuse. The changeover to electronic payment processing has reduced errors (for example transfers to wrong accounts and data corruption or loss) and enabled computerised controls.

The shifting of large urgent (express) credit transfers to the RTGS and POPS system has reduced the risks and enabled the introduction of control limits.

Staff incompetence and human errors, carelessness in effecting payment transfers and maintaining systems, neglect of control and reporting procedures, or failure to provide instructions for the use of backup systems in the event of a disturbance may lead to situations wherein customers' orders are delayed or not executed. Credit transfers may go to the wrong accounts and transaction information may be corrupted or lost due to various kinds of errors. Banks are generally able to correct individual errors, but simultaneous occurrence of a number of large errors may lead to a situation that is difficult to manage and thus, in the absence of clear instructions, create a serious problem.

(Risk grades: j = none, p = minor, s = minor)

2.3.3 Crime risks

Criminal activity in connection with credit transfers may occur outside or inside the bank and may be based for instance on someone making credit transfers using the name and account data of a genuine sender but directing the funds to his own or an accomplice's account. This may be done, for example by creating an unauthorised order in someone else's name, by forging someone else's order, or by appropriating a security code that has not been kept secure. By multiplying manifold genuine transactions and transferring the funds to his own account, a criminal can cause significant losses. A criminal tries to act quickly so as to obtain funds before anything is noticed. In this, he is aided by modern fast ICT systems.

The security risk in interbank express credit transfers was reduced with the introduction of the POPS system. Since there is still a risk in transactions between customer and bank if the bank accepts customers' orders by phone or fax, this practice is not recommended.

The risk of fraudulent payment orders also exists in the provision of payment services since customers' signatures on payment orders are not fully verified in all banks.

Crimes related to electronic services are continuously on the rise, so that banks need to maintain and enhance the security systems used in remote electronic services provided for example in the Internet environment. The international risks of remote operations are obvious in connection with Internet.

(Risk grades: j = minor, p = minor, s = none)

2.4 Environmental risks

2.4.1 Risks of changes in legislation or established banking practices

Established practices regarding customer payments with credit transfers have long been based on standard agreements between customer and bank. These include general clauses for example on refund procedures in cases where bank or customer is guilty of faulty operations. In disputed cases, the consumer ombudsman and the courts have usually protected the weaker party, ie the customer. Because of the small values of credit transfers and rarity of disputes, banks generally have carried only minor risks in this connection.

Interbank exchanges of credit transfer information and covering funds are based on interbank agreements.

Recent legislation on finality and validity of netting of payments and settlement has made it easier to assess the risks and clarified the situation also for the customer.

(Risk grades: j = none, p = none, s = none)

2.4.2 Loss-of-confidence risks

A loss-of-confidence risk could arise in the banks' credit transfer system if individual payments do not go through in the proper amounts or if a participating bank is unable to transmit outgoing and credit incoming credit transfers to customer accounts. Particularly serious problems may result if the wage or benefit payments of a large payer (for example nation pension benefits) are not timely entered into payees' accounts. The cause might be a technical or liquidity disturbance or an insolvency. A quick resolution of the problem is crucial in order to prevent the expansion of a bank-specific risk into a threat to confidence in the whole system and further into a systemic risk.

A massive counterfeiting operation could also weaken customers' confidence in a particular payment system.

(Risk grades: j = minor, p = minor, s = minor)

2.4.3 Technological change risks

The banks' payment transfer system is completely automated, technically of high quality and reliable, and it is an inexpensive means of handling large payment volumes. In technical terms, it competes with various services provided via data networks, eg inexpensive Internet payment services, which combine product ordering and payment into a single service. The most serious problems continue to be the guaranteeing of adequate security and gaining of public confidence. The numbers and values of transactions are small. Thus it is unlikely that in the coming years significant volumes of credit transfers will be handled outside the banks' payment systems, especially since banks are offering their own services also via Internet.

In certain situations, failures or ageing of security systems could call for rapid changes.

(Risk grades: j = minor, p = none, s = none)

2.4.4 Catastrophe risks

The banks' credit transfer system is highly dependent on ICT, which makes it vulnerable to electricity interruption, flood damage, fire, sabotage, terrorist attack, etc. The decentralised structure of the system does however reduce the vulnerability. Because of the risks of catastrophe, banks' need their own backup systems, which should be tested at regular intervals to ensure the possibility of quick start-up when needed.

Banks' computer centres and other premises are traditionally well protected against external threats, and banks generally develop different types of backup systems. However, the level of readiness of these systems varies across banks.

In the event of a catastrophe, a major problem for an individual is how to pay bills and withdraw money from his account if his bank should become unable to operate. For a big company, the problem is to determine quickly the stage of its payments at the time a bank withdraws from the payment system, so that payments can be rerouted through another bank if necessary.

(Risk grades: j = minor, p = minor, s = minor)

2.5 Clearing and settlement risks

2.5.1 Systems risks

The Bank of Finland acts as a clearing and settlement centre for credit transfer covering funds going to banks. For this reason, it is important that these central banking functions and systems not become inoperative and thus cause a shutdown of the whole credit transfer process. It is essential that the Bank of Finland have backup systems and agreed operating procedures for clearing and settlement in case of an internal technical disturbance. Insolvency of a system participant will cause an interruption of transmission of its credit transfers and possible liquidity problems for other participants.

Repeated errors will lead to removal of a bank from the clearing process, so that there is little chance of taking advantage of potential misuse situations. Finnish banks' current practice is to compare the clearing information in transmitted payment messages.

(Risk grades: j = none, p = minor, s = minor)

2.5.2 Collateral risks

In Finland interbank clearing is carried out without collateral.

(Risk grades: j = none, p = none, s = none)

2.5.3 Settlement cancellation risks

Clearing is based on multilateral netting, which cannot be unwound under current PMJ rules.

(Risk grades: j = none, p = none, s = none)

2.6 Systemic risk

The danger of credit transfer risks expanding into systemic risk is very small.

(Risk grades: j = none, p = minor, s = minor)

3 Risks associated with cheques and bank drafts/cheques

Regular use of cheques and bank drafts is concentrated in securities trading and companies' payments between banking groups. Use of cheques in securities transactions has decreased, as these have been largely displaced by express transfers. Large cheques are still used fairly widely for making international payments.

3.1 Credit risks

3.1.1 Bank credit risks

The limits applied in the POPS system have effectively reduced bank credit risks. If a cheque is to be redeemed via the POPS system, the receiving bank cannot credit the amount to a customer account until it has received covering funds from the sending bank. Hence the redeeming bank does not bear a bank credit risk. For small-value cheques for which payment-specific cover is not transmitted and for which the PMJ system is used as a backup system for redemption, there exists a bank credit risk, amounting to the limit agreed between the two banks.

(Risk grades: j = none, p = minor, s = minor)

3.1.2 Customer credit risks

The sending bank bears the customer credit risk when the PMJ system is used for backup in cheque redemption if no reservation of covering funds is made by phone. When the POPS system is used, this risk is eliminated by automatic, immediate reservation of covering funds from the customer's account.

(Risk grades: j = none, p = minor, s = minor)

3.2 Liquidity risks

Individual sums transferred by cheque can be quite large. Large-value cheques are nowadays used especially when large corporate customers shift funds across their own accounts at different banks and in connection with securities transactions. Developments in payment methods in securities markets have reduced the risks associated with the use of cheques in securities transactions.

(Risk grades: j = none, p = minor, s = minor)

3.3 Operational risks

3.3.1 Information system risks

Normal processing of cheque transactions is still done manually, since customers' cheques are delivered physically to banks. Presentments and receipts of cheques trigger corresponding entries in bank information systems. Interbank clearing and settlement of cheques is done on a net basis in the POPS system, except when cheque value exceeds the POPS gross limit, in which case it is handled on a gross basis in the BoF-RTGS. Large-value cheques can also be processed manually, so that system-specific and systemic risks are obviated.

(Risk grades: j = none, p = minor, s = none)

3.3.2 Administrative risks

The banks' current practice of agreeing with large customers on daily non-verification of cover in connection with payment transaction accounts increases banks' customer risks.

In some cases, a bank executes a transaction for a customer that irrevocably obligates the bank but does not require immediate funds transfer from the customer's account. However, in doing this, the bank is (irrevocably) obliged to send covering funds later to the receiving bank. If in such case the sending bank does not reserve cover in the customer's account, it exposes itself to a credit risk. But, because the cause of the risk is in the bank's internal procedures, it is treated as an administrative risk.

Special care must be taken in the physical processing, safekeeping, archiving, and signing of cheques. The bank's processing procedures should ensure that persons responsible for processing and safekeeping of cheques do not also have the authority to sign them. Special attention should be paid to the cheques' safekeeping, record-keeping, and removal from the vault.

Careful observance of procedures is crucial in accepting cheques. It is the bank's duty to verify the amount of a cheque and the authenticity of the signatures. A bank is also obliged to identify stolen cheques that are reported to it.

(Risk grades: j = none, p = minor, s = none)

3.3.3 Crime risks

It is possible to forge cheques and bank signatures. Cheques and bank drafts can also be stolen and misused. Increased forging activity has forced banks to limit cheque sales to persons and companies that are known to be reliable users of cheques. Doubts about possible forgeries may cause banks to delay cheque honouring by submitting them for collection. Criminal activity aimed at an individual small bank may cause a bank-specific crisis.

(Risk grades: j = none, p = minor, s = none)

3.4 Environmental risks

3.4.1 Risks of changes in legislation and banking practices

In Finland, legislation and banking practices regarding cheques are stable and the velocity of cheque circulation is very high.

(Risk grades: j = none, p = none, s = none)

3.4.2 Loss-of-confidence risks

Overall confidence in cheques is good, but large-scale misuse could necessitate a switch to more secure payment practices. An individual bank could face a situation where its cheques are no longer trusted.

(Risk grades: j = minor, p = minor, s = none)

3.4.3 Technological change risks

Paper-based cheques seem to be persevering as a payment means despite the development of new electronic payment media. It does however seem that changeovers to new technologies will happen in a controlled manner, without interruptions to bank operations or systems.

(Risk grades: j = none, p = none, s = none)

3.4.4 Catastrophe risks

In Finland settlement of cheque transactions depends on the POPS and RTGS systems. Catastrophes affecting these systems could cause risk realisations that would affect the use of cheques. Realisation probabilities for bank-specific and system-specific risks are however very small.

(Risk grades: j = none, p = minor, s = none)

3.5 Clearing and settlement risks

3.5.1 Systems risks

In the POPS system, covering funds for cheques exceeding the gross limits are immediately transferred one-by-one in the BoF-RTGS. Covering funds for smaller cheques, in contrast, are transferred after netting. Receiving banks present cheques to sending banks for payment subject to bilateral net limits.

The BoF-RTGS has strict requirements for operational reliability since even a brief interruption of services could expose participant banks to cumulating bank-specific risks so long as the real time settlement is delayed.

Numbers of large-value cheques are so small that clearing and settlement even can be done manually.

(Risk grades: j = none, p = none, s = none)

3.5.2 Collateral risks

Collateral is not used in interbank clearing and settlement.

(Risk grades: j = none, p = none, s = none)

3.5.3 Settlement cancellation risks

Under present legislation and POPS rules, netting cannot be unwound.

(Risk grades: j = none, p = none, s = none)

3.6 Systemic risk

Realisation of systemic risk in connection with large-value cheques is possible but highly unlikely. But misuse within a bank is more likely. This could result from a breakdown of internal controls and resultant exposure to customer-specific misuse, even to the extent of threatening a small bank's liquidity position.

(Risk grades: j = none, p = minor, s = minor)

4 Risks associated with express transfers

Express transfers account for a notable share of the value of payment flows and are particularly important as regards payments in the money and investment markets.

4.1 Credit risks

4.1.1 Bank credit risks

A payee's bank bears a bank credit risk if it credits the payee's account before covering funds are transferred. The situation has been corrected in Finland by the introduction of POPS limits and handling of loro payments as RTGS payments, so that bank credit risk has been eliminated from the domestic payment systems.

The receiving bank encounters a bank credit risk if the sending bank's responsibility for payment delivery does not end with the transfer of funds and payment information. In this connection, there is some uncertainty about the application of Finnish legislation as regards the sending bank's responsibility for payment delivery.

(Risk grades: j = none, p = none, s = none)

4.1.2 Customer credit risks

Banks bear customer credit risks when they forward express transfers without verifying covering funds. Some banks have agreed with large corporate customers on non-verification of accounts on the assumption that funds will arrive later in the day. In such case, the

bank is extending intraday uncollateralised credit. These risks have been reduced inter alia by verifying cover of intraday customer limits.

(Risk grades: j = none, p = none, s = none)

4.2 Liquidity risks

The sending bank needs liquidity in order to transfer funds to the receiving bank (whether for net settlement or RTGS transfer). Liquidity risk has increased because RTGS transfers are handled on a gross basis and POPS limits may be 'emptied' during the day. If transaction processing is skewed over the course of the day (outgoing payments processed first and incoming later), some banks may have huge liquidity needs while others have surpluses.

There is also the danger of a large bank overestimating its liquidity position and thus creating a liquidity shortage that lengthens payment queues for all the banks and causes system gridlock.

(Risk grades: j = none, p = medium, s = medium)

4.3 Operational risks

4.3.1 Information system risks

Information system risks are significant in connection with express transfers because the effects are noticed immediately in real time systems. Express transfers have tight schedules and customers depend on timely execution. Banks still enter some of their funds transfer transactions in the BoF-RTGS manually, which slows the processing and creates additional risks.

If information systems are not functioning properly, transaction data may be multiplied or lost. Few banking systems have control limits for ensuring that large-value payments remain within statistically defined limits.

Management of information systems associated with large-value payments is made easier by the relatively small number of such transactions, which means that a significant share of payments can be processed manually in an exceptional situation.

(Risk grades: j = none, p = minor, s = minor)

4.3.2 Administrative risks

A significant risk associated with large-value payments is that the credit may be made to the wrong account. Currently, payments are credited to accounts strictly on the basis of account number, even though the customer is also asked to provide the payee's name.

(Risk grades: j = none, p = medium, s = minor)

4.3.3 Crime risks

A criminal may seek financial gain by sending an unauthorised payment order to a bank in another person's name or forging another person's order. This type of operation is made easier by defects in the verification of order authenticity. To a certain extent, express transfers can still be sent electronically by way of non-secret data transfers. Paper-based express transfers can be sent to the bank by mail or similar means, and in such case the only available verifying procedure is signature comparison. Thus the systems of Finnish banks are vulnerable to crime, especially if the criminals are aided by bank or company employees. The responsibility usually falls on the banks if it can shown that their system controls were inadequate.

Another important type of crime is terrorism that aims at rendering inoperable a bank or whole system. In Finland the highly automated payment systems could be made inoperable by incapacitating ICT equipment through viruses or physical damage.

(Risk grades: j = none, p = medium, s = minor)

4.4 Environmental risks

4.4.1 Risks of changes in legislation or market practices

Legislation on credit transfers and netting have clarified responsibilities in connection with payment transactions. It is no longer unclear who is responsible for payment delivery in the different phases of the payment process. The agreement between bank and customer can be helpful mainly in clarifying errors due to carelessness. However, in case of bankruptcy of a contracting party, contract validity may become questionable. Banks' risks have

increased due to a definite tendency to shift responsibility from customer to bank.

(Risk grades: j = none, p = medium, s = medium)

4.4.2 Loss-of-confidence risks

Loss-of-confidence risks arise mainly when customers do not consider the system secure and reliable (eg payments are delayed due to technical or liquidity problems or are lost or altered). If this risk is realised, customers may shift their orders to other banks. Customers who send express transfers tend to react swiftly to recurrent problems or service breakdowns.

(Risk grades: j = none, p = medium, s = medium)

4.4.3 Technological change risks

Procedures for large-value transfers are under continuous pressure for further development. The next few years will witness a number of projects concerning systems for large-value payments, inter alia, in connection with Internet, market consolidation and bank mergers. Tight timetables and simultaneity of several projects may complicate the coordination.

Large-value transfers represent significant financial benefits. Thus it is possible that in future we will see a global network for real time large-value payment transfers. The technology already exists. Should this happen, there would be a dramatic reduction in payments made outside the network. Dependence on ICT and security systems gives rise to the danger of operational breakdown in the event of a serious disturbance.

(Risk grades: j = medium, p = medium, s = medium)

4.4.4 Catastrophe risks

Catastrophe risks are tied closely to ICT systems. However, in Finland numbers of payment transactions are still so small that in exceptional situations large banks can process most large-value payments manually if necessary.

(Risk grades: j = none, p = medium, s = medium)

4.5 Clearing and settlement risks

4.5.1 Systems risks

The settlement of express transfers can be executed in two different ways: in the POPS system as RTGS payments or in the backup system as a part of the PMJ net settlement transfer. The latter procedure is used only in exceptional situations. Strict requirements as to operational reliability are placed on the BoF-RTGS, because even a brief interruption of services could expose participating banks to cumulating bank-specific risks if covering funds for express transfers cannot be transmitted in real time. Real time settlement is especially important for large-value express transfers. As volumes increase, it becomes essential that backup systems be in working order.

Systems connected with banks' fund transfers, cheque account facility interfaces, clearing systems, and liquidity management software comprise a single entity that must operate smoothly also in unusual situations within and between banks.

(Risk grades: j = none, p = medium, s = medium)

4.5.2 Collateral risks

Collateral is not used in interbank clearing.

(Risk grades: j = none, p = none, s = none)

4.5.3 Settlement cancellation risks

Under present legislation and payment system rules, settlements cannot be cancelled.

(Risk grades: j = none, p = none, s = none)

4.6 Systemic risk

For express transfers, systemic risk can be large in the event of a serious disturbance.

(Risk grades: j = none, p = major, s = medium)

Annex 2

Mitigation of payment system risks

1 Control of credit risks

1.1 Bank credit risks

RTGS payment

Bank credit risk is eliminated by either simultaneous transfer of payment message and covering funds or transfer of covering funds before crediting of customer accounts.

Counterparty limits

In a netting payment system, risks can be contained if there are interbank counterparty limits. An effective arrangement would include real time limits that cannot be breached. Risks can also be reduced by way of monitoring triggers that automatically stop the transaction processing when a limit is approached or exceeded. In using limits it is necessary to be aware of the asymmetric risk that arises when, for structural reasons, the risks between two counterparties are frequently or continually tilted toward the same party.

Monitoring system

A system for monitoring counterparty positions should be either real time or updated at least several times during the day.

Collateral

Risks associated with counterparty debit positions can be reduced by the use of collateral.

Agreements and legal matters

Rules on payment finality and specification of responsibilities of receiving vis-à-vis sending banks facilitate risk management. If legislation supports netting (for example, a bankrupt's estate cannot unwind executed payments), bilaterateral counterparty positions can be netted without the risk of unwinding. Valid multinetting of counterparty positions can also be accomplished by way of institutional arrangements.

1.2 Customer credit risks

Customer credit risks in payment transactions are eliminated if debiting customer accounts for outgoing payments and cheques is timely and subject to adequate funds.

Transaction- and customer-specific limits

To be effective, the monitoring of transaction-specific, account-specific, and customer-specific limits should be done on a real time basis.

Collateral

Collateral requirements can be used to reduce risks connected with customer limits.

Monitoring system

Banks' credit risk monitoring systems should be sufficiently comprehensive to include short-term customer risks associated with payment services.

Risk analysis and classification of customers

Setting of customer limits should be based on substantiated analysis of customer-related risks.

Customer-specific division of responsibilities

For each loan customer, a bank should designate someone in the bank to be responsible for the relationship with that customer.

2 Controlling liquidity risks

Netting

Binding netting reduces fluctuations and liquidity needs in a payment system with uneven payment flows.

Timing of payments

Liquidity can also be managed by scheduling payment flows and centralising the queuing system. Scheduling payment flows and possible setting of timetables requires cooperation between concerned parties in establishing common market practices.

Flexible adjustment of limits and collateral

To avoid unnecessarily large limits and collateral, the arrangements for these should be readily adjustable to changing liquidity needs.

Estimating liquidity needs

It is essential that a bank's internal estimating system is able to forecast with sufficient accuracy its liquidity needs over the course of the day.

Relative liquidity requirement

The ratio of a bank's short-term funds to its estimated intraday liquidity position should be kept at a reasonable level.

3 Reducing operational risks

3.1 Reducing information system risks

Reliable operation of a payment system is based largely on reliable information systems. Besides the automated elements, these systems include manual elements, and these must be smoothly and functionally interlinked.

Coordinated decision-making and standards

Risks associated with information system interdependencies can be reduced by coordinating the related decision-making within a single operating unit and between parties. Various types of standards comprise one of the primary means of coordination.

Systematic planning and maintenance

Systematic planning and maintenance reduces the probabilities of various errors and disturbances and improves recovery possibilities. Quality standards and systematic high-quality work are parts of systematic planning and maintenance.

Sound information systems architecture

Sound information systems architecture – based on good selection of platforms, communication solutions, implementation, other tools, etc – reduces the risks entailed in an overly complex system.

Qualified personnel

Avoiding and reducing risks, particularly those connected with automated parts of information, requires sufficiently skilled employees.

Employee training

Continuous training of employees helps to keep their expertise up to date and to make appropriate use of changing systems.

Written instructions

Written instructions help employees to understand the effects of their actions on the overall operation and steer them toward the best working procedures.

Clear interfaces

Clear interfaces reduce errors and facilitate proper interpretation of information.

Fixed format for controlling change

A fixed format for controlling change, which includes sufficient testing of changes in information systems, reduces risks.

Backup systems and copies and contingency plans

Pre-planned and tested backup systems reduce losses from realised risks and speed up recovery. Sufficient backup copies are critical to the operation of backup systems. Written contingency plans ensure that provisions are adequate and available as needed.

Systems solutions that enhance ICT security

Solutions that enhance ICT security – such as user names and passwords, transaction logs, encryption and signature checks – reduce the risks of misuse of internal and information networks.

Effective internal control

Effective internal control helps in anticipating future risks. Internal audit can complement control and ensure its effectiveness.

3.2 Reducing administrative risks

Administrative risks associated with payment systems are usually related to bank procedures, existence and functionality of internal risk management processes, employee skills, existence and functionality of backup systems, preparedness for disturbances and problems, and organisation of systems maintenance and use.

Administrative risks associated with payment systems can be obviated or reduced by the following:

Prudent practices
(Observance of good payment transfer practices)

- requiring sufficient information on payment sender and receiver
- verifying information of incoming and outgoing payments
- care in physical processing, safekeeping, dispatch to customers, archiving, and signing (cheques, bank drafts, debit cards, prepaid cards etc)
- observance of practices agreed between banks
- ensuring that only authorised persons can access and alter systems (access control and other physical security measures).
- appropriate customer interfaces based on agreements
- protection of systems from outside intruders.

Effective use of internal means of risk control
(adequate control methods)

- consumer information is sufficient and up to date (use of customer controls)
- operation of all systems, the payments and their processing, and controls are described phase by phase in sufficient detail (use of documentation)
- system operative functions are sufficiently separated from system monitoring

- all systems are overseen by responsible persons and internal owners
- for all outgoing payments exceeding a specified value, two employees check and verify the payment information or checking and protective procedures are available
- written system-specific risk controls are explained and distributed to everyone who is to observe or oversee them
- management instructions are available and responsible persons are assigned at various levels of the organisation for controlling and monitoring maximal risks and related decision-making procedures are in place
- management receives regular reports on customer credit risk and bank credit risk limits and amounts. Exceptional situations (eg limit overages and their causes) are quickly reported to management and responsible persons.

Employees adequate in numbers and skills
(sufficient expertise)

- responsibility for staff size and skills is assigned to a specific person and to senior management
- adequate training and on-the-job initiation is arranged for all system users and monitors
- management is sufficiently aware of broad system functions and related potential risks and takes responsibility for training new managers
- there is an arrangement for backup personnel, trained to assume the tasks in question when necessary
- there is adequate extra training for maintaining expertise.

Well organised systems maintenance and use
(conscientious systems maintenance)

- there is sufficient documentation and instructions on systems maintenance, use, service, repair, and the related organisation, as well as a logging-on system, records of use, and logging-off, which enable verification of times and persons
- changing and updating of system software is appropriately secured
- there are instructions on, and specified responsible persons for, updating, secure storing, destroying, altering, retrieving, and archiving system information

– access of service and repair personnel to equipment areas and software is appropriately restricted, monitored, and verified.

Readiness to handle problems and disturbances
(adequate instructions for handling disturbances)

– all banks should have written instructions on how to respond to the most common disturbances and problems
– all participating banks (including the central bank) should have instructions on how to proceed in the event that a bank is removed from the clearing system due to insolvency, especially as regards the handling of the bank's payments.

Existence and functionality of backup systems
(adequate backup systems)

– backup systems and other arrangements, for example with another party, are needed to handle potential technical or other disturbances and ensure service availability without undue customer inconvenience
– backup systems and arrangements should be periodically tested to ensure functionality in case of a disturbance.

Written agreements between parties
(adequate contractual basis)

– adequate agreements are needed between banks and cooperating banks and between banks and corporate and private customers on damages due to errors and delays in connection with payment transfers
– banks should have lists of payment orders that have led to disputes and payment of damages.

3.3 Reducing crime risks

Security policy and procedural instructions

Written security policy, nomination of persons responsible for its implementation, and procedural instructions for risk situations form a basis for secure operations.

Security planning as part of system planning

Information system risks can be reduced at the planning stage through a layered approach to protection that aims at preventing crime, increasing the probability of apprehension, and minimising the effects of crime.

Monitoring/control

The main monitoring and control tools for reducing crime risk are alert limits, control reports, reporting of exceptional cases, recognition of pattern behaviour, and statistical monitoring.

Separation of duties and other administrative measures

Effective administrative means of preventing internal misuse include the requirement of having two persons for certain operations; verification or implementation of a task by a second employee; breaking down tasks into subtasks, each handled by a different person; and occasional rotation of duties.

Procedures that increase security

Security of customer services can be increased by means of customer identification and knowledge of their habits and behaviour; verification of authenticity of documents and signatures; and debiting before crediting accounts. In connection with electronic services, the related security and ID features should always be used.

Physical security

Physical security against crime can be increased through locking premises, controlling access, camera surveillance of premises and surrounding areas, employment of guards, and use of alarm systems.

Controlling access to information systems

Unauthorised use of information systems can be reduced by user identification, access rights control, and monitoring of access violations. Outsider entry into a system can be regulated via firewalls and other similar technical means.

Exchange of experiences

Protection against crime can be improved by exchanging information about criminal methods and means of protection.

Training

Appropriate training of employees helps them in timely recognition of crime risks and taking appropriate measures.

4 Reducing environmental risks

4.1 Reducing risks of changes in legislation or market practices

Active lobbying and anticipation of change

It is often difficult to find means of protection against risks of changes in legislation. This is partly due to the fact that in the EU context legislative drafting has become more international. Thus the most important means of avoiding and reducing risks associated with legislative change might well be acquisition of information from various sources and active lobbying – based on expertise – of domestic and foreign legislators and authorities.

Cooperation and discussions with interest groups

Means of protecting against changes in market practices are closely associated with protection against legislative changes. In both, the objective is to eliminate both the insecurity that hampers operations and the potential financial losses. This approach serves to guide banks' operational policies, information collection, and discussions with different interest groups.

4.2 Reducing loss-of-confidence (reputation) risks

Correct and timely information

The spreading of problems and growth of losses can usually be avoided via effective dissemination of information. Weak, untrustworthy or cover-up communications can have the opposite effect, in which case a limited loss of confidence can spread across the whole banking system.

It is difficult to find means of protection against confidence loss, based on facts or in situations where the basic problems cannot be addressed immediately. In certain situations there may be rumours due to misunderstandings, over generalising, etc, in which case loss-of-confidence risks can be reduced by timely and effective communication.

Regular information

Advance and regular communications can effectively prevent rumours.

Well organised communications

Successful communications requires a well-functioning communications organisation and policy supported by a crisis organisation with ample decision-making authority. This applies to both individual banks and authorities.

4.3 Reducing technological change risks

The primary technological risks reflect a struggle between security methods and the most recent means of breaching these, as well as the rapid outdating of the technology is use.

It is difficult to protect oneself in advance against the risks of technological change. Technological advance cannot be prevented. Following the current trends already in the early phases can identify the associated risks. It is important to quickly find appropriate countermeasures for perceived significant changes or means of adapting to these.

Adoption of new security techniques

It is worthwhile investing in advance in new security systems and using parallel means of protection. Customers are nowadays very quick to adopt new techniques. Electronification of customer activities also causes rush hour peaks in communication and other systems more often than before.

Allowing for system expansion

It is important to take account of future needs for system expansion so as to enable short-run accommodation of growth and fluctuations in payment volumes and obviate disturbances and capacity bottlenecks. Because adding to capacity takes time, the need should be anticipated well in advance.

In the offing are further technological changes in banks' operating environment that affect service provision. Customer services are becoming less personal and more remote, and increasingly based on communication networks. At least some customers will in future be served via virtual bank branches. Facing these challenges, banks need a survival strategy that utilises new possibilities and readily adapts to a changing operational environment.

Creating a basis for good agreements

A minimal requirement in the new world is to lay the foundation for agreements that enable efficient allocation of a bank's resources in response to changes in demand.

4.4 Protection against catastrophe risks

Effective access control

Finland has been largely spared from natural catastrophes and terrorism. Although these risks are small, they are increasing, as evidenced in recent years by for example increased monitoring of computer centres and gradual upgrading of physical and other security systems. There is still room for improving protection against these risks in Finland too.

Backup equipment and resources

Potential catastrophe calls for readiness to quickly employ backup equipment and other backup resources and for persons trained to handle unusual situations. Although the situation has improved, preparedness to cope with catastrophes is still at a low level in Finland. A serious ICT catastrophe in a bank would very likely paralyse the bank's operations.

Decentralisation of systems

Decentralised systems and backup systems enable partial operation of banking networks during a major disturbance. Finnish banking networks are however highly centralised and hence highly vulnerable. Moreover, because the Finnish banking sector is also highly centralised, problems in a single large bank can easily expand into system risk.

Contingency plans

Banks should have plans in place for providing essential services in the event of a crisis. Advance testing of implementation is critical. Each bank needs its own plans for changing over to a restricted service menu when only some of the computer systems are available. To cover the possibility of a protracted interruption of ICT services, it is essential to have appropriate plans and instructions for starting up manual operations.

5 Controlling clearing and settlement risks

Covering funds before payment

Clearing and settlement risks are eliminated if banks consistently credit customer accounts for payments only after interbank transfer of covering funds.

Functionality of systems

Clearing and settlement risks can be reduced by ensuring that existing systems and communication links are of high quality, secure and well functioning. Hot or cold standby systems can help contain or prevent the adverse effects of disturbances.

Adequate and secure collateral arrangements for credit

By requiring that participants post adequate collateral for credit, losses stemming from a participant's insolvency or bankruptcy can be avoided. Moreover, in systems involving international parties in particular, asset pledging must be legally valid in case of insolvency or bankruptcy.

Irrevocability of settlements

Settlement finality can be ensured and disturbances and losses caused by payment cancellations can be prevented by means of legislated regulations on payment finality in both gross and net systems.

6 Controlling systemic risk

Structures and procedures

Systemic risk can be reduced via payment system structures that prevent the onset of systemic risk (eg Lamfalussy minimum standards for netting systems) or practices that reduce the likelihood of realisation of bank-to-bank or system-to-system contagion (eg RTGS, PVP, DVP).

Liquidity support systems

Systemic risk can be reduced via central bank or clearing house provision of liquidity to parties having temporary payment difficulties, for instance after a market crash or settlement interruption due to a technical problem.

Good backup systems

Also critical are tested and operational backup systems and links that are ready to operate at the onset of a disturbance. Such backup systems can prevent a disturbance from spreading and cumulating in a systemic crisis.

Annex 3

Payment system rules

Rules for PMJ interbank payment system
Maintainer: Finnish Bankers' Association

Rules for POPS system for banks' online express transfers and cheques
Maintainer: Finnish Bankers' Association

Settlement system rules regarding payment obligations between cooperative banks
Maintainer: OKO Bank

Rules for settlement system for payment transfers between savings and cooperative banks
Maintainer: Aktia Savings Bank

The above-mentioned rules can be obtained if necessary from the maintainer or Ministry of Finance.

Annex 4

Finnish Bankers' Association guidelines for risk surveys

Guideline for survey of payment system risks

1 General

The Financial Supervision Authority (FSA) requires that banks produce written, up-to-date product-specific descriptions of payment system risks so as to facilitate the identifying, limiting and monitoring of system-specific risks associated with payment flows. This guideline has been produced by the Finnish Bankers' Association[20] to assist banks in carrying out this task.

Risk surveys should be done in writing, by payment system and product. A description of the risks relating to a particular product or service should identify the systems used in providing the product or service. It should also include aspects of services that are not covered by system-specific risk surveys.

Regular (yearly) risk surveys are the responsibility of those responsible for each product. The contents are to be decided jointly by those responsible for the product and for the application, with participation of those units handling manual operations for support and customer services so that each of these approves the survey contents as pertains to its own operations.

In connection with the analysis as described in point 8 below, the participants should include all the above-mentioned parties. The results of the analysis should be written according to the directions in point 8. After all sections have been completed, the participants should approve the risk survey.

[20] The guideline – produced in cooperation with the the Finnish Bankers' Association and supervising authorities – is of the nature of a recommended framework.

2 General description

A general description is a broad overall description of risks including background for the areas, services, transactions, and operations covered in the survey.

2.1 General description

Describe the service/s provided via the system. Specify the limitations of the survey.

2.2 Operations

Describe briefly the system's operations – including manual operations – that are important in terms of risks. It is especially important to make note of information controls and possible security limits. If the description is too vague, some risks may be overlooked. In this connection, application documents etc may be useful. Operational charts can help to clarify the text.

2.3 Transaction types and volumes

Specify the transaction types handled in the system (credit transfers, express transfers, repetitive transactions, direct debits, payment terminal transactions, cheques, agreement contents) and give volume information that is pertinent in terms of risks.

2.4 Agreements

Specify service contacts and other similar agreements that pertain to service provision via the system. Also note essential attachments such as handbooks. Agreements etc are good information sources for risk surveys. Contracting parties' responsibilities and obligations are described in point 7 below.

2.5 Other aspects

Describe any other factors that are essential for the risk survey and for which the related risks are examined.

3 Links

Describe links to other systems and platforms. The aim here is to present an overall picture of service production and system risks associated with links. Show how the links 'serve' the scrutinised system or what information or transactions are transferred or received via the links. Charts can help to clarify the text.

4 Backup systems

Give a general description of the operations of backup systems and backup arrangements, and replacement systems and services.

Describe the bank's responsibilities for the existence of backup systems; for example the invoicer – not the bank – is responsible for the backup system for network invoicing.

Provide usage data if possible.

Reference can be made to the bank's special plans for handling possible catastrophes and other exceptional situations.

5 Security limits

There should be a description, note, or reference to a description of how controls are built into the system so as to secure customers' and banks' information. For example, PATU or SSL security solutions could be referred to by name; the technologies need not be described.

The bank's instructions on the handling of internal security should be described or referred to. The access rights for manual procedures should also be described.

The risks of general security procedures are to be described separately.

6 Availability

Describe usage and availability of the system or service from customers' or other banks' viewpoint as well as the promised availability level and open hours in agreements and general conditions covering the service.

Describe or refer to the bank's instructions on system preparations for handling disturbance situations. Explain also how customers are informed of disturbances and interruptions in service provision.

7 Liabilities and obligations

Describe the bank's liabilities and obligations to customers and other banks as per agreements and general service conditions.

Describe agreement conditions that are material in terms of (primarily operational) risks.

Legal risks associated with agreements are to be covered separately.

8 Risk survey

8.1 Risk analysis

Risks should be analysed by type. One approach is to put together a group of experts and beforehand give each one a copy of the risk survey report, each section of which has been approved by the respective responsible persons (eg product, ICT, support, and customer service operations). This will enable them to become familiar with the situation. These experts then analyse the system or product risks for example in accord with the Bank of Finland's publication, 'Payment risks in Finland and the need for regulation and supervision' (A:101, 1998).

8.1.1 Operational risks

Analysis of payment systems should focus on operational risks. Of these, information system risks are connected with both normal system operations and manual operations.

Administrative risks are connected for example with operating methods, quality and observance of instructions, and preparations for handling problem situations.

Risks associated with crime and security procedures can be analysed in cooperation with the bank's security experts.

8.1.2 Environmental risks

Environmental risks entail possible losses in connection with large and rapid changes in the operating environment.

Risks associated with changes in legislation, market practices and contract law should be analysed in cooperation with the bank's legal experts.

Risks associated with loss of confidence can arise eg in connection with an operational disturbance affecting service provision. Reliability of the bank's services is a key criterion of quality.

Risks associated with technological change are usually related to service provision or security systems.

The handling of catastrophe risks is a part of the bank's preparedness planning.

8.1.3 Customer credit risks

Confront the issue of whether realisation of customer risk is possible in exceptional or disturbance situations.

Bank credit, clearing and settlement risks are connected with interbank payment systems.

In describing these risks, the bank can make use of the Bank of Finland's publication A:101 and its appendix 1, 'Detailed description of payment system risks', as well as the banks' jointly produced surveys of payment service risks.

8.2 Risk evaluation

Risk realisation probabilities can be classified eg as follows:

- very small (less frequently than once in 5 years)
- small (less frequently than once a year)
- fairly small (about once a year).

Sizes of realisation losses (monetary or image) can be classified as follows:

– minor
– medium
– major

8.3 Risk management

Describe the limits that are applied to the different risks and the other means of controlling and reducing risks.

Delegate responsibility to someone for taking the proposed measures.

It may also be useful to monitor certain specific risk situations.

9 Monitoring and reporting

The bank should collect data on realised risk situations and events.

The risk survey report should be updated with information on realised risk situations and risks that have been noticed for the first time and possibly those connected with changes in systems. State the persons and methods involved in monitoring realised risk situations, as well as who receives the reports.

10 Summary

Indicate the importance to the bank of each product or system, using eg volume data.

State also the major risks associated with each product or system, as well as their realisation probabilities and loss sizes.

Explain the bank's risk control procedures for each product and system.

State the recent years' realised risks.

Guideline for survey of legal risks

1 General

In this context, legal risk refers to legal uncertainties regarding business operations; for example possible illegality of operations, uncertainty in interpreting an agreement or even nullification of it or one of its conditions, or the bank's possible liabilities and damages.

Legal risks often concern activities or products and related agreements. The aim of this guideline is to highlight the main agreement parts and activities that may involve legal risk.

As regards banking, it should be noted that the scope of business operations allowed for a bank is stipulated in the Act on Credit Institutions, section 20. The activities pursued and the products developed and offered by credit institutions must be such as can be considered to fall within the scope of operations allowed by the law.

1.1 Legal risks connected with the environment

Operations or practices may be seriously affected by rapid, unpredictable or significant changes in the operating environment, including legislation and other regulation. These risks can be anticipated by actively monitoring EU legislative processes and developments in domestic legislation and regulation. Anticipation can reduce risks and ease the impacts of environmental change.

Legislation and regulation that is unclear and prone to numerous interpretations cause legal risks, as the prevailing rule of law is unclear. In such situations, legal risks may be tackled by bringing shortcomings and needs for change to the knowledge of authorities and drafters of legislation.

Even though, in Finland, court rulings lack the binding precedent effect of case law, court rulings do nonetheless influence prevailing practices and are relied on for guidance. Therefore it is also necessary to monitor court rulings, especially those of the Supreme Court, in order to ensure that operations conform to prevailing legal interpretations.

The significance of legislation, regulation and environmental risks increases when operations are started abroad or services are launched outside the home country. In these situations, the legislation and regulation of the operational environment should be studied with particular care and operations delayed until regulations and guidelines governing the operations are understood by everyone involved.

Effective elimination of environmental risks requires that changes in the environment pertaining to different projects be taken into account at as early a stage as possible. This in turn requires sufficient resources and effective flow of information within the organisation.

Is the monitoring of changes in legislation and regulation and case law organised so that information on changes and new solutions will reach everyone whose tasks in the areas of product development or contracts require that information.

1.2 Legal risks related to agreements

Agreements and their conditions should be drafted so as to meet the requirements laid down in the Contracts Act (228/1929).

Finalised agreements and the necessary preparatory material should be documented and archived so that they can be quickly and easily located and used.

1.2.1 Concluding an agreement

An oral agreement always constitutes a risk to the parties, as its existence and contents are difficult to establish ex post. To avoid these risks, agreements should always be concluded in writing or other documented form. Whenever contracting parties invoke an agreement, they must be able to prove that the agreement is duly signed, regardless of the technical format of the signature. An essential prerequisite for the validity of an agreement is that it be signed by the correct counterparties. Hence, a party must be known and it must be ensured that any private individual who signs the agreement is legally competent and any person who signs on behalf of a corporation has the right to so act on behalf that corporation.

When an operation is started, is there a signed agreement concerning the operation?
Is the other party known sufficiently well and has it been ascertained that the signatory person has the right to conclude the agreement?
Is the agreement either written or otherwise documented so that its contents can be verified afterwards?

1.2.2 Wording of an agreement

Unclear wordings and conditions and those that lend themselves to multiple interpretation may, when disputed, lead to problems or even interpretations that were not intended when the agreement was concluded. This may be the case especially if interpretation is entrusted to a court or other third party.

Conditions and the wording of an agreement should be so unambiguous as to avoid the occurrence of unclear situations. When standard contracts are used, it should be borne in mind that an unclear condition in a standard contract is usually interpreted to the disadvantage of its drafter.

Is the wording of the agreement clear and unambiguous?
Which parts of the agreement are particularly prone to a variety of interpretations?

1.2.3 Agreement conditions

Agreement conditions should be drafted as clearly as possible and should cover all circumstances intended within the scope of the agreement. The conditions should cover all activities based on the agreement, and practice should conform to what has been agreed. If activities in practice do not conform to agreement conditions, it may give rise to uncertainty about the validity of the agreement or whether an activity is covered by the agreement. In order to avoid risks, agreement conditions should be adjusted to correspond with practice, whenever practice diverges from the agreement or is based on established customs between the contracting parties.

Some services or products may involve several separate agreements. In such situations, it should be ascertained that the conditions in the various agreements are mutually consistent.

1.2.4 Amendment of agreement or conditions

An agreement often contains conditions for its amendment. Particular attention should be paid to conditions stating that one of the contracting parties may unilaterally change the conditions. In such a case, it must be ensured that the agreement includes sufficiently clear conditions – fair to both parties – on how changes are notified and enter into force.

Agreements may have annexes, eg system descriptions, which constitute parts of the agreement. When annexes or the agreement itself are amended, it must be verified whether the amendments require changes also in the agreement or annexes. Also, it must be verified that the amendments do not render the annexes and agreement inconsistent.

Has an amendment to the agreement been agreed in a sufficiently clear manner?
Is the agreement consistent with its annexes?

2 Responsibility issues

Many services include parts supplied by third parties not covered by an agreement. Furthermore, supplying, producing or receiving a service may in some respects depend on actions by parties other than the contracting parties. The agreement may not be fulfilled if eg a third party fails to deliver a piece of information or perform an action. Legal risks may emerge if the agreement does not stipulate in sufficiently clear and unambiguous terms the responsibilities and restrictions of responsibilities of both contracting parties.

Agreements may include conditions that transfer responsibility to a third party or stipulate that a contracting party is not responsible for the actions of a third party that may affect fulfilment of the agreement. Such conditions always entail the risk that the agreement or its terms cannot be fulfilled or observed for some reason pertaining to a third party.

Responsibilities must also be clear whenever a given function is outsourced. The bank is always responsible to the customer for administering an outsourced function. Before a function is outsourced, it must be ascertained that the contracting party responsible for the outsourced function is capable of performing the tasks entrusted with it. The outsourcing contract must stipulate sufficiently clearly the limits of responsibility both between the contracting parties and with third parties. If the party in charge of the outsourced function makes use of subcontractors, the bank’s consent to the outsourcing contract is needed.

Does the agreement define the limits of responsibility with sufficient clarity?
Have the capabilities of the company or agent responsible for an outsourced function been verified, and is the conduct for an outsourced activity monitored regularly and closely?

3 Fairness issues

The use of unfair contract conditions is prohibited in Finland by the Contracts Act and the Act on Regulations Concerning Contractual Terms Between Traders. Moreover, as regards consumers, there are several provisions on unfair conditions in agreements with consumers.

The unfairness of agreement conditions should be assessed both when concluding the agreement and during its period in force. A condition that is initially fair for the contracting parties may become unfair while in the agreement is in force and thus affect the stringency of the agreement, at least as far as the condition that has become unfair is concerned.

Credit institutions must submit the conditions used in their standard contracts to the FSA. Although the FSA reviews these conditions, those who draw up agreements remain responsible if any agreement conditions become unfair at a later point.

Has the fairness of agreement conditions been assessed from the viewpoint of a probable contracting party?
Have the standard contracts in use been submitted to the FSA for review?

4 Corporate reorganisation

Reorganisation measures such as mergers or divestment of business may cause a change of contract party. Legal risks arise, if the reorganisation leads to uncertainty as to the continuity of the contract or the actual contract party.

Is the contract made in the name of the actual agent?
Does the contract provide for the circumstances related to the transfer of the contract?

5 Established practices and conventions

The practices and procedures followed by the contracting parties may diverge from those specifically agreed to. If the wording of the agreement does not correspond to existing practice, it may have been intended to amend the contents of the agreement or the existing practice itself may be regarded as having changed the agreement.

Following a practice that does not correspond to an agreement or allowing such a practice to be followed may be regarded as an implied change of agreement or consent to a change the agreement. To avoid uncertainties and difficult incidents of interpretation, agreements should be updated to correspond to the existing practice.

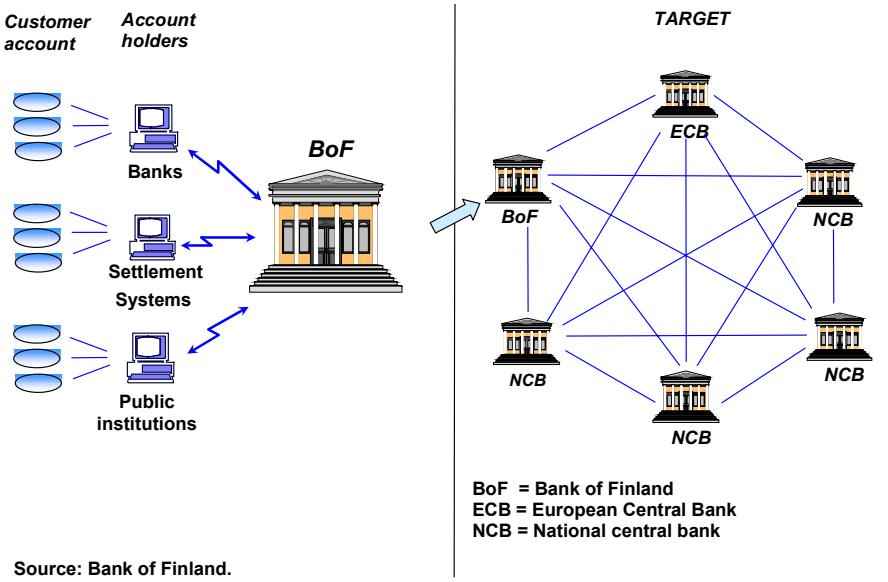
Does existing practice correspond to the wording of the agreement?

Annex 5

Descriptions of Finland's key payment systems

1 BoF-RTGS

Figure 2. **BoF-RTGS and TARGET**



Source: Bank of Finland.

The BoF-RTGS is the real time gross settlement system maintained by the Bank of Finland. 'Real time' and 'gross' indicate that payments are executed one-by-one and that the related funds and information are transferred simultaneously. Participating banks can send payments to each other in real time across their accounts at the Bank of Finland. The system also executes settlements for the banks' other payment systems: PMJ and POPS.

BoF-RTGS is also part of the TARGET system for euro area central banks and the ECB. The EU countries not participating in the euro area also participate in TARGET, which comprises the national RTGS systems, ECB payment mechanism, and their interlinking system. TARGET's basis and operations are governed by principles issued by the ECB and included in the pertinent legislation.

BoF-RTGS is used for real time gross payments of central banks, between banks, and for customers. In 2002 the system was used to

execute 1,540 payments (amounting to about EUR 14.7 bn) per day on average.

BoF-RTGS rules, which are included in the Bank of Finland's agreements with account holders, observe the ECB's international guidelines for the ECB's TARGET system.

Requirements for participation in BoF-RTGS also observe TARGET guidelines. A BoF-RTGS account holder must be a publicly supervised credit institution licensed to operate in the EEA. The Bank of Finland can also approve for participation the State Treasury as well as EEA-licensed investment firms and clearing and settlement service companies. Such a firm or company must be supervised by competent authorities and have a minimum paid-up capital of EUR 2.5 million.

There are now just over ten members of the BoF-RTGS, including the major Finnish banks, HEX, Automatia, and the State Treasury. The key indirect members are the savings banks, OP Bank Group and the independent local cooperative banks. The central financial institutions for these banks are BoF-RTGS members and act on behalf of their member-banks.

The BoF-RTGS comprises the Bank of Finland's system application, an account holder interface, a SWIFT interface, and an account holder application supplied by the Bank of Finland.

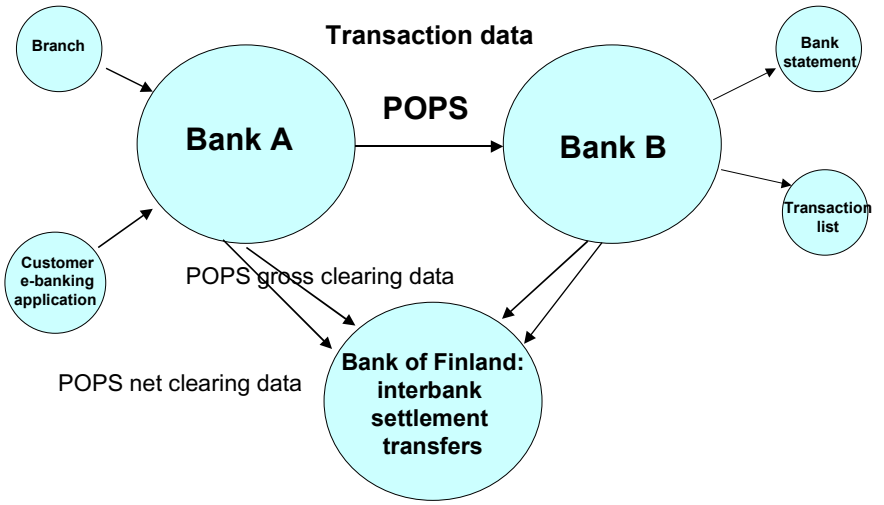
Operating principles

In the BoF-RTGS, payment orders are sent to the Bank of Finland via the members' account holder application or SWIFT interface, which provide system access. To ensure information security, all information flows are encrypted. All TARGET payments requiring, ie those transferred via other EU-country central banks, use the SWIFT interface.

Besides transferring payment orders, an account holder can use the account holder application to check its liquidity situation, since all of its transactions can be viewed in real time. System users can obtain various reports, bank statements, etc. It is also possible to inform account holders of important system matters via the account holder application.

2 POPS

Figure 3. **POPS system**



In the POPS system, bank A's customer can make an express transfer to another bank's customer at his own bank branch or via e-banking applications. The payee's account can be in any bank (B) in the system. Bank A sends payment details to bank B via the POPS network. The receiver is informed of incoming payments, eg via a bank statement. A corporate customer can also obtain details on incoming express transfers from the electronic transaction list and enter them directly in its computer-based accounting system. As per sender's wishes, the receiving bank can also advise the payee immediately when the funds become available.

A cheque written from bank A is redeemed at bank B by real-time reserving of covering funds in the writer's account in bank A. Bank B is informed immediately if there are any conditions or remarks on discrepancies concerning the cheque or if the writer's account in bank A lacks sufficient funds.

The interbank settlement (A to B) occurs across accounts at the Bank of Finland.

2.1 POPS system handles express transfers and cheques

The POPS system handles domestic cheques, bank drafts (ie bank cheques), gift cheques, and express transfers. In 2002 the system handled daily on average about 2,600 transactions, amounting to some EUR 1.5 billion.

The member banks decide on acceptance of new members. In 2002 POPS included eight clearing banks, three of which were Finnish branches of foreign banks.

POPS employs a closed network owned by the banks for transmitting transaction information. All transactions are executed in

real time. When, for instance, a customer's cheque is redeemed in another bank, the corresponding debit occurs in real time, along with checking eg for conditions attached to the account.

The PMJ serves as a backup system for POPS.

2.2 Net and gross transfers in POPS

In POPS, interbank settlements are effected between banks on both net and gross bases. To contain risks, the system applies both net and gross limits. If a transaction exceeds the gross limit, the interbank settlement is accomplished individually across accounts in the BoF-RTGS. Only after this is the payee's account credited. If the sending bank does not transfer the covering funds, the payee is not paid.

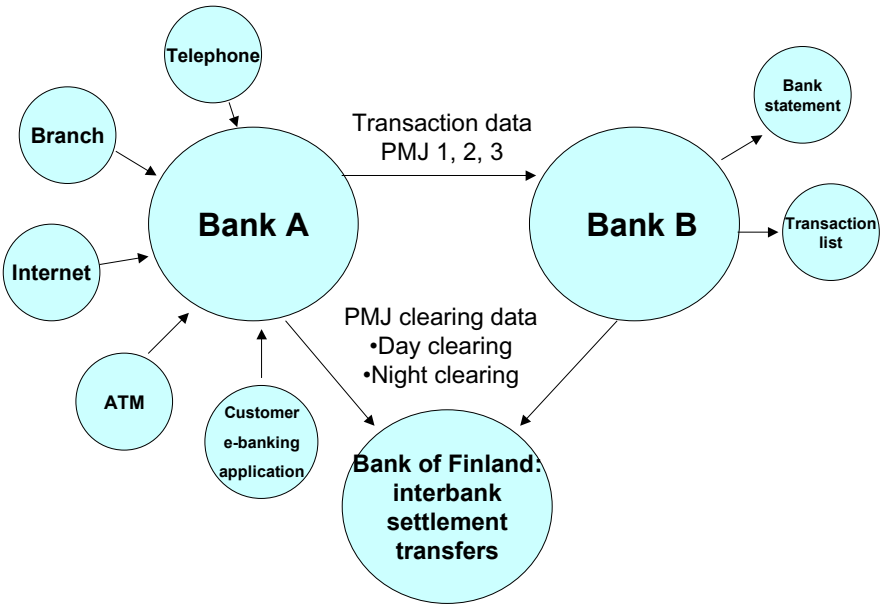
Smaller payments are netted, based on bilateral net positions. Interbank risks are contained by bilateral net limits, which are the maximal for settlement risks. A net limit is twice the size of the corresponding gross limit. The net settlement arrangement makes use of 'warning triggers', which are equal to corresponding gross limits. If two banks' bilateral net position, which they monitor in real time, exceeds the warning trigger, the debtor bank must transfer funds to the other bank in the amount of the warning trigger. If the net position would rise above the net limit, the bank carrying the risk discontinues payments transmission until it receives the anticipated covering funds. At the end of the day, the 'short' bank transfers the final amount to the 'long' bank across accounts at the Bank of Finland and the bilateral position is zeroed.

2.3 POPS settlements – final and irrevocable

The POPS system rules have been approved by the Ministry of Finance and notified to the European Commission. The rules ensure that funds transfers are final and irrevocable, as required by the legislation pertaining to POPS. Under the rules, a POPS **gross payment** is entered for settlement when the real time transfer message is sent via the BoF-RTGS to the Bank of Finland. In POPS, a gross payment becomes binding when the settlement is affected at the Bank of Finland. A **net payment**, in contrast, is final as soon as the transaction amount has affected the net positions of the sending and receiving banks.

3 PMJ system

Figure 4. **PMJ**



Bank A's customer can make a payment in several ways: from a bank branch, or by ATM, phone, e-banking application, or Internet. The payee's account can be in any bank (B) in the system. Bank A sends payment details to bank B by batch transfer using the banks' joint information network. The information is made available to the payee by his bank (B), eg in the bank statement. A corporate customer can also obtain details on incoming payments via the electronic transaction list and can enter them directly in its computer-based accounting system.

Bank A settles with bank B across accounts at the Bank of Finland.

3.1 PMJ for batch payment transfers

PMJ is used for interbank payment (and related information) transfers on behalf of domestic customers. The main types of payments handled are credit transfers, recurring payments, direct debiting, and card transactions. In 2002 some 1.7 million transactions (about EUR 719 m) were handled in PMJ daily on average.

The PMJ system includes all banks that participate in the POPS system.

Backup arrangements for PMJ include the use of cassettes and diskettes for interbank transfers of payment information. Several options exist for sending settlement orders to the Bank of Finland.

3.2 All interbank transactions handled by computer

In the PMJ in 2002 customers sent over 92% of all orders in electronic format. by customers. A growing share of transactions enter banks' systems via e-banking, even though companies still rely mainly on other computer connections than Internet, especially batch-based e-banking applications. The share of giro-ATM transactions (credit transfers via ATMs) is also on the rise, while transacting in bank branches continues to lose ground.

Interbank transactions are completely computerised and batch-transferred two or three times a day.

3.3 Settlements made twice daily

Each bank calculates daily its net total of debit and credit transactions against each of the other system banks. This clearing calculation is sent to counterparty banks for tallying and to the Bank of Finland for settlement.

Settlements are executed at the Bank of Finland twice a day, based on clearing calculations. The night clearing is automatically executed in the early morning hours, and the afternoon clearing takes place around normal closing time. Settlement occurs immediately in connection with the clearing, provided there are sufficient funds in all the affected accounts at the Bank of Finland.

If a bank lacks sufficient funds, the clearing is carried out by eliminating that bank. If a bank lacks sufficient funds for the night clearing, an extra clearing takes place in the morning.

Banks exchange transaction information already prior to settlement at the Bank of Finland, but transactions are not entered into customer accounts until it is ascertained that all the banks have sufficient funds; if a bank lacks sufficient funds, its transactions are not entered.

3.4 PMJ settlements are irrevocable

The Ministry of Finance has also confirmed the rules of the PMJ and notified them to the European Commission. The rules ensure that funds transfers are final and irrevocable, as prescribed in the legislation on payment systems. Under the rules, a payment is entered for PMJ settlement when the Bank of Finland receives the clearing calculation in question. A payment becomes binding (final) for the

operator when the sending bank's account at the Bank of Finland is debited in the PMJ settlement entry.

Annex 6

Abbreviations used in the text

APK	=	Finnish Central Securities Depository; handles settlement of quoted shares and other securities
BAC	=	Banking Advisory Committee; European Commission's committee for advising banking sector entities
BIS	=	Bank for International Settlements; international forum for cooperation among owner-central banks
BoF-RTGS	=	Bank of Finland Real-Time Gross Settlement System; real time system for large-value interbank payments
BSC	=	Banking Supervision Committee; ESCB committee operating in connection with European central banks
CLS	=	Continuous Linked Settlement; enables linking of payments in currency trades to obviate settlement risk
CPSS	=	Committee on Payment and Settlement Systems; G10 forum for payment and settlement systems, under BIS aegis
DVP	=	Delivery versus payment; applied in securities trading
EBA	=	Euro Banking Association; banks' linking arrangement for settling euro payments (former name: ECU Banking Association)
EEA	=	European Economic Area
EMI	=	European Monetary Institute (now ECB)
EMU	=	Economic and Monetary Union
ESCB	=	Europe System of Central Banks
Euro1	=	EBA system for handling large-value euro payments
FIBV	=	Federation Internationale des Bourses de Valeurs; international cooperative body for securities exchanges
FSAP	=	Financial Sector Assessment Programme; IMF programme
G10	=	Group of Ten, ten-country group mainly for cooperation among central banks
G20	=	Group of Twenty; cooperative body for banks of 20 countries

G30	=	Group of Thirty; cooperative body for banks of 30 countries
GdC	=	Groupe de Contact; unofficial cooperative body for banking supervisors
IMF	=	International Monetary Fund
IOSCO	=	International Organization of Securities Commissions; international cooperative body for securities market supervisors
ISO	=	International Organisation for Standardisation
ISSA	=	International Securities Services Association; international cooperative body for securities depositories
LORO	=	Loro clearing; system for clearing foreign euro payments
PATU	=	Finnish system for secure information links
PIN	=	Personal identification number; used in accessing ATMs
PMJ	=	Finnish banks' system for (mainly) mass payment transfers
POPS	=	Finnish banks' system for online express transfers and cheques
PSSC	=	Payment and Settlement Systems Committee; ESCB/ECB committee on payment and settlement systems
PVP	=	Payment versus payment
RTGS	=	Real-Time Gross Settlement System
SEPA	=	Single Euro Payments Area
SSL	=	Secure Sockets Layer; Internet security system for privacy in information exchange between service provider and customer determination of service provider's authenticity
STEP1	=	EBA system for small-value euro payments
SWIFT	=	Society for Worldwide Interbank Financial Telecommunication, which maintains a worldwide network for interbank information exchange
TARGET	=	Trans-European Automated Real-Time Gross Settlement Express Transfer System; European payment system that handles EU countries' RTGS and interlinking of their central banks
WGPS	=	Working Group on EU Payment Systems; established by EMI in 1994

Publications of the Bank of Finland

Series A (ISSN 1238-1683, print) (ISSN 1456-5943, online)

(Nos. 1–35. Publications of the Bank of Finland Institute for Economic Research,
'Economic Analyses', a collections of articles from the period 1942–1972,
in Finnish and Swedish, ISSN 0081-9476);
nos. 36–92: Publications of the Bank of Finland in several languages, ISSN 0355-6034);
nos. 93– in several languages.

A:93 Jarmo Kariluoto **Suomen maksutase. Laadintamenetelmät, tiedonhankinta ja vuosien 1975–92 aikasarjat** (Finland's Balance of Payments: Methods of Compilation, Acquisition of Data and Time Series for the Years 1975–92). 1995. 221 p. ISBN 951-686-456-2.

A:94 Juhani Laurila **Finnish-Soviet Clearing Trade and Payment System: History and Lessons**. 1995. 44 p. ISBN 951-686-469-4.

A:95 Jouko Rautava (ed.) **Russia's Financial Markets and the Banking Sector in Transition**. 1996. 201 p. ISBN 951-686-489-9.

A:96 Paavo Peisa (ed.) **Euro – yhteinen raha** (Euro – the Single Currency). 1996. 162 p. ISBN 951-686-499-6.

A:97 Juhani Hirvonen – Matti Virén **Käteisrahan käyttö suomalaisissa yrityksissä** (The Use of Cash in Finnish Business Firms). 1996. 78 p. ISBN 951-686-510-0.

A:98 Jarmo Kariluoto **Finland's Balance of Payments. Compilation methods, sources of information and the time series for 1975 to 1992**. (Finnish version – A:93). 1996. 182 p. ISBN 951-686-522-4.

A:99 Markku Malkamäki (ed.) **Suomen rahoitusmarkkinat 1996**. **(**Financial markets in Finland 1996). 1996. 196 p. ISBN 951-686-524-0. (published in English as a special issue of the Bank of Finland Bulletin, 1996, see p. 5)

A:100 Harry Leinonen – Veikko Saarinen **Suomalaiset maksujärjestelmäriskit ja niiden sääntely- ja valvontatarpeet**. (English version – A:101). 1998. 89 p. ISBN 951-686-565-8.

A:101 Harry Leinonen – Veikko Saarinen **Payment system risks in Finland and the need for regulation and supervision**. (Finnish version – A:100). 1998. 89 p. ISBN 951-686-577-1.

A:102 Heikki Koskenkylä (toim.) **Suomen rahoitusmarkkinat 2002** (Finnish financial markets 2002). Compilation. (English version – A:105). 2002. 357 p. ISBN 952-462-023-5, print; ISBN 952-462-024-3, online.

A:103 Timo Iivarinen – Harry Leinonen – Matti Lukka – Veikko Saarinen **Maksujärjestelmäriskien sääntely ja hallinta – suomalainen näkökulma** (Regulation and control of payment system risks – a Finnish perspective). (English version – A:106). 2003. 136 p. ISBN 952-462-053-7, print; ISBN 952-462-054-5, online.

A:104 Katja Taipalus – Kari Korhonen – Pertti Pylkkönen **Arvopaperistaminen** (Securitisation). 2003. 180 p. ISBN 952-462-067-7, print; ISBN 952-462-068-5, online.

A:105 Heikki Koskenkylä (ed.) **Finnish financial markets 2002** (Suomen rahoitusmarkkinat 2002). Compilation. (Finnish version – A:102). 2003. 360 p. ISBN 952-462-090-1, print; ISBN 952-462-091-X, online.

A:106 Timo Iivarinen – Harry Leinonen – Matti Lukka – Veikko Sarinen **Regulation and control of payment system risks – a Finnish perspective** (Maksujärjestelmäriskien sääntely ja hallinta – suomalainen näkökulma). (Finnish version – A:103). 2003. 135 p. ISBN 952-462-104-5, print; ISBN 952-462-105-3, online

Regulation and control of payment system risks – a Finnish perspective

Bank of Finland Studies A:106 • 2003

ISBN 952-462-104-5
ISSN 1238-1683

Vammalan Kirjapaino Oy
Vammala 2003