EUROPEAN CENTRAL BANK

EUROSYSTEM

OVERSIGHT FRAMEWORK FOR DIRECT DEBIT SCHEMES

AUGUST 2009

EUROPEAN CENTRAL BANK

EUROSYSTEM

In 2009 all ECB publications feature a motif taken from the €200 banknote.

OVERSIGHT FRAMEWORK FOR DIRECT DEBIT SCHEMES

AUGUST 2009

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

ISBN 978-92-899-0458-2 (online)

CONTENTS

1 INTRODUCTION 4

2 THE STRUCTURE OF THE STANDARDS 5

3 THE RISK PROFILES 5

4 SCOPE OF THE FRAMEWORK 6

5 THE ADDRESSEES 7

6 THE FIVE STANDARDS 7

Standard 1: The direct debit scheme should have a sound legal basis under all relevant jurisdictions 8

Standard 2: The direct debit scheme should ensure that comprehensive information, including appropriate information on financial risks, is available to the actors 9

Standard 3: The direct debit scheme should ensure an adequate degree of security, operational reliability and business continuity 10

Standard 4: The direct debit scheme should have effective, accountable and transparent governance arrangements 14

Standard 5: The direct debit scheme should manage and contain financial risks in relation to the clearing and settlement process 16

ANNEXES

A Overview of direct debit schemes 17

B Glossary of terms and definitions 19

I INTRODUCTION

Central banks have the explicit objective of fostering financial stability and promoting the soundness of payment and settlement systems. According to 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 a new policy statement for its oversight activities.[1] 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 "Harmonised oversight approach and oversight standards for payment instruments" (ECB, 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 remaining national (non-SEPA) payment instruments if it deems 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 differently from one payment instrument to the next, on account of the diversified nature of their operation.

This oversight framework for direct debit schemes applies relevant definitions given in the EC Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market (hereinafter referred to as the "Payment Services Directive" or the "PSD"). Therein, a direct debit is defined as a "payment service for debiting a payer's payment account, where a payment transaction is initiated by the payee on the basis of the payer's consent given to the payee, to the payee's payment service provider or to the payer's own payment service provider".[2] Further terms used in this document are defined in the "Glossary of terms and definitions" (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 direct debit payments functions and addresses the relevant risks to which direct debit schemes are exposed throughout the entire payment cycle, including clearing and settlement.

The aim of the oversight framework for direct debit schemes is to ensure the soundness and efficiency of payments made with such instruments. Direct debit schemes may be exposed to various risks, as is any payment system. Direct debit schemes should be protected against all risks that could have an overall impact on the confidence of users of the instrument.

1 ECB, "Eurosystem oversight policy framework", February 2009.
2 Title I, Article 4(28), of the Payment Services Directive.

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 issues 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 direct debit 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 direct debit schemes and a glossary of terms.

Direct debit scheme – a definition

In line with the PSD definition of a direct debit payment, a direct debit scheme can be regarded as a set of functions (see Annex A), procedures, arrangements, rules and devices that enable the authorised debiting of the payer's payment account, initiated by the payee either as a single payment or a series of payments. The oversight framework covers the entire payment cycle, i.e. access to the scheme, the initiation phase, the transaction phase and the clearing and settlement phase. It takes into account concerns relating to both the retail payment system and the payment instrument used.

2 THE STRUCTURE OF THE STANDARDS

This oversight framework follows the Eurosystem's "Harmonised oversight approach and oversight standards for payment instruments".[3] The common standards have been developed on the basis of identified risk profiles (see Section 3). The framework accommodates the specificities of direct debit 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 and explained in an explanatory memorandum.

3 THE RISK PROFILES

The actors in the scheme (payer, payee, payer's PSP, and payee's PSP) may be exposed to certain risks. A payment may be returned, reversed or fail to be settled for various reasons, such as fraud, operational failures or the financial position of one of the actors involved. The different risks identified for direct debit schemes 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 arises if the rights and obligations of parties involved in a direct debit scheme are subject to legal uncertainty. The analysis of legal risks in a direct debit scheme is difficult owing to the complexity and diversity of such a scheme, which involves various steps and stakeholders (e.g. payer, payer's PSP, payee, payee's PSP, service providers and clearing and settlement mechanisms). The legal structure of a direct debit scheme that operates internationally is even more complex, 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 incurred in financial transactions, including both liquidity and credit risk. The oversight standards aim to mitigate financial risks including potential losses resulting from operational risk (e.g. fraud). Within a direct debit scheme,

3 ECB, "Harmonised oversight approach and oversight standards for payment instruments", Frankfurt, February 2009.

financial risks may arise for all participants, payees, payers and participating PSPs. The clearing and settlement phase of direct debit schemes may give rise to financial risks related to the default or insolvency of the settlement agent or service providers. Financial risk arising from the poor management of mandates is specific to direct debit schemes.

Operational risk results from inadequate or failed internal processes or systems, human errors or external events related to any element of a direct debit scheme.[4] Operational risk can arise as a result of a failure to follow or complete one or more steps in the payment process. Operational risks are often linked to the availability conditions of the direct debit scheme.

Operational risk 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. A typical fraud risk is the unauthorised debiting of the payment account, which could potentially have an impact on some involuntary payers. Some fraud risks are due to specific technological choices, such as the routing and lodging of the mandate and the verification of the validity of direct debit transactions.

Reputational risk can be defined as the potential for negative publicity regarding an institution's business practices – whether grounded in fact or not – to cause a decline in the customer base, costly litigation, revenue reductions, liquidity constraints or significant depreciation in market capitalisation. For a direct debit 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, direct debit 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 refers to the 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 direct debit scheme. The main consequences of this risk are a potential conflict of interests among actors and the inability or unwillingness to sustain market dynamics and innovations and to react appropriately to crises. 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 direct debit 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

4 Bank for International Settlements, "Sound practices for the management and supervision of operational risk", revised, July 2002, Bank of Canada, *Working Paper*, 2003-2, page 11.

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 direct debit scheme uses payment systems within the oversight scope of a Eurosystem central bank (e.g. for clearing and settlement), the governance authority can use this fact in its risk assessment. The overseer may also consider results of Eurosystem oversight activities, relevant assessments or activities of supervisory bodies and include, when relevant, the operation of direct debits 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. The governance authority is accountable for the overall functioning of the direct debit scheme, for promoting the payment instrument and for ensuring that all actors of the scheme are compliant with the rules. In agreement with the overseer, however, the governance authority may appoint another specific actor or actors to be responsible for certain direct debit scheme functions. In such cases, the boundaries set for the responsibilities of these actors must be clearly defined, transparent and documented. These actors then have to meet the relevant standards (or parts thereof) of this oversight framework. Oversight activities will be conducted taking into account this division of responsibility. Nevertheless, all measures and activities taken within the scheme should be in line with the security policies defined by the governance authority.

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 direct debit 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. have 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 direct debit scheme will be assessed against these standards for issues with 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 DIRECT DEBIT 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 direct debit scheme, the relationship between the governance authority and the payee's PSP, the payer's PSP, the payee, the payer and service providers, as well as the rules and contractual arrangements governing the direct debit 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 direct debit scheme and its relations with its actors.

  Where the rules and contractual arrangements (including the mandates between payers and payees) 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 direct debit payments between actors (including PSPs and customers) which are not complete or appropriate 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 direct debit 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, the absence of a regular monitoring of the legal environment and a prompt adaptation of scheme rules and contracts could create conflicts between the scheme rules and current legislation and, as a result, lead to uncertainty regarding the direct debit scheme. For example, the direct debit 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 direct debit 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 (including the mandates) clearly and unambiguously specify the governing law and the relevant jurisdiction. If these are not specified, the enforceability of the direct debit scheme's rules and contractual arrangements may be challenged in the event of a dispute.

STANDARD 2: THE DIRECT DEBIT 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 direct debit 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 (payees' PSPs, payers' PSPs, payees and payers) should have access to relevant information in order to evaluate risks affecting them, including financial risks. Moreover, sufficient information should be provided to the payers by other actors (e.g. payers' PSPs and payees). In particular, payers should be aware of the direct debit transactions they authorise and the mandates they issue, and they should also be informed appropriately about collections.

Explanatory memorandum

- Clear, comprehensive and up-to-date documentation is essential for the smooth functioning of the direct debit 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 direct debit schemes, operational risk, including fraud, could lead to financial losses for one or more of the parties involved. The governance authority of the direct debit 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 direct debit 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 not all actors (payees' PSPs, payers' PSPs, payees and payers) have access to relevant information about the risks they face as a consequence of participating in the scheme, they may face potential risks stemming from clearing and settlement, and from fraud and/or refund obligations. Owing to the complexity of direct debit schemes, they may not be in a position to identify and assess the risks that could affect them.

  In direct debit schemes, payers are particularly exposed to the risk of unauthorised, unjustified or unexpected debiting of their accounts. A lack of appropriate information about mandates given and collections (or refunds) could expose payers to financial difficulties or losses resulting from unexpected collections, including fraud or other unauthorised transactions. Payees are exposed to the same risks for refunds if they are not appropriately informed about the payments they receive and their subsequent exposure to risks.

STANDARD 3: THE DIRECT DEBIT 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 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, there should be an effective monitoring of fraud.

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 electronic mandates) during the initiation phase and the transaction phase, 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 the control of both physical and logical access to direct debit 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, initiation, transaction)

3.2.1 Adequate security requirements should be defined and enforced for the access of actors such as payees to the scheme, the initiation phase (including the option to use electronic mandates and the cancellation of mandates) and the transaction phase (including R-transactions).

3.2.2 Effective and secure procedures should cover electronic mandates and the dematerialisation of paper mandates.

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 direct debits can be processed at all times, even on peak days.

3.2.5 Sufficient evidence should be provided to enable 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 direct debit 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 direct debit 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 direct debit scheme and could lead to a financial loss for the parties involved. They could also undermine users' confidence in the direct debit scheme. Mitigation of these risks supposes appropriate measures to ensure:

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

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

- **Proper 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 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 direct debit scheme. 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, can happen 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 also arise 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, dangers regarding confidentiality, data privacy, 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 initialisation, storage of data for future recurrent transactions, transaction and termination. Protecting sensitive data is particularly important in the direct debit scheme since usurped information (notably STP identifiers – IBAN and BIC) can also be used to create fake mandates or transactions, and failures may go undiscovered or be reported too late.

– Risks related to deliberate actions or unintentional incorrect behaviour may arise in the event of unauthorised intrusions on the premises requiring protection or into sensitive applications (e.g. applications linked to account management, initiation of collections or storage of private data).

- **Security throughout the different phases (access, initiation, transaction)**
  – Direct debit transactions are made up of several phases: user access to the scheme, the mandate (initiation and termination) and the collection of funds (transaction and refund). It is thus important that the security measures defined and implemented by the actors address all of these phases.

  – Since the direct debit scheme may involve the use of electronic mandates or the dematerialisation of mandates, it is important to ensure that the dematerialised mandate data and the payment collection data are accurate and consistent with the actual content of the mandate and with the pre-notified information about the collection. If this is not the case, this may result in unauthorised collections.

  – 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. Therefore, steps to mitigate such a risk could be implemented, e.g. managing payees, implementing transaction limits. These should be in line with the scheme's security policy and that of the actors.

  – As direct debits are largely used for recurrent transactions that occur at a given frequency, 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 and acceptance of the scheme would be endangered if such situations occurred too often.

- **Secure clearing and settlement**
  – Problems within clearing and settlement processes could lead to financial losses, especially for the payee and/or the payee's PSP. These 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 could occur and result in financial losses.

- **Control of outsourcing**
  - If some functions of the direct debit scheme 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 proper 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 DIRECT DEBIT 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 direct debit 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 direct debit 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 direct debit 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 direct debit scheme has a wide variety of stakeholders, including payers' PSPs, payees' PSPs, payers and payees.

  – Adequate and transparent governance arrangements are vital for ensuring that the governance authority of the direct debit 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 direct debit scheme functions and the risks they may face. They also help to ensure that the direct debit 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 direct debit scheme from a customer perspective is vital for its smooth functioning. It is important from a governance perspective to evaluate and anticipate the evolution of transaction flows to ensure availability of the scheme even on peak dates. If the governance authority of the direct debit scheme fails to collect information relating to customer confidence regarding whether or not the scheme is meeting its standards (whether these are explicit or implicit), customer needs and expectations might 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 direct debit scheme.

  – Effective risk management processes ensure that the direct debit 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 direct debit 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 DIRECT DEBIT SCHEME SHOULD MANAGE AND CONTAIN FINANCIAL RISKS IN RELATION TO THE CLEARING AND SETTLEMENT PROCESS

Key issues

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

5.2 The direct debit 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 direct debit 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 direct debit transactions and the financial stability of the direct debit 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, losses. 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 DIRECT DEBIT SCHEMES

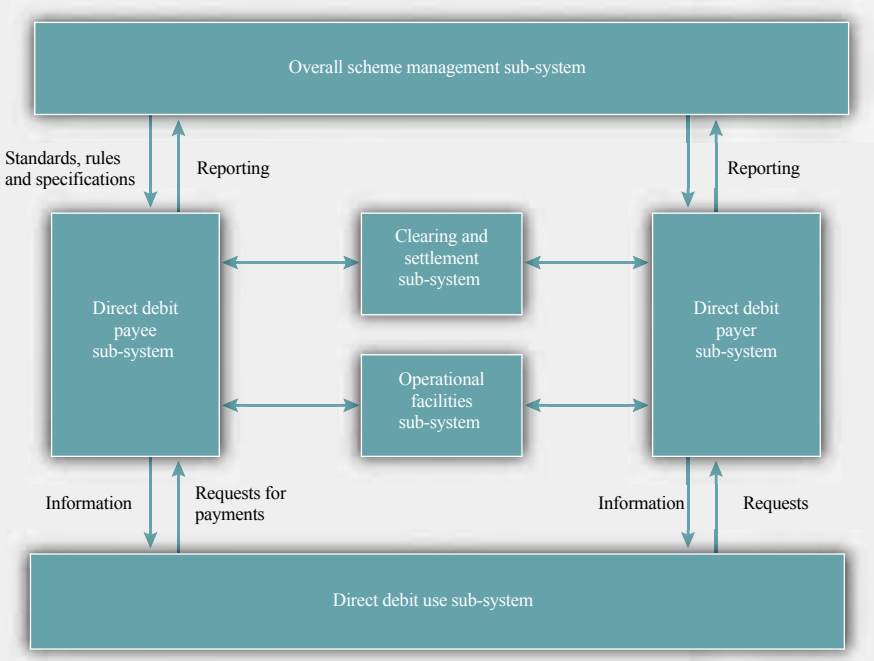
GENERAL MODEL

A direct debit scheme can be broken down into six sub-systems:

1. overall scheme management;
2. direct debit use;
3. direct debit payee sub-system;
4. direct debit payer sub-system;
5. operational facilities; and
6. clearing and settlement.

The different sub-systems present in the direct debit scheme are described below. The sub-systems are presented on the basis of the tasks they carry out, and not on that of the physical elements or entities that carry them out. It should be clarified that, within each sub-system, several entities may be involved in performing the related tasks.

Chart 1



Source: ECB.

The overall scheme management sub-system is dedicated to governance. Its responsibilities include, for example, the definition and evolution of standards, rules and specifications or the selection and adoption of existing ones, as well as policies concerning access to the scheme, competition, pricing, fraud prevention, governance, monitoring of activities, compliance with the standards, dispute resolution, etc. For example, in the SEPA direct debit scheme most of these functions are assumed by the EPC (European Payments Council) (Plenary or Scheme Management Committee).

The *direct debit payee sub-system* includes, notably, accreditation and management of payees, monitoring of activity and fraud, verification, forwarding and execution of transactions (including R-transactions). These activities are generally assumed by the payee's PSP.

The *direct debit payer sub-system* deals with the relationship with payers and the execution of transactions. These activities are generally assumed by the payer's PSP.

The *direct debit use sub-system* covers the relationships between the payer and the payee (mandates, information regarding transactions).

The *operational facilities sub-system* represents technical and organisational services, for example, the telecommunication networks enabling the exchange of data between the payee's PSP and the payer's PSP during the different phases, or other services such as the allocation of identifiers. These activities may be specific to the direct debit scheme or common with other services and may be performed by the same entities as clearing and settlement.

The *clearing and settlement sub-system* concerns all activities and infrastructures needed for the bilateral or multilateral clearing and settlement of direct debit transactions. Different forms of clearing and settlement may be used within the scheme.

ANNEX B
GLOSSARY OF TERMS AND DEFINITIONS

There may be differences in definitions between direct debit schemes. In order to clarify the differences, the definitions used in this document are aligned, as far as possible, with the definitions on direct debits set out in the Payment Services Directive 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 (PSPs or customers) to the scheme.

Actors of the direct debit scheme are the governance authority, the payer's PSP, the payee's PSP, service providers (notably for the operational facilities sub-system and the clearing and settlement sub-system) and the customers (payee and payer).

Collection is the process by which the payment service providers transfer funds from the payer to the payee.

Customers of the direct debit scheme are the parties – the payee and the payer – using the services of the direct debit scheme.

- **Payee** (or creditor) is a natural or legal person who is the intended recipient of funds that are the subject of a direct debit transaction.
- **Payer** (or debtor) is a natural or legal person who holds a payment account and authorises a direct debit transaction from the payment account.

Direct debit is a payment service for debiting a payer's payment account, whereby a payment transaction is initiated by the payee on the basis of the payer's consent which has been given to the payee, to the payee´s payment service provider or to the payer's own payment service provider.

Direct debit scheme is a set of functions, procedures, arrangements, rules and devices that enable an authorised debit of the payer's payment account initiated by the payee, either as a single payment or a series of payments. The oversight framework covers the entire payment cycle, i.e. the initiation phase, the transaction phase and the clearing and settlement phase. It takes into account concerns relating to both the retail payment system and the payment instrument used.

Initiation phase encompasses the creation, management and end (cancellation) of the mandate.

Mandate is the authorisation (consent) given by the payer to the payee and/or to the own payment service provider to debit the account. A mandate may exist as a paper document that has been physically signed by the payer. Alternatively, it may be an electronic document which is created and signed in a secure electronic manner. The mandate, whether in paper or electronic form, must contain the necessary legal text and the names of the parties signing it. In some national variants of direct debit schemes (e.g. one-off direct debit transactions), the mandate is not used.

Outsourcing is a situation where a service provider contracts a third party to fulfil its own responsibilities as defined by the direct debit 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, controlled and monitored in the same way as if they were operated by the service provider himself.

Payment service providers (PSPs) – as defined by the Payment Services Directive – 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.

- **Payer's (debtor's) payment service provider** is the PSP where the payment account to be debited is held and 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 collection of the direct debit originated by the payee by debiting the payer's account.
- **Payee's (creditor's) payment service provider** is the PSP where the payee's payment 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 and executes instructions from the payee to initiate the direct debit transaction by forwarding the collection to the payer's PSP.

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

R-transactions is the umbrella term for the following terms:

- **Refunds** are claims by the payer for reimbursement of contested debits on the account.
- **Refusals** are instructions issued by the payer prior to settlement, for whatever reason, to the effect that the payer's PSP should not make a direct debit payment.
- **Reject** is the result of a failed transaction whereby the payment has already been declined prior to interbank settlement. Possible causes include technical reasons, closed account, insufficient funds.
- **Returns** are direct debit collections that are diverted from normal execution following interbank settlement and are initiated by the payer's PSP.
- **Reversal** is initiated by the payee after settlement in the event that a direct debit that has already been paid should not have been processed. Consequently, it is the reimbursement of funds by the payee to the payer.
- **Revocation** is the request by the payee to recall the direct debit collection prior to acceptance by the payee's PSP.

Transaction phase is the whole process of the execution of a direct debit payment, starting from the collection initiated by the payee up to its finality (the normal execution, or the reject, return or refund of the collection). It is the end-to-end execution of a direct debit payment.