EUROPEAN CENTRAL BANK

EUROSYSTEM

OVERSIGHT FRAMEWORK FOR CREDIT TRANSFER SCHEMES

OCTOBER 2010

EUROPEAN CENTRAL BANK

EUROSYSTEM


In 2010 all ECB publications feature a motif taken from the €500 banknote.

OVERSIGHT FRAMEWORK FOR CREDIT TRANSFER SCHEMES

OCTOBER 2010

Address
Kaiserstrasse 29
60311 Frankfurt am Main
Germany

Postal address
Postfach 16 03 19
60066 Frankfurt am Main
Germany

Telephone
+49 69 1344 0

Website
http://www.ecb.europa.eu

Fax
+49 69 1344 6000

Unless otherwise stated, this document uses data available as at xxx.

ISBN 978-92-899-0457-5 (online)

CONTENTS

1 INTRODUCTION

Central banks have the explicit objective of fostering financial stability and promoting the soundness of payment and settlement systems. In accordance with Article 105(2) of the Treaty establishing the European Community and Articles 3 and 22 of the Statute of the European System of Central Banks and of the European Central Bank, one of the basic tasks of the Eurosystem is "to promote the smooth operation of payment systems".

In February 2009 the Eurosystem decided to provide a more precise description of its role in the field of oversight by publishing the "Eurosystem oversight policy framework". This policy statement provides an overview of the set of tools and instruments that the Eurosystem employs and underlines the fact that payment instruments are an essential part of payment systems. The risks involved in providing and using payment instruments have not generally been considered to be of systemic concern, but the safety and efficiency of payment instruments are important for both maintaining confidence in the currency and promoting an efficient economy.

The creation of the Single Euro Payments Area (SEPA) is changing the retail payment landscape significantly, increasing the importance of having a consistent approach in the oversight of payment instruments. The Eurosystem has thus developed a generalised approach and a minimum set of common oversight standards for payment instruments, which are described in the document entitled "Harmonised oversight approach and oversight standards for payment instruments", published by the ECB in February 2009. The aim of these standards is to create a common ground for all payment instrument frameworks, while leaving enough flexibility for the specificities of the individual instruments involved. Hence, they form the basis for the development of oversight frameworks for SEPA direct debits and SEPA credit transfers, as well as for new payment instruments that are used SEPA-wide. Furthermore, each national central bank (NCB) may also decide to apply the common standards to the oversight of other national (non-SEPA) payment instruments if they deem this to be appropriate. In order to take into account the specificities of each of the payment instruments, in addition to applying the standards, the specific content of each of the steps identified in the Eurosystem's harmonised oversight approach for payment instruments needs to be adapted from one payment instrument to the next, on account of the diversified nature of their operation.

For the purposes of this document, a credit transfer scheme is a set of functions, procedures, arrangements, rules and instruments – either paper-based or electronic – that makes it possible to execute a payment order given by the payer to the payment service provider (PSP)[1] for the purpose of placing funds at the disposal of the beneficiary (called the payee). The payer (or originator) is the natural or legal person who gives a payment order; the payee (or beneficiary) is the natural or legal person who is the intended recipient of funds that are the subject of a payment transaction. The transfer of funds is executed by debiting and crediting accounts, regardless of the way the payer provides the funds (the payer may hold an account or provide the funds in cash). Further terms used in this document are defined in the glossary (Annex B).

The oversight framework is based on a "building block" and risk-based approach to ensure, in particular, that it takes into account the way the market for credit transfer payments functions and addresses the relevant risks to which credit transfer schemes are exposed throughout the entire payment cycle, including clearing and settlement.

The oversight framework covers the entire payment cycle, i.e. access to the scheme, the transaction phase, and the clearing and

1 Defined in Title I, Article 4(9), of the Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market.

settlement phase. It takes into account concerns relating to both the retail payment system and the payment instrument used.

The aim of the oversight framework for credit transfer schemes is to ensure the soundness and efficiency of payments made with such instruments. Credit transfer schemes may be exposed to various risks, as is any payment system. Credit transfer schemes should be protected against all risks that could have an overall impact on the confidence of users of the instrument. A clear distinction is made between issues with a scheme-wide impact (e.g. a breach of common rules or security standards, which would place all or a huge proportion of actors in jeopardy) and issues relating to individual actors (e.g. the insolvency of one actor, which would be handled by banking supervision) or that need to be mitigated by the individual actor concerned. In addition, it is particularly important to put efficient and effective governance arrangements in place, as well as to emphasise the importance of preventing any damage to the instrument's reputation.

This note is structured as follows: Section 2 summarises the structure of the oversight standards; Section 3 sums up the different risks to which the participants of a credit transfer scheme are subject; Section 4 specifies the scope of the framework; Section 5 identifies the addressees for the standards; and Section 6 elaborates on the standards. The annexes contain an overview of credit transfer schemes and a glossary.

2 THE STRUCTURE OF THE STANDARDS

This oversight framework follows the Eurosystem's "Harmonised oversight approach and oversight standards for payment instruments", published in February 2009. The common standards have been developed on the basis of identified risk profiles (see Section 3). The framework accommodates the specificities of credit transfer schemes, especially with regard to security-related and operational issues.

Each of the common oversight standards has a number of key issues that are explored in an explanatory memorandum.

3 THE RISK PROFILES

Actors in the scheme may be exposed to certain risks. A payment may fail to be settled for various reasons (discussed below), such as fraud, operational failures or the financial position of one of the actors involved. The different risks identified for a credit transfer scheme may be legal, financial, operational, reputational or linked to overall management.

Legal risk refers to the risk of loss as a result of the unexpected application of a law or regulation, or because a contract cannot be enforced. Legal risk may arise if the rights and obligations of parties involved in a credit transfer scheme are subject to legal uncertainty. Legal risk in a credit transfer scheme may affect various steps and actors. The legal structure of a credit transfer scheme that operates in a cross-border environment is a more complicated issue, as a variety of regulatory frameworks have to be considered in order to ensure enforceability under all relevant jurisdictions.

Financial risk covers a range of risks inherent in financial transactions, including liquidity risk. The oversight standards aim to mitigate financial risks related to the credit transfer scheme, including potential losses resulting from operational risks (e.g. fraud). Within a credit transfer scheme, financial risks may arise for all actors, payees, payers and participating PSPs. The clearing and settlement phase of the credit transfer scheme may give rise to financial risks related to the default or insolvency of the settlement agent or service providers.

Operational risk results from inadequate or failed internal processes or systems, human errors, or external events related to any element of the credit transfer scheme. It can arise as a result of a failure to follow or complete one or more steps in the payment process. Operational risk is often linked to the availability conditions of the credit transfer scheme. It also includes the risk of fraud, since this can be defined as a wrongful or criminal deception which may lead to a financial loss for one of the parties involved and may reflect inadequate safety arrangements. The major fraud risk is the unauthorised debiting of the payer's account. Some fraud risks are due to specific technological choices (such as the routing of orders, or the verification of their validity). On account of the fact that credit transfer schemes mainly rely on interbank operations, internal fraud might be of particular importance.

Reputational risk can be defined as the potential for negative publicity surrounding an actor's business practices – whether grounded in fact or not – to cause a decline in the customer base, costly litigation, decreased revenue, liquidity constraints or significant depreciation in market capitalisation. For a credit transfer scheme, the complexity of the scheme and the high level of automation involved in the processing of transactions make it difficult for customers to understand in detail how it functions. However, credit transfer schemes are closely linked to the operational processes of business end-users, who are able to assess the extent to which the scheme is capable of satisfying their operational needs. This is an important parameter for end-users when choosing a scheme, together with its reputation and cost. What makes reputational risk difficult to quantify and/or identify is that it is both a risk in itself and a derivative risk, i.e. one which stems from other areas of risk and vulnerability. Damage to the scheme's reputation might be the unexpected outcome of operational problems, or of the provision of erroneous or insufficient information to end-users. In other words, as with bank runs, reputational risk generally results from vulnerabilities in other risk areas. However, once it has started, it has its own relevance and requires specific action.

Overall management risk generally arises owing to a lack of strategic choices and policies for the adequate governance and management of the scheme. An overall management risk usually arises if roles and responsibilities are not properly assigned and if decisions regarding objectives and performances are not shared by all actors. An overall management risk often leads to other risks (operational, legal, etc.), since it relates to the core governing functions of any credit transfer scheme. The main consequences of such a risk are a potential conflict of interests among actors and an inability or unwillingness to sustain market dynamics and innovation and to react appropriately in crisis situations. This risk may also have an impact on competitiveness if access policies are non-transparent and inappropriate. The lack of a proper definition of roles and responsibilities can hamper a prompt reaction in the event of a crisis.

4 SCOPE OF THE FRAMEWORK

The Eurosystem will apply this framework to the SEPA credit transfer scheme. Each NCB may also decide to apply these standards for the oversight of other national (non-SEPA) payment instruments, if they deem this to be appropriate. Since the goal of the SEPA initiative is a migration to common standards, the introduction of oversight for national payment instruments in countries where there is no such oversight thus far should only be envisaged if there is sufficient evidence that the national systems will not be phased out within the applicable SEPA deadlines.

As explained in the "Harmonised oversight approach and oversight standards for payment instruments", the Eurosystem intends to avoid overlaps and duplication of work between the oversight standards for payment instruments and other oversight activities or regulations, e.g. other Eurosystem oversight frameworks (such as those for large-value and retail payment systems) or other regulatory authorities (such as banking supervisors). Where the credit transfer scheme uses payment systems within the oversight scope of a Eurosystem central bank (e.g. for clearing and settlement), the governance authority can take this into account in its risk assessment. The overseer may also consider the results of Eurosystem oversight activities, relevant assessments or activities of supervisory bodies and include, where relevant, the operation of credit transfers in the regular monitoring of correspondent banking activities. These provisions do not, however, overrule any national legal obligations or mandates that an NCB might have for payment instruments operating within its national jurisdiction.

5 THE ADDRESSEES

For oversight purposes, the Eurosystem considers the governance authority to be the addressee of the standards.

Governance authority is a term which refers to the actor(s) performing the governance functions described in the scheme's overall management sub-system. The actor performing governance functions is responsible for the functions it performs within the scheme and is the addressee of the standards in this respect. If there is more than one actor for a given scheme, they are jointly accountable for the overall functioning of the credit transfer scheme, for promoting the payment instrument, for ensuring compliance with the scheme's rules and for setting clearly defined, transparent, complete and documented boundaries for their responsibilities within the scheme. These actors must then jointly ensure that all the relevant standards (or parts thereof) of this oversight framework are met. Oversight activities will be conducted taking into account the division of responsibility. Nevertheless, all measures taken and all activities carried out within the scheme should be in line with the security policies defined by the actor(s) performing governance functions

The Eurosystem focuses its approach for the oversight of payment instruments on issues of scheme-wide importance that are under the control of the governance authority of the scheme providing the payment instrument. Although this is a common Eurosystem approach, it is possible for each NCB to go further, and to adopt an approach that also encompasses other actors of the scheme, for instance, if this is required by national law.

6 THE FIVE STANDARDS

Based on the above, five standards have been identified that deal with legal issues, transparency, operational reliability, good governance and sound clearing and settlement processes. A credit transfer scheme should:

1. have a sound legal basis under all relevant jurisdictions;
2. ensure that comprehensive information, including appropriate information on financial risks, is available to the actors;
3. ensure an adequate degree of security, operational reliability and business continuity;
4. implement effective, accountable and transparent governance arrangements; and
5. manage and contain financial risks in relation to the clearing and settlement process.

At the Eurosystem level, the SEPA credit transfer scheme will be assessed against these standards for issues with a scheme-wide impact. To this end, following the harmonised oversight approach for payment instruments, the Eurosystem intends to develop an assessment methodology to serve as a guide for a comprehensible and efficient assessment. Based on their legal mandate, NCBs may implement adjustments for their assessments, if necessary.

STANDARD 1: THE CREDIT TRANSFER SCHEME SHOULD HAVE A SOUND LEGAL BASIS UNDER ALL RELEVANT JURISDICTIONS

Key issues

1.1 The legal framework governing the establishment and functioning of the credit transfer scheme, the relationship between the governance authority and the payer's PSP, the payee's PSP, the payer, the payee and the other service providers,[2] as well as the rules and contractual arrangements governing the credit transfer scheme should be complete, unambiguous, up to date, enforceable and compliant with the applicable legislation.

1.2 If the scheme operates under various different jurisdictions, the law of these jurisdictions should be analysed in order to identify the existence of any conflicts. Where such conflicts exist, appropriate arrangements should be made to mitigate the consequences of these conflicts.

Explanatory memorandum

- The absence of a correct legal incorporation may result in the unlawfulness of all rules and contractual arrangements governing the credit transfer scheme and its relations with its actors.

  Where the rules and contractual arrangements do not comply with the applicable legislation, they (or certain parts thereof) will be invalid, which may give rise to uncertainties. It is thus important to pay due attention to legal compliance from the outset. It is during the initial phase of establishing the scheme that the foundations are laid for its sound functioning in the future.

  Rules and contractual arrangements that are relevant for credit transfer payments between actors (including PSPs and customers), and which are incomplete or inappropriate, may have an impact on other actors in the scheme and this should therefore be a matter of concern for the scheme. Even if the governance authority is not in direct contractual relation with all actors, the rules of the scheme may prevent this impact by defining appropriate minimum requirements for contractual issues between actors (e.g. PSPs and customers), where relevant for the functioning of the scheme.

  Where the legal framework of the credit transfer scheme is sound, and where its rules and contractual arrangements are unambiguous, all of its actors will have a clear understanding of their rights and obligations. This minimises the possibility of their being confronted with unexpected risks and costs resulting from ambiguous legal formulations.

  Given that the law can change, failure to regularly monitor the legal environment and promptly adapt the scheme's rules and contracts accordingly could create conflicts between the scheme's rules and the current legislation and, as a result, lead to uncertainty regarding the credit transfer scheme. For example, the credit transfer scheme may be subject to the risk of scrutiny by competition or data protection authorities, given the nature of its business. Should such a risk materialise, it could ultimately have serious consequences for the scheme concerned.

- The credit transfer scheme may operate in a cross-border environment. Such an environment complicates the task of ensuring legal certainty. Furthermore, in this context, it is very important that the rules and contractual arrangements clearly and unambiguously specify the governing law and the relevant jurisdiction. If these are not specified, the enforceability of the credit transfer scheme's rules and contractual arrangements may be challenged in the event of a dispute.

2 Communication network service providers, IT service providers, clearing providers and the settlement providers.

STANDARD 2: THE CREDIT TRANSFER SCHEME SHOULD ENSURE THAT COMPREHENSIVE INFORMATION, INCLUDING APPROPRIATE INFORMATION ON FINANCIAL RISKS, IS AVAILABLE TO THE ACTORS

Key issues

2.1 All rules and contractual arrangements governing the credit transfer scheme should be adequately documented and kept up to date. All actors and potential actors should be able to easily access information relevant to them, to the extent permitted by data protection legislation, so that they can take appropriate action in all circumstances. Sensitive information should only be disclosed on a need-to-know basis.

2.2 All actors directly involved in the financial flow (payees' PSPs, payers' PSPs, payees and payers) should have access to relevant information in order to evaluate risks affecting them, including financial risks.

Explanatory memorandum

- Clear, comprehensive and up-to-date documentation is essential for the smooth functioning of the credit transfer scheme. In the absence of proper documentation (e.g. contracts) regarding the roles and responsibilities of all actors involved in the scheme or of the proper management of communication between these actors, an overall management risk could arise. In credit transfer schemes, operational risk, including fraud, could lead to financial loss for one or more of the parties involved. The governance authority of the credit transfer scheme should ensure that consistent and up-to-date information on how they can act to mitigate fraud is available to all actors.

  Relevant documentation for evaluating possible risks stemming from participation in the credit transfer scheme should also be available to potential actors. However, the disclosure of sensitive information could endanger the security or reputation of the scheme. Such information should thus only be disclosed on a need-to-know basis, notably with regard to potential actors that are not yet participating in the scheme.

- If the actors directly involved in the financial flow (payees' PSPs, payers' PSPs, payees and payers) do not all have access to relevant information about the risks (that they bear as a consequence of participating in the scheme), they may face potential risks stemming from clearing and settlement, and from fraud (including the liabilities defined by law or contractual agreements). Owing to the complexity of credit transfer schemes, they may not be in a position to identify and assess the risks that could affect them.

  In credit transfer schemes, payers are particularly exposed to the risk of unauthorised payment orders debiting their accounts. A lack of appropriate information about technological/procedural choices (such as order routing and verification of the validity of the orders) could expose payers to financial difficulties or losses resulting from unexpected payment orders, including fraud or other unauthorised transactions.

STANDARD 3: THE CREDIT TRANSFER SCHEME SHOULD ENSURE AN ADEQUATE DEGREE OF SECURITY, OPERATIONAL RELIABILITY AND BUSINESS CONTINUITY

Key issues

3.1 Security management

3.1.1 Risk analysis related to security, operational reliability and business continuity should be conducted and kept up to date in order to determine an acceptable level of risk and to select adequate policies and appropriate procedures for preventing, detecting, containing and correcting violations. Compliance with such formalised policies should be assessed on a regular basis.

3.1.2 Management and staff of all stakeholders involved should be trustworthy and fully competent (in terms of skills, training and number of staff) to make appropriate decisions, endorse security policies and carry out their scheme-related responsibilities and duties.

3.1.3 Operational and incident management should be clearly defined and effectively implemented. As part of this operational management, fraud should be monitored effectively.

3.1.4 The scheme's security policy should ensure the privacy, integrity and authenticity of data and the confidentiality of secrets (where applicable, e.g. for access to remote banking, authentication of the payer and validation of orders) throughout all transaction phases, whenever data are processed, stored or exchanged. Effective contingency plans should be in place in case confidential information is revealed or compromised.

3.1.5 Explicit policies for controlling both physical and logical access to credit transfer processing systems and locations must be defined and documented. Access rights must be used in a restrictive way.

3.2 Security throughout the different phases (access, transaction)

3.2.1 Adequate security requirements should be defined and enforced for the access phase (including the definition of secure procedures for remote electronic payment orders in e-banking systems, for instance, for the delivery of security devices or secrets for the authentication of the actors involved), and for the complete transaction phase (including R-transactions).

3.2.2 Effective and secure procedures should: (i) cover the transmission of the payment order (either paper or electronic) given by the payer to the PSP; and (ii) be in place for the authentication of such orders (in particular for electronic orders) and for avoiding the unauthorised debiting of the payer's account at the PSP.

3.2.3 The activities of payers and payees should be adequately monitored in line with the scheme's security policy in order to enable a timely reaction to fraud and any risks posed by such activities. Appropriate measures should be in place to limit the impact of fraud.

3.2.4 Appropriate arrangements should be made to ensure that credit transfers can be processed at all times, even on peak days.

3.2.5 Sufficient evidence should be provided to enable a transparent and easy clarification of disputes regarding payment transactions between actors.

3.3 Clearing and settlement

3.3.1 Clearing and settlement arrangements should ensure an adequate degree of security, operational reliability and availability, taking into account the settlement deadlines specified by the credit transfer scheme.

3.4 Business continuity

3.4.1 The scheme's business impact analyses should clearly identify the operations that are crucial for the smooth functioning of the credit transfer scheme. Effective and comprehensive contingency plans should be in place in the event of a disaster or any incident that jeopardises the availability of the scheme. The adequacy and efficiency of such plans should be tested and reviewed regularly.

3.5 Outsourcing

3.5.1 Specific risks resulting from outsourcing should be managed with complete and appropriate contractual provisions. These provisions should cover all relevant issues for which the actor who outsources activities is responsible within the scheme.

3.5.2 Outsourcing partners should be managed and monitored appropriately. Actors who outsource activities should be able to provide evidence that their outsourcing partners comply with the standards for which the actor is responsible within the scheme.

Explanatory memorandum

Operational risks, including fraud, could have a serious impact on the credit transfer scheme and could lead to a financial loss for the parties involved. They could also undermine users' confidence in the credit transfer scheme. Mitigation of these risks requires appropriate measures to ensure:

- sound security management;
- security throughout the different phases (access, transaction);
- secure and reliable clearing and settlement;
- business continuity; and
- sound management of outsourcing.

In order to reduce the risk of fraud, the information allowing the transfer of funds from an account by way of straight-through processing (STP) should be adequately protected. Rules should also be designed so that unauthorised transactions can be detected quickly.

In a general model (see Annex A), the operations may not all be under the direct responsibility of the governance authority and some of them may often be in the competitive sphere. However, a lack of security in one specific domain (e.g. PSP to customer) could have an impact on other domains and may therefore be a matter of concern for the whole scheme. Even if the governance authority is not directly involved in all operations, the rules of the scheme should aim to ensure security, operational reliability and business continuity by defining appropriate requirements for other actors (e.g. PSPs, payees and clearing and settlement mechanisms), where applicable and relevant for the overall functioning of the scheme. The aim of such requirements should not be to impose specific solutions: actors should remain responsible for how they implement these requirements.

- **Sound security management**
  - Without regular analyses of operational and security risks to the scheme using widely accepted and up-to-date methodologies, it may not be possible to define appropriate and comprehensive security policies for the scheme. A lack of proper risk management could result in the existence of a set of security standards that do not minimise or eliminate security risks at an acceptable cost. If risk management does not demonstrate clear support for, and a commitment to, the implementation of the security policy, risks may not be addressed adequately.

  - If staff are inadequately qualified or the number of staff is insufficient to cope with the security challenges involved, this may hamper the smooth functioning of the credit transfer. Insufficient knowledge on the part of management regarding risk management processes and IT security may lead to inappropriate decisions being made.

  - Security incidents, including fraud cases, may occur even when all precautions appear to have been taken. Therefore, it is necessary to monitor fraud cases and security incidents. It may be impossible to detect the origin of incidents or to identify the type of vulnerability present. This could be attributable to inadequate or missing contingency plans for limiting the damage. Moreover, if the assets are not clearly and comprehensively understood and defined, it will be difficult to identify the impact of a security breach. Security incidents may also occur as a result of the failure to transmit alerts to the relevant recipients, as a consequence of which they will be unable to react properly to vulnerability and fraud.

- If unauthorised persons are able to execute actions, risks regarding confidentiality, data privacy, and availability and integrity of data or secrets can arise. Moreover, an adequate degree of security is needed to ensure the privacy, integrity and authenticity of data during the transaction (from the creation of the payment order) and in the storage of related data (e.g. data for recurrent transactions). Security features (such as secrets or security devices) used to access remote banking, authenticate the payer and validate payment orders could be disclosed or compromised if sound security management procedures are not in place. Protecting sensitive data is important in the credit transfer scheme since usurped information (notably STP identifiers – IBAN and BIC) can also be used to make unauthorised payment orders in the credit transfer scheme, or to carry out fake transactions via other payment schemes (e.g. creating fake mandates in a direct debit scheme); related risks could be very high if failures are not discovered or reported on time.

- Risks related to wilful misconduct or gross negligence may arise in the event of unauthorised access to high-security areas or to sensitive applications.[3]

- **Security throughout the different phases (access, transaction)**

  Credit transfer operations are made up of several phases: user access to the scheme, the normal execution of the order, and management of R-transactions. It is thus important that the security measures defined and implemented by the actors address all of these phases. Since the payer can make a payment order to the PSP using either paper or electronic instruments and via any of a variety of channels (internet, mobile channel, phone channel, etc.), it is important to ensure that the order is transmitted in a secure way and that the orders are verified/authenticated. If this is not the case, it may result in an unauthorised transaction. The transmission procedure used by the payer to send the payment order to the PSP should maintain the confidentiality, integrity and availability of the payment order details and the identity of the originator. Confidentiality breaches may result in sensitive data being used to carry out fraud within the scheme.

  - Technical failures or criminal deception could result in an unauthorised credit transfer transaction with related financial losses for one of the parties involved. Such risks could arise from:

    (a) procedural choices, such as the routing of orders among PSPs;
    (b) technical failures or counterfeits in hardware/software components;
    (c) an abuse/usurpation of rights;[4]
    (d) fraudulent behaviour by staff; and/or
    (e) a payment order made by a fraudster using a false identity or usurped identifiers (particularly for remote transactions).

3 Applications linked to account management, transmission of a remote payment order, or storage of private data.

4 If unauthorised persons are able to execute actions, risks regarding the proper allocation of funds, or the confidentiality, availability and integrity of data may arise.

Owing to the fact that credit transfer schemes mainly rely on interbank operations, internal risks (points a to d) could be of particular importance. If identifiers can be usurped (e.g. login and password for online banking obtained by fraudsters via "phishing" attacks) and reused, if payers are not identified properly by their PSPs, or if payment orders are not checked/authenticated, the risk that a fraudster will be able to initiate an unauthorised payment order is also of great significance.

– Unless appropriate security measures and facilities are in place to monitor the activities of payers and payees, it is very difficult to limit the impact of fraud. In this respect, data gathered from information exchanged among sub-systems (such as message logging, tracing, etc.) can help to monitor payee/payer behaviour. Therefore, steps could be implemented to mitigate such a risk, e.g. implementing transaction limits or paying special attention to transactions above a certain amount. These should be in line with the scheme's security policy and that of the actors.

– As credit transfers are also used for recurrent transactions related to the real economy (such as periodical mortgage payments, utility bills, payments by instalments, salaries or pensions), many transactions may be concentrated on a few days each month. Apart from the financial issues related to this concentration of transactions, each actor or service provider in the scheme can only process or store a certain amount of data. If this limit is reached, availability and integrity problems may occur on peak days.

– Disputes between actors cannot be solved if transparent and easily accessible information and evidence is not available. Confidence in the scheme would be endangered if such situations occurred too often.

- **Secure and reliable clearing and settlement**
  – Problems within clearing and settlement processes could lead to financial loss for the actors. This could occur on account of inadequate operational reliability, security or business continuity. An adequate degree of security, operational reliability and availability, in line with both the level of risk and contractual obligations (e.g. settlement deadlines), is important to ensure the integrity of all data exchanged within the clearing and settlement processes.

- **Business continuity**
  – Disasters or major events affecting critical business processes could result in prolonged unavailability. If business continuity plans are missing or inadequate, availability, confidentiality and integrity problems may occur and could result in financial loss.

- **Sound management of outsourcing**
  – If some of the credit transfer scheme's functions are outsourced, service level agreements may not be complete or precise enough, and/or inadequate monitoring of the provision of services may cause security breaches. Detailed service level agreements and a penalty system in the event of fraud, processing errors or a loss of availability can, for example, help ensure the sound management of outsourcing.

  – The concentration of activities among a reduced number of outsourcers could pose serious problems with regard to availability and dependence.

STANDARD 4: THE CREDIT TRANSFER SCHEME SHOULD HAVE EFFECTIVE, ACCOUNTABLE AND TRANSPARENT GOVERNANCE ARRANGEMENTS

Key issues

4.1 Effective, efficient and transparent rules and processes should be defined and implemented when:
- making decisions about business objectives and policies, including access policies;
- reviewing performance, usability and convenience of the credit transfer scheme; and
- identifying, mitigating and reporting significant risks to the scheme's operation.

4.2 There should be an effective internal control framework, including an adequate and independent audit function.

Explanatory memorandum

Poor governance may affect the credit transfer scheme. Efficient decision-making bodies and processes are needed in order to prevent, detect and react promptly to disruptions. An updated and comprehensive security policy is needed to build and maintain the trustworthiness of the credit transfer scheme. Effective internal control processes are essential for preventing a loss of confidence in the scheme. Reputational risks may increase significantly if contentious relationships and information needs are not managed properly.

- The credit transfer scheme has a wide variety of stakeholders, including payers' PSPs, payees' PSPs, payers and payees.

  – Adequate and transparent governance arrangements are essential for ensuring that the governance authority of the credit transfer scheme is able to take decisions appropriately, balancing the needs of all stakeholders. Clear and effective communication is a way of achieving transparency. For example, transparent access policies contribute to the awareness of participants and customers regarding how the credit transfer scheme functions and the risks they may face. They also help to ensure that the credit transfer scheme sustains market dynamics and innovation, manages the conflicts of interest that can arise from the involvement of such a wide variety of stakeholders, and reacts promptly and effectively to a crisis situation. Equally important to transparency is the establishment of fair admission/exit criteria.

  – The availability of the credit transfer scheme from a customer perspective is essential for its smooth functioning. It is important from a governance perspective to evaluate and anticipate the evolution of transaction flows to ensure the availability of the scheme even on peak dates. If the governance authority of the credit transfer scheme fails to collect information relating to customer confidence as to whether or not the scheme is meeting its standards (whether these are explicit or implicit), customer needs and expectations may fail to be met. This could also lead to disputes among the actors and/or problems arising as a result of poor performance. These aspects – if properly addressed – help to preserve customer confidence in the credit transfer scheme.

  – Effective risk management processes ensure that the credit transfer scheme is able to prevent, detect and react appropriately to events. Effective risk management should address risks appropriately, in the context of the speed of technological change, changing customer expectations, proliferation of threats and vulnerabilities. It also ensures that the most significant risks are identified and reported regularly to the scheme's governance authority.

  – Effective internal control processes are essential for preventing and promptly highlighting any disruption, errors or instances of fraud resulting in a loss of confidence in the credit transfer scheme. Internal review processes ensure that the causes of errors, fraud and inconsistencies are swiftly identified and that appropriate remedial action can be taken without delay. A regular independent audit provides additional assurance as to the soundness of the arrangements in place.

STANDARD 5: THE CREDIT TRANSFER SCHEME SHOULD MANAGE AND CONTAIN FINANCIAL RISKS IN RELATION TO THE CLEARING AND SETTLEMENT PROCESS

Key issues

5.1 The credit transfer scheme should identify the financial risks involved in the clearing and settlement arrangements and define appropriate measures to address these risks.

5.2 The credit transfer scheme should ensure that all selected clearing and settlement providers are of sufficient creditworthiness, operational reliability and security for their purposes.

5.3 If there are arrangements to complete settlement in the event of an actor defaulting on its obligations, it must be ensured that any resulting commitment by an actor does not exceed its resources, potentially jeopardising the solvency of that actor. The credit transfer scheme must also ensure that actors are fully aware of their obligations under any such arrangement, in line with Standard 2.

Explanatory memorandum

The finality of credit transfer transactions and the financial stability of the credit transfer scheme itself may be jeopardised if the scheme's governance authority does not assess – and mitigate as appropriate – the financial risks involved in the clearing and settlement process.

- A financial default or an operational/security failure by a settlement provider could lead to significant, although not systemic, loss. This is a particularly important issue if the actors carry positive balances with the settlement provider during the process. It is, therefore, important that the creditworthiness and operational/security reliability of the clearing and settlement providers are monitored regularly.

- Arrangements may exist to complete settlement in the event of an actor defaulting on its obligations, in order to contain credit and liquidity risks. This can be beneficial both in terms of reducing financial risks and improving the clarity and certainty of potential financial risks for all actors, especially in multilateral net systems where settlement could gridlock and/or create an unexpected shortage of liquidity.

ANNEX A
OVERVIEW OF CREDIT TRANSFER SCHEMES

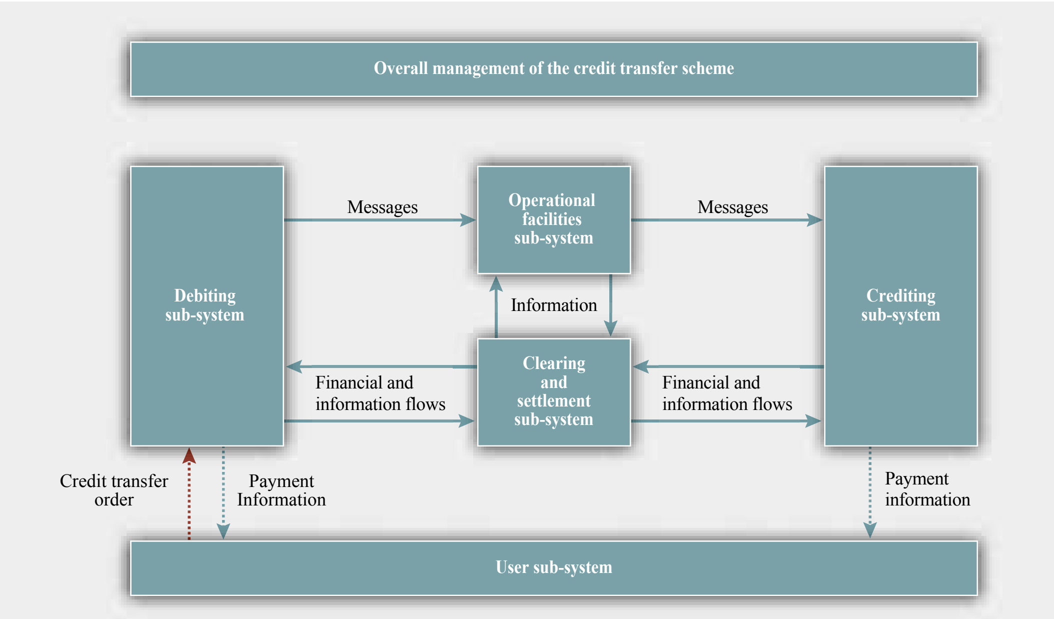
GENERAL MODEL

A credit transfer scheme can be broken down into six sub-systems:

1. overall management of the credit transfer scheme;
2. initiation;
3. crediting;
4. use;
5. operational facilities sub-system; and
6. clearing and settlement.

The different sub-systems present in any credit transfer scheme are described below. Each sub-system is related to a specific function and is explained on the basis of the tasks carried out, and not on that of the physical elements or entities/actors that carry them out. It should be clarified that, within each sub-system, several entities might be involved in performing the related tasks; for instance, in the initiating sub-system, there may also be other entities involved in addition to the payer's PSP. Both the payment instructions and the funds referred to therein move from the payer's PSP to the payee's PSP, possibly via several other PSPs. A person or an entity can play more than one role within the credit transfer scheme, e.g. the payer's PSP and the payee's PSP may be one and the same entity, or one person may be both the payer and the payee.

Credit transfer scheme [1]



Source: ECB.
1) Standard case not necessitating R-transactions.

OVERALL MANAGEMENT OF THE CREDIT TRANSFER SCHEME

This is dedicated to governance (e.g. the definition and allocation of roles and responsibilities, as well as legal arrangements). It covers, for example, the definition of standards (or their selection and adoption when they are publicly available) and rules, the setting of policies concerning access to the scheme, fraud prevention, compliance with the standards and possibly dispute resolution regarding credit transfer scheme rules, etc. It also covers the setting of strategic and interoperability plans. In the SEPA credit transfer scheme, most of these functions are assumed by the European Payments Council (EPC) (Plenary or Scheme Management Committee).

INITIATION SUB-SYSTEM

In the initiation sub-system, the credit transfer instruction is transmitted to, received and checked by the payer's PSP. The payer's PSP is the institution servicing an account for the payer. The instruction is submitted by any means agreed between the payer's PSP and the payer. The initiation sub-system exchanges flows with the crediting sub-system through the clearing and settlement sub-system (financial and information flows) and the operational facilities sub-system (messages).

CREDITING SUB-SYSTEM

In the crediting sub-system, the payee´s PSP receives the credit transfer message, checks the financial and information credit transfer message, credits the account of the payee and makes the proper information available to the payee. The payee´s PSP is the institution servicing an account for the payee. The crediting sub-system exchanges flows with the initiation sub-system through the clearing and settlement sub-system (financial and information flows) and the operational facilities sub-system (messages).

USE SUB-SYSTEM

The use sub-system covers the payment relationship between payers and payees (information on account identifiers) and between them and their PSPs (e.g. terms and conditions for the use of the credit transfer scheme, reporting on the execution/rejection of the order). In this sub-system, the payer originates the credit transfer order, which implies that he/she gives consent to the execution of the payment transaction.

CLEARING AND SETTLEMENT SUB-SYSTEM

This concerns all activities and infrastructures needed for the bilateral or multilateral clearing and settlement of transactions. Different forms of clearing and settlement may be used within the scheme.

OPERATIONAL FACILITIES SUB-SYSTEM

The operational facilities sub-system represents all the technical or organisational services that may be common to actors in the credit transfer scheme. It concerns, for instance, the telecommunication networks enabling the exchange of data between the payee's PSP and the payer's PSP (such as payment orders, returns or rejects, and other information exchanged between participants, e.g. with regard to fraud).[5]

5 Services carried out by the operational facilities sub-system may also include the allocation of specific identifiers to payees and payers.

ANNEX B
GLOSSARY

There may be differences in definitions between various credit transfer schemes. In order to clarify these differences, the definitions used in this document are aligned, as far as possible, with the definitions on credit transfers set out in the Payment Services Directive[6] and by the EPC. This results in the following definitions, which have been applied throughout this document.

Access phase encompasses the access of the actors (service providers or customers) to the scheme.

Actors of the credit transfer scheme are the governance authority, the payer's payment services provider (PSP), the payee's PSP, the technical service provider, the clearing provider and the settlement provider, and the customers (payee and payer).

Credit transfer scheme is a set of functions, procedures, arrangements, rules and instruments, either paper-based or electronic, that enables the execution of a payment order given by the payer to the PSP for the purpose of placing funds at the disposal of the beneficiary (the payee). The transfer of funds is executed by debiting and crediting accounts, regardless of the way the payer provides the funds (the payer may hold an account or provide the funds in cash).

Customers of the credit transfer scheme are the parties (the payee and the payer) using the services of the credit transfer scheme.
- **Payer** (or originator) is the natural or legal person who gives a payment order to the payer's PSP in order to originate a credit transfer transaction.
- **Payee** (or beneficiary) is the natural or legal person who is the intended recipient of funds which are the subject of a payment transaction.

Governance authority is a term which refers to the actor(s) performing the governance functions described in the scheme's overall management sub-system. The actor performing governance functions is responsible for the functions it performs within the scheme and is the addressee of the standards in this respect. If there is more than one actor for a given scheme, they are jointly accountable for the overall functioning of the direct debit scheme, for promoting the payment instrument, for ensuring compliance with the scheme's rules and for setting clearly defined, transparent, complete and documented boundaries for their responsibilities within this scheme. These actors must then jointly ensure that all the relevant standards of this oversight framework are met. Oversight activities will be conducted taking into account the division of responsibility. Nevertheless, all measures taken and all activities carried out within the scheme should be in line with the security policies defined by the actor(s) performing governance functions.

Outsourcing occurs when a service provider contracts a third party to fulfil its own responsibilities as defined by the credit transfer scheme. In general, each service provider is fully responsible for all outsourced activities. Such a service provider must ensure that all outsourced services and activities are provided, managed and monitored in the same way as if they were operated by the service provider itself.

Payment account is an account used for the execution of payment transactions.

6 Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market.

Payment service providers (PSPs) are: (a) credit institutions; (b) electronic money institutions; (c) post office giro institutions; (d) payment institutions; (e) the European Central Bank and national central banks when not acting in their capacity as monetary authorities or other public authorities; and (f) Member States or their regional or local authorities when not acting in their capacity as public authorities.[7] However, in addition, overseers might assess the services of other service providers with a different legal status if their services have an influence on the security of credit transfer schemes.

Thus, with regard to compliance with the oversight standards, there is no differentiation between the legal status of PSPs.

- **Payee's payment service provider** is the PSP where the payee's account is held and which has concluded an agreement with the payee about the rules and conditions of a product based on the scheme. On the basis of this agreement, it receives transactions from the payer's PSP and executes them by crediting the payee's account.
- **Payer's payment service provider** is the PSP which has concluded an agreement with the payer about the rules and conditions of a product based on the scheme. On the basis of this agreement, it executes each payment order given by the payer by forwarding the transaction to the payee's PSP.

R-transactions is the umbrella term for reject and return transactions.

- **Reject** is the result of a failed transaction whereby a credit transfer has already been declined prior to reaching the stage of interbank settlement. Possible causes, among others, could be technical reasons, an incorrect account/bank identifier or regulatory reasons.
- **Return** is the result of a failed transaction that occurs when a credit transfer is diverted from normal execution following interbank settlement and is initiated by the payee's PSP. Reasons could be, among others, closed/blocked/invalid account, regulatory reasons, beneficiary deceased.

Scheme refers to **credit transfer scheme**.

Technical service providers offer technical services within the scheme, such as communications network service, IT service or other technical services.

Transaction phase is the whole process of the execution of a credit transfer payment (normal execution, or the reject/return of a payment order). It is the end-to-end execution of a credit transfer payment.

7 As defined in the Payment Services Directive.