

TERMS OF REFERENCE FOR THE OVERSIGHT ASSESSMENT OF EURO SYSTEMICALLY AND PROMINENTLY IMPORTANT PAYMENT SYSTEMS AGAINST THE CORE PRINCIPLES

These Terms of Reference for the assessment of euro systemically and prominently important payment systems against the applicable Core Principles for Systemically Important Payment Systems¹ (hereafter referred to as the “ToR”) are aimed at providing clear and comprehensive guidelines for the Eurosystem’s payment systems oversight function for the oversight assessments of the relevant systems and the preparation of the respective oversight reports. The use of these ToR should contribute to:

- **minimising the risk of having major inconsistencies** in the implementation of the minimum standards for the Eurosystem’s common oversight policy on systemically important payment systems, as adopted by the Governing Council of the ECB in January 2001, and of the “Oversight standards for euro retail payment systems”, as adopted by the Governing Council of the ECB in June 2003².
- **maximising the credibility of the oversight mission** exercised by the Eurosystem by applying the appropriate level of formalisation in the collection of relevant information, yet taking into account the diversity of the systems subject to the Eurosystem’s oversight policy and keeping an appropriate level of flexibility for assigning observance levels. This flexibility is imperative, not least because the “Oversight standards for euro retail payment systems” explicitly state that the application of some of the Core Principles to euro retail payment systems that are of prominent importance for the economy does not necessarily require the same strict interpretation as for SIPSs.

Despite the use of a single set of ToR for the oversight assessment of both systemically and prominently important payment systems, a distinction still remains under the aspect of “business continuity” of Core Principle VII with respect to the key issues that have to be fulfilled by each category of systems, on the basis of the oversight expectations with regard to business continuity for SIPS³.

¹ See Committee on Payment and Settlement Systems (CPSS), “Core Principles for Systemically Important Payment Systems”, BIS, January 2001. The Governing Council of the ECB adopted the Core Principles as the minimum standards of the Eurosystem’s common oversight policy on payment systems January 2001.

² According to the “Oversight standards for euro retail payment systems”, only Core Principles I, II, VII, VIII, IX and X are applicable to euro prominently important payment systems (PIRPS).

³ See “Business Continuity Oversight Expectations for Systematically Important Payment Systems (SIPS)” adopted by the Governing Council of the ECB, www.ecb.int, 9 June 2006.

The ToR are divided into **three main parts**. Part I addresses the preparation of the introduction to the oversight assessment report and lists the features and aspects that should be covered therein. Part II explains the general modalities of the assessment process, and Part III specifies these general modalities for each individual Core Principle.

Part I: Content of the introduction to the oversight assessment reports

It is recommended that the oversight assessment report starts with a brief introductory part, containing

- a clear definition of the scope/perimeter of the system assessed;
- a short high-level description of the system assessed (including the classification of the system (RTGS, hybrid, deferred net settlement system), the objectives of the system, the access criteria, the architecture, the payment cycles, the intraday and overnight credit arrangements, the pricing rules, the management and governance of the system, basic statistical data (e.g. volumes and values for the last year, peak volume and value days during the last 12 months; projected trends; the intraday pattern; the percentage of customer payments; the number and category of participants; the type and volume of transactions that are typically rejected; and the envisaged changes to the system, if any);
- a brief overview of the results of former oversight assessments, if any, for example the level of observance in the previous assessment as compared with the suggested level of observance for the present assessment.

Part II: General modalities of the assessment process

The ToR require for each of the Core Principles:

- the answers to the key questions with a view to identifying and collecting relevant information/documentation/evidence needed to allow for the sound evaluation of the key issues⁴;
- the description of and the evaluation of any changes or reforms that are in process or that are envisaged and that would modify the existing situation;
- the evaluation of the key issues on the basis of both the evaluated answers to the key questions and the evaluated description of the changes or reforms in order to determine the extent to which a system observes the Core Principle;
- the assignment of a level of observance (observed, broadly observed, partly observed, not observed) on the basis of the evaluation of the information/documentation/evidence collected through the answers to the key questions, the description of any changes or reforms, and the fulfilment of the key

⁴ The key questions that are not relevant for the assessment of a system should be indicated in the assessment report.

issues, thereby taking into account the importance of a system (SIPS or PIPS). Regarding the assignment of a level of observance, the following **guideline** applies.

- **Observed:** all key issues have to be fulfilled;
- **Broadly observed:** some minor problems may be present which do not, however, have a significant impact on the fulfilment of the key issues and, thus, the safety and/or efficiency of the system;
- **Partly observed:** significant issues/risks exist with a significant impact on the fulfilment of the key issues and, thus, the safety and/or efficiency of the system, but these issues/risks will be addressed by the system owner/operator within a reasonable time frame;
- **Not observed:** significant issues/risks exist with a significant impact on the fulfilment of the key issues and, thus, the safety and/or efficiency of the system and the system operator/owner has not planned to address these issues/risks within a reasonable time frame.

When the relevant Eurosystem central bank concludes that the system assessed does not observe a Core Principle, the assessment of this Core Principle should include oversight **recommendations for follow-up actions deemed to be considered and further developed/implemented by the system owner/operator.**

Part III: Specification of the general modalities for each of the ten Core Principles

1. Core Principle I

The system should have a well-founded legal basis under all relevant jurisdictions.

Key issues

1. The legal infrastructure of the system is clearly identified (e.g. the jurisdiction governing the system, applicable laws, statutes, case law, contracts, rules and procedures).
2. Legal issues are clearly identified and understood (e.g. is the Settlement Finality Directive (SFD) implemented in the jurisdiction governing the system, definition of irrevocability, finality, clear liability rules, potential legal risks stemming from relevant jurisdictions other than that governing the system).
3. Legal issues are properly addressed so that the system's rules and procedures are enforceable and their consequences predictable (e.g. system designation under the SFD, specific legal arrangements in case of access of foreign participants).

Key questions

1.1 The legal infrastructure is clearly identified (e.g. the jurisdiction governing the system, applicable laws, statutes, case law, contracts, rules and procedures).

- 1.1.1 What general Community level legislation is applicable to the system?
- 1.1.2 Which jurisdiction governs the system (i.e. what is the jurisdiction under whose law the system's rules and procedures are to be interpreted)?
- 1.1.3 What relevant legislation (laws, statutes, case law, etc.) exists in the jurisdiction governing the system that is applicable to the system?
- 1.1.4 Is there any specific national legislation in the jurisdiction governing the system that relates to payments (please list) and/or is there any specific national legislation that relates to the electronic processing of payments (please explain)?
- 1.1.5 Which specific and legally binding rules (and procedures)/contracts/terms and conditions govern the system? Broadly speaking, what areas do they cover?

1.1.6 What jurisdiction and legal framework governs the establishment and activities of the system operator itself?

1.2 Legal issues are clearly identified and understood (e.g. is the Settlement Finality Directive (SFD) implemented in the jurisdiction governing the system, definition of irrevocability, finality, clear liability rules, potential legal risks stemming from relevant jurisdictions other than governing the system).

1.2.1 Has the Settlement Finality Directive (SFD) been fully implemented in the jurisdiction which governs the system or has a legal review process identified any issues related to the implementation of the SFD in the law governing the system? (please explain)

1.2.2 Has the system been designated under the SFD? If so, when and by whom?

1.2.3 If the system allows for foreign participation, has the SFD or, in the case of foreign participants from non-EU/non-EEA countries, a piece of legislation similar to the SFD been fully implemented in the jurisdiction(s) of these foreign participants or has a legal review process of the jurisdiction(s) governing these foreign participants identified any issues related to the aspects covered by the SFD (in particular related to irrevocability, finality, enforceability of collateral in case of insolvency of a foreign participant)? (please explain).

1.2.4 Has the enforceability of rules and procedures of the system ever been challenged in a national and/or foreign court? If enforceability was not confirmed, provide specific information of relevant cases.

1.3 Legal issues are properly addressed so that the system's rules and procedures are enforceable and their consequences predictable (e.g. system designation under the SFD, specific legal arrangements in case of access of foreign participants).

1.3.1 In general and in particular, for example if the system has not been designated under the SFD, does the legal infrastructure applicable to the system (including the system's rules and procedures) cover clearly:

- The timing of irrevocability and final settlement, especially if there is insolvency?
- The enforceability of collateral (i.e. are the collateral arrangements and agreements supporting the system legally sound), especially if there is insolvency (if applicable)?

- 1.3.2 Which are the specific legal arrangements, if any, that apply in case of access of foreign participants (i.e. participants from other EU, EEA, non-EU/non-EEA countries) to contain legal risks?
- 1.3.3 Have legal capacity and/or country opinions ever been sought and/or have legal investigations been made regarding the enforceability of the system's rules and procedures? If yes, have these legal opinions been sought/investigations been made on the basis of specific terms of reference? Which legal issues/risks have been revealed?
- 1.3.4 What measures have been taken by the system operator/owner to ensure a continuous sound legal basis of the system under all relevant jurisdictions?

2. Core Principle II

The system's rules and procedures should enable participants to have a clear understanding of the system's impact on each of the financial risks they incur through participation in it.

Key issues

1. The documentation covering the management and containment of financial risks (i.e. credit and liquidity risk) is clearly identified.
2. The documentation covering the management and containment of financial risks is up to date, comprehensive and clear.
3. The system operator/owner provides adequate monitoring and support to enable participants and other involved parties (e.g. infrastructure service providers) to understand the rules relating to the management and containment of financial risks.
4. The key rules for the management and containment of financial risk are publicly disclosed, thereby taking due account of possible confidentiality constraints.

Key questions

2.1 The documentation covering the management and containment of financial risks (i.e. credit and liquidity risk) is clearly identified.

- 2.1.1 Which documents comprise the system's rules and procedures?
- 2.1.2 Which parts of the system's rules and procedures are relevant to the management and containment of financial risks?
- 2.1.3 Other than those mentioned under 2.1.1, are there any additional documents/publications (e.g. explanatory material) or procedures relevant to the management and containment of financial risks in the system and/or referring to the rights and obligations/roles and responsibilities of relevant parties?

2.2 The documentation covering the management and containment of financial risks is up to date, comprehensive, and clear.

- 2.2.1 Are the system's rules, procedures, and, insofar as it exists, explanatory material relating to the management and containment of financial risks up to date and accurate and allow for the conclusion that the system owner/operator has a sound understanding of the financial risks that participants might incur through participation in the system?
- 2.2.2 Are arrangements in place that ensure that agreed changes to the rules, procedures, and, if available, explanatory material are incorporated quickly?
- 2.2.3 Do the relevant parts of the system's rules and procedures explain the basic design of the system and its timetable (including a description of the life cycle of a payment in normal circumstances)?
- 2.2.4 Do the relevant parts of the system's rules and procedures relating to the management and containment of financial risks comprehensively cover the rights and obligations as well as the roles and responsibilities of all relevant parties (participants, operators, settlement agent etc.)?
- 2.2.5 Are the rights and obligations as well as the roles and responsibilities of all relevant parties (participants, operator, settlement institution etc.) relating to the management and containment of financial risks clearly explained/described in a structured way and easily understandable in terms of the language used?
- 2.2.6 Do the relevant parts of the system's rules and procedures explain the system's legal basis?
- 2.2.7 Do the relevant parts of the system's rules and procedures explain where and how discretion in decision-making can be exercised with respect to:
 - a) the operation of the system?
 - b) unilateral changes in the rules and procedures of the system and any period of notice?
 - c) the process for consultation and agreement on proposed changes?
 - d) the application of the system's rules and procedures?
- 2.2.8 Do the relevant parts of the system's rules and procedures explain the handling of abnormal situations (decision and notification procedures, and the timetables)?
- 2.2.9 Do the relevant parts of the system's rules and procedures explain remedies to mistakes made by a sending participant and the system operator and remedies to the malfunctioning of the system itself?

2.3 The system operator/owner provides adequate monitoring and support to enable participants and other involved parties (e.g. infrastructure service providers) understanding the rules relating to the management and containment of financial risks.

2.3.1 Does the system operator/owner provide appropriate (technical and non-technical) support and explanations, in particular for new participants and for new staff of existing participants?

2.3.2 Is the performance of participants monitored as evidence of their understanding?

2.3.3 If the system operator/owner identifies participants who do not demonstrate a thorough understanding of the procedures and who could therefore be creating unnecessary risks to the system and its other participants, does the operator advise the participant concerned at an appropriate level within the institution, or, in important cases, the system's overseer or the participant's supervisor?

2.4 The key rules for the management and containment of financial risk are publicly disclosed hereby taking due account of possible confidentiality constraints.

2.4.1 Are the system's rules and procedures and their updating process made transparent to participants, new applicants (i.e. ready before implementation) and involved parties?

2.4.2 Is background information or supporting documentation about the degree of legal certainty associated with the rules and procedures and the enforceability of the rules in various situations (e.g. conclusions of legal opinions together with the analysis of risks) provided to all involved parties?

2.4.3 Are all rules on financial risks disclosed to the public, thereby taking due account of possible confidentiality constraints?

3. Core Principle III

The system should have clearly defined procedures for the management of credit risks and liquidity risks, which specify the respective responsibilities of the system operator and the participants and which provide appropriate incentives to manage and contain those risks.

Key issues:

Credit exposure:

1. The quality of the existing rules and procedures for the management and containment of credit exposures is such that they emphasise the importance of appropriate management of credit risk, provide incentives for its management and containment, and enable all parties to have the capabilities to manage and contain the credit risk they bear.
2. There are clearly defined analytical procedures and/or tools (e.g. information systems for the clear, full and timely monitoring, access criteria based on creditworthiness) in place to analyse credit exposures that participants pose to the system and that the settlement agent might incur.
3. There are clearly defined operational procedures (e.g. credit limits; pre-funding, collateralisation) in place to control and address [manage and contain] in real-time credit exposures that participants pose to the system and that the settlement agent might incur.
4. The existing rules and procedures for the management and containment of credit exposures clearly allocate/specify the system operator, the settlement agent's, and the participants' responsibilities for the management and containment of credit risk.

Liquidity exposure:

5. The quality of the existing rules and procedures for the management and containment of liquidity risk is such that they emphasise the importance of appropriate management of liquidity risk, provide incentives for its management and containment, and enable all parties to have the capabilities to manage and contain the liquidity risk they bear.
6. Clearly defined analytical procedures and/or tools (e.g. information systems for the clear, full and timely monitoring) are in place to analyse liquidity risks that participants pose to the system and that the settlement agent might incur.
7. Clearly defined operational procedures (e.g. queuing facility, pre-funding, redistribution of liquidity intraday) are in place to control and address [manage and contain] in real time liquidity risks that participants pose to the system and that the settlement agent might incur.
8. The existing rules and procedures for the management and containment of liquidity exposures clearly allocate/specify the settlement agent's and the participants' responsibilities for the

management and containment of liquidity risk, and the system operator's and participants responsibilities for monitoring and facilitating a smooth flow of payments through the system.

Key questions: credit exposures

3.1 The quality of the existing rules and procedures for the management and containment of credit exposures is such that they emphasise the importance of appropriate management of credit risk, provide incentives for its management and containment, and enable all parties to have the capabilities to manage and contain the credit risk they bear.

3.1.1 Can any credit exposures arise between participants as a result of the system design? If yes, please describe any actual problems that have occurred in the system in this respect.

3.1.2 What are the incentives provided for in the rules and procedures of the system for the management and containment of credit risk? For example, are incentives provided by means of on-going monitoring and analysis of the credit and liquidity risks participants pose to the system, limits on exposures, by pre-funding or collateralisation of obligations?

3.1.3 Do the rules and procedure of the system allow for an unwinding of payments in the event of a participant failure leading to a recalculation of settlement obligations?

3.1.4 Are there loss-sharing arrangements and/or "defaulter pays" arrangements? If yes, what is the formula used in determining the shares that each participant would bear in case of failure?

3.2 There are clearly defined analytical procedures and/or tools (e.g. information systems for the clear, full and timely monitoring, access criteria based on creditworthiness) in place to analyse credit exposures that participants pose to the system and that the settlement agent might incur.

3.2.1 What type of analytical procedures and/or tools, for example, membership/access criteria based on creditworthiness, controls on the availability of information on unsettled items, are in place to analyse the credit risk?

3.3 There are clearly defined operational procedures (e.g. credit limits; pre-funding, collateralisation) in place to control and address [manage and contain] in real-time credit exposures that participants pose to the system and that the settlement agent might incur.

3.3.1 Which operational procedures (e.g. credit limits, pre-funding, collateralisation, multiple settlement cycles intraday) are in place to control and address [manage and contain] in real-time credit exposures that participants pose to the system and that the settlement agent might incur.

3.3.2 Do the system's rules and procedures foresee that (bilateral and/or multilateral) limits are placed on the maximum level of credit risk that can be created by any participant? If yes, what are the factors (e.g. creditworthiness, operational considerations) that usually influence the levels at which these limits are set? Can these limits be varied intraday?

3.3.3 Can any credit exposure arise for the settlement agent/institution (providing liquidity) vis-à-vis the participants? If yes, is this credit risk mitigated, and how (collateral, haircuts, etc.)?

3.4 The existing rules and procedures for the management and containment of credit exposures clearly allocate/specify the system operator, the settlement agent's, and the participants' responsibilities for the management and containment of credit risk.

3.4.1 What are the responsibilities of the system operator, settlement agent and the participants for the management and the containment of credit risk (e.g. real-time financial information to participants)?

Key questions: liquidity risks

3.5 The quality of the existing rules and procedures for the management and containment of liquidity risk is such that they emphasise the importance of appropriate management of liquidity risk, provide incentives for its management and containment, and enable all parties to have the capabilities to manage and contain the liquidity risk they bear.

3.5.1 Can any liquidity risks arise between participants as a result of the system design? If yes, please describe any actual problems that have occurred in the system in this respect.

- 3.5.2 What are the incentives provided for in the rules and procedures of the system for the management and containment of liquidity risk? For example, are incentives provided by means of the pricing structure (including possibly contractual penalties), for example to reinforce throughput guidelines or to discourage borrowers of intraday liquidity from the central banks from failing to repay by the end of the system's operating day?

3.6 Clearly defined analytical procedures and/or tools (e.g. information systems for the clear, full and timely monitoring) are in place to analyse liquidity risks that participants pose to the system and that the settlement agent might incur.

- 3.6.1 What type of analytical procedures and/or tools, for example membership/access criteria based on creditworthiness, controls on the availability of information on unsettled items, do the system's rules and procedures foresee to control liquidity risk and to address it once it crystallises?
- 3.6.2 What system facilities and/or other procedures are available for participants to monitor and acquire information on their position in the system? What type of information is made available to participants and how frequently is this done?
- 3.6.3 How sizeable are the liquidity needs of the system in relation to the values processed (e.g. value of liquidity needed as a proportion of value of payments)?
- 3.6.4 How sizeable are the liquidity needs of the system in relation to participants' resources (quantitative and/or qualitative judgements needed on how sizeable is the liquidity demand)?
- 3.6.5 Are any other analytical tools used for managing and containing liquidity risk? (If yes, please describe them.)

3.7 Clearly defined operational procedures (e.g. queuing facility, pre-funding, redistribution of liquidity intraday) are in place to control and address [manage and contain] in real time liquidity risks that participants pose to the system and that the settlement agent might incur.

- 3.7.1 What type of procedures/mechanisms/tools does the system provide that potentially enable participants to economise on their liquidity needs (e.g. offsetting mechanisms, centralised queues, others)?

- 3.7.2 Has gridlock occurred? If yes, what mechanisms are in place to mitigate the risk of gridlock and/or to clear gridlocks?
- 3.7.3 If the system employs payment queues, is there a management of payment queues? (If yes, please describe in more detail the queuing algorithm (e.g. FIFO), including the basis on which payments are queued, released and settled. Do the system rules provide all parties involved with a clear understanding of the status and treatment of payments that remain in any queue at the close of the system's operating day?)
- 3.7.4 Are any other operational mechanisms/tools used for managing and containing liquidity risk? (If yes, please describe them.)
- 3.7.5 Do the system's rules and procedures foresee that (bilateral and/or multilateral) limits are placed on the possible liquidity constraints that can be created by any participant? If yes, what are the factors (e.g. creditworthiness, operational considerations) that usually influence the levels at which these limits are set? Can these limits be varied intraday?
- 3.7.6 What additional financial resources, for example the extension of intraday liquidity from the central bank/settlement agent/settlement institution, are available to overcome liquidity constraints?
- 3.7.7 Does the system have throughput guidelines or similar rules/agreements? What measures are taken (e.g. close monitoring by the participant concerned and the system operator) to ensure that these guidelines/rules/agreements are enforced effectively?

3.8 The existing rules and procedures for the management and containment of liquidity exposures clearly allocate/specify the settlement agent's and the participants' responsibilities for the management and containment of liquidity risk, and the system operator's and participants' responsibilities for monitoring and facilitating a smooth flow of payments through the system.

- 3.8.1 What are the responsibilities of the system operator's, the settlement agent and the participants for the management and the containment of liquidity risks?

4. Core Principle IV

The system should provide prompt final settlement on the day of value, preferably during the day and at a minimum at the end of the day

Key issues

1. Any payment order that is accepted by the system for settlement should be finally settled promptly and at the latest at the end of the intended day of value on which it is due to the receiving participant in the system.
2. The life cycle of a payment in the system (submission, validation, acceptance, irrevocability, rejection, finality of a payment) should be clearly defined in the relevant system's rules and procedures and these rules and procedures should be legally effective.

Key questions

4.1 Any payment order that is accepted by the system for settlement should be finally settled promptly and at the latest at the end of the intended day of value on which it is due to the receiving participant in the system.

- 4.1.1 What type of payment instrument does the system use for settlement?⁵
- 4.1.2 In which cases, if any, does the central bank/settlement institution/settlement agent give an explicit and legally valid guarantee for the settlement on the intended day of value, even if final settlement does not actually occur on the intended day of value?
- 4.1.3 In case of the system being an RTGS or hybrid system, what is the maximum time lag (interval) between the system's acceptance of a payment for settlement and the final settlement of that payment under normal circumstances?
- 4.1.4 In case of the system being a deferred net settlement system, how often are net balances/positions settled under normal circumstances (e.g. at several designated times in the course of the operating day or at the end of the day only)? Are participants with short positions required to fund their positions rapidly? Once participants with short positions have funded these positions, are these funds paid out promptly to the participants with long positions? Is it ensured that no pay-outs are made before pay-ins are completed? What tools are available to the

⁵ See report on Core Principles for Systemically Important Payment Systems, CP IV, page 31, paragraph 7.4.2. For example, if the system uses cheques for settlement, this system would not satisfy CP IV; the reason being that cheques are themselves settled finally only after the day of value.

participants to keep the time lag as short as possible (e.g. real time information of final account balances)?

4.1.5 Does the final settlement of a payment or position (in case of a net settlement system) – as defined in the system’s rules and procedures – take place on the intended day of value under normal circumstances?

4.2 The life cycle of a payment in the system (submission, validation, acceptance, irrevocability, rejection, finality of a payment) should be clearly defined in the relevant system’s rules and procedures and these rules and procedures should be legally effective.

4.2.1 Under normal circumstances, what are the respective cut-off times for submitting payments and for settlement processes? Are these cut-off times strictly enforced? Under what circumstances can these cut-off times be extended and are the system’s rules governing the approval of and the allowable length of time for extensions clear on that? Do the rules make clear that extensions of cut-off times are exceptional and require individual justification?

4.2.2 If the system allows payments to pass the risk management test before the intended day of value are such payments regarded as being accepted for settlement on the start of operations on the intended day of value only?

4.2.3 Under normal circumstances, by whom, when and under what conditions can payment orders be rejected? How is the sender informed?

4.2.4 What happens with mistaken payments (e.g. incorrect value date, non-existing receiving bank)?

4.2.5 What are the possibilities to change the status of a payment (e.g. assignment of priorities, if applicable, cancellation)?

4.2.6 Are the operating procedures compatible with the system’s rules concerning irrevocability of a payment order, in particular in case of insolvency of a participant?

4.2.7 Are the operating procedures compatible with the system’s rules concerning finality of a payment?

- 4.2.8 Are the system's rules and procedures clear about the fact that a payment order accepted by the system for settlement cannot be removed from the settlement process?⁶
- 4.2.9 Is unwinding possible and, if so, what are the system's rules in view of the finality of payments? Is the procedure tested regularly?
- 4.2.10 Is information about final settlement provided to the sender and receiver?

⁶ This key question addresses the issue of removing a payment order from the settlement process, i.e. during the time between the system's acceptance of a payment order for settlement (acceptance) and the time when the settlement account of the receiving participant within the payment system has been credited and settlement is unconditional and irrevocable (settlement with finality). Acceptance is achieved once the payment order has successfully passed all of the system's risk management and other tests (i.e. the technical and financial validation of the payment order was positive) and, thus, can be finally settled. Using this reasoning, payment instructions in a waiting queue are not considered to be accepted by the system. In an RTGS system, there is an assumption that, after the moment of acceptance, the payment order cannot be removed from the settlement process anymore and that settlement with finality follows immediately. In a DNS system, after the moment of acceptance, the payment is netted and settlement with finality only takes place at a designated time. Particularly in this environment, the system's rules and procedures should be clear that the payment cannot be removed from the settlement process after its acceptance by the system. For further details, see report on Core Principles for Systemically Important Payment Systems, page 32, Box 9.

5. Core Principle V⁷

A system in which multilateral netting takes place should, at a minimum, be capable of ensuring the timely completion of settlement in the event of an inability to settle by the participant with the largest single settlement obligation.

Key issues

1. Deferred net systems settling on a multilateral net basis must be able to withstand as a minimum the inability to settle of the largest single net debtor to the system.
2. The system's financial risk management features in place to withstand as a minimum the inability to settle of the largest single net debtor to the system should allow for a timely completion of daily settlement.

Key questions

5.1 Deferred net systems settling on a multilateral net basis must be able to withstand at a minimum the inability to settle of the largest single net debtor to the system.

- 5.1.1 Do participants of the system have obligations against the system operator or against the other participants? Does the system operator have obligations (e.g. the provision of liquidity) towards the participants?
- 5.1.2 Which features for the management of financial risks has the system established to ensure, with a high degree of confidence, that daily settlement in the case of the inability to settle of the largest single net debtor to the system will be completed? On which arrangements are these features based (e.g. pre-collateralised positions (so called "defaulter pays") vs. loss sharing arrangements (so called "survivors pay"))?
- 5.1.3 If the system requires deposits by participants as additional financial resources to form a pool of collateral with a view of enabling the system to complete settlement in adverse circumstances, is it guaranteed that the exposures of the largest net debtor do not exceed the size of the deposits? How are the shares of individual institutions to the pool of collateral determined? Who controls the pool?

⁷ Core Principle V is not applicable for RTGS systems. If systems of other types, such as hybrid systems, involve multilateral netting and the deferral of settlement, the overseeing central bank will consider whether the risks are similar. If the overseeing central bank concludes that the risks are similar, it will apply an approach similar to Core Principle V.

- 5.1.4 If the system requires the participants to provide securities to form a pool of collateral as additional financial resources with a view to enabling the system to complete settlement in adverse circumstances, is it guaranteed that the exposures of the largest net debtor do not exceed the value of the securities? How are the shares of individual institutions to the pool of collateral determined? Who controls the pool? Are there any (custodial and control) mechanisms in place to ensure that the collateral will actually be available to complete settlement as planned by the system? Are the securities that make up the pool of collateral revalued frequently (at least daily)?
- 5.1.5 If the system applies loss-sharing arrangements, how do these function? How are individual shares in the loss sharing defined?

5.2 The system's financial risk management features in place to withstand at a minimum the inability to settle of the largest single net debtor to the system should allow for a timely completion of daily settlement.

- 5.2.1 How is it ensured that the financial risk management features which the system applies will allow for a timely completion of settlement, i.e. on the intended day of value? For example, regarding the use of a securities-based collateral pool, are there any (custodial and control) mechanisms in place to ensure that the collateral will actually be available to complete settlement as planned by the system? Are the securities making up the pool of collateral revalued frequently (at least daily)?
- 5.2.2 Is the settlement period timed appropriately to allow for a triggering of financial risk management procedures compatible with the operating hours of the settlement agent?
- 5.2.3 Are sufficient additional liquid financial resources for settlement readily available to complete settlement quickly?
- 5.2.4 How is the use of the collateral pool, if any, organised?
- 5.2.5 Is there a minimum level for collateral (e.g. deposits, securities) required for starting the operations or for covering intraday debit positions?

6. Core Principle VI

Assets used for settlement should preferably be a claim on the central bank; where other assets are used, they should carry little or no credit risk and little or no liquidity risk

Key issues

1. The settlement asset carries little or no credit/liquidity risk.
2. Risk management measures are in place concerning the settlement institution if the settlement asset is not a claim on the central bank.

Key questions

6.1 The settlement asset carries little or no credit/liquidity risk

- 6.1.1 Who is the provider of the settlement asset?
- 6.1.2 If the settlement institution is not the central bank that issues the currency, would the failure of this settlement institution translate in significant credit/liquidity risks for participants to the system?

6.2 Risk management measures are in place concerning the settlement institution if the settlement asset is not a claim on the central bank

- 6.2.1 If the settlement institution is not a central bank, is the scope of the activities of the settlement institution reduced to limited functions? What activities are allowed? Is the settlement institution a supervised institution?
- 6.2.2 What are the arrangements between the settlement institution and the settlement agent concerning the settlement asset? What is the purpose of this arrangement?⁸
- 6.2.3 Is a high standard for the creditworthiness of the issuer of the settlement asset demanded? How is the creditworthiness of the settlement institution assessed (e.g. capital level, credit ratings, etc.)? Is it assessed regularly by the system operator?

⁸ In case of liquidity shortages, has the settlement agent made special arrangements with the issuer of settlement assets to cater for urgent liquidity needs?

- 6.2.4 Is the size and duration of involuntary exposures towards the settlement institution assessed? Is the time of exposure minimised by the system design?
- 6.2.5 What are the risk management features/controls to reduce credit and liquidity risks in respect of claims on the settlement agent?
- 6.2.6 What is the time span, if any, for exchanging the settlement asset, i.e. the time between debiting the ordering participant and crediting the receiving participant?
- 6.2.7 How readily can the settlement asset used for settlement of payment obligations within the system be transferred into other liquid assets or claims on a central bank?

7. Core Principle VII

The system should ensure a high degree of security and operational reliability and should have contingency arrangements for the timely completion of daily processing

Key issues

General

1. The system operator, the participants and any relevant third party have agreed on a set of security policies and operational service levels that have to be met by all of them. These policies and service levels are in line with international standards in terms of confidentiality, integrity, authentication, non-repudiation and availability of information, as well as auditability of processes and procedures.
2. If new technologies are applied, the implications for security and operational reliability should be well understood and addressed.

Security

3. Security objectives, policies and procedures exist and are commensurate with the importance of the payment system in terms of transaction volumes and values.
4. Responsibilities for information security are clearly defined.
5. A risk assessment is regularly performed by the system operator and results are reported to the system owner.
6. The system is subject to a continuous independent security review.

Operational reliability

7. Operational and technical procedures are comprehensive, rigorous and well documented.
8. Changes are properly tested, authorised and documented.
9. Capacity requirements are incorporated in the design of the system, monitored and upgraded when necessary.
10. The system should be administered and operated by an adequate number of well-trained staff.
11. Operational and security incidents are reported, recorded, analysed and followed-up appropriately.

Business continuity - for prominently important payment systems (notably PIRPS)

12. Business continuity arrangements ensure that the agreed service levels are met in the event of the malfunctioning of one or more of the system components/in the event of a variety of plausible scenarios and commensurate to the importance of system.
13. Business continuity arrangements are documented and regularly tested.
14. Business continuity arrangements include crisis management, information dissemination, and analysis of residual risks.

*Business Continuity - for systemically important payment systems (large-value and retail SIPS)*⁹

The fulfilment of the following four key issues by SIPS is dependent on the evaluation of the information gathered regarding the respective “standard practices” as well as “good practices” as included in the “Guide for the assessment against the business continuity oversight expectations for SIPS” (see Annex).

15. Systems should have a well-defined business continuity strategy and monitoring mechanism endorsed by the board of directors. Critical functions should be identified and processes within these functions categorised according to their criticality. Business continuity objectives for SIPS should aim at the recovery and resumption of critical functions within the same settlement day.
16. Business continuity plans should envisage a variety of plausible scenarios, including major natural disasters, outages and terrorist acts affecting a wide area. Systems should have a secondary site, and the latter’s dependence on the same critical infrastructure components used by the primary site should be kept to the minimum necessary to enable the stated recovery objectives for the scenarios concerned to be met.
17. System operators should establish crisis management teams and well-structured formal procedures to manage a crisis and internal/external crisis communications.
18. The effectiveness of the business continuity plans needs to be ensured through regular testing of each aspect of the plan. System operators should consider performing whole days of live operations from the secondary site, and the latter should also be tested periodically with the participants’ contingency facilities. Systems should participate in industry-wide testing organised and coordinated by a commonly agreed financial authority. System operators’ business continuity plans should be periodically updated, reviewed and audited to ensure that they remain appropriate and effective. Operators should consider the partial disclosure of business continuity plans to external stakeholders such as other SIPS, overseers and banking supervisors.

⁹ Until June 2009, the assignment of a level of observance of Core Principle VII (as far as the aspect of “business continuity” is concerned) to systemically important payment systems will depend on the fulfilment of the key issues (and the collection of information via the respective key questions) on “business continuity” for prominently important payment systems.

Annex: “Guide for the assessment against the business continuity oversight expectations for SIPS”

Key questions

General

7.1 The system operator and the participants and any relevant third party have agreed on a set of security policies and operational service levels that have to be met by all of them. These policies and service levels are in line with international standards in terms of confidentiality, integrity, authentication, non-repudiation and availability of information, as well as auditability of processes and procedures.

7.1.1 Have security objectives, policies, procedures and service levels been established during the design of the system and has the system been developed and operated accordingly?

7.1.2 Have objectives, policies and procedures related to the security and operational reliability of the system (especially in terms of confidentiality, integrity, authentication, non-repudiation, availability and auditability) been selected according to national, international or industry-wide standards (please indicate which standard)?

7.1.3 Do these objectives, policies and procedures apply to the operator and the participants in the system?

7.1.4 Has the system owner/operator consulted the participants and any relevant third party with a view to agreeing on specific policies and service levels?

7.1.5 How is it ensured that the relevant parties (participant, operator, third parties) adhere to the agreed principles and share the security objectives?

7.1.6 Security objectives, policies, and procedures are reviewed periodically and updated when appropriate.

7.2 If new technologies are applied, the implications for security and operational reliability should be well understood and addressed.

7.2.1 Are security policies and service levels reviewed in the light of market and technology developments?

Security

7.3 Security objectives, policies, and procedures exist and are commensurate with the importance of the payment system in terms of transaction volumes and values.

7.3.1 What considerations underpin the definition of the security objectives, policies and procedures in place? Who is responsible for their definition and implementation?

7.4 Responsibilities for information security are clearly defined.

7.4.1 If applicable, are there arrangements to ensure that all parties involved in the outsourcing of information processing (including sub-contractors) are aware of their security responsibilities?

7.5 A risk assessment is regularly performed by the system operator and results are reported to the system owner.

7.5.1 Are the systems subject to regular security assessment and risk analysis using recognised methodologies? If yes, which elements do the security assessment and the risk analysis cover (e.g. identification of threats and their likelihood and impact if they materialise)?

7.5.2 How are the security assessment and the risk analysis process structured? Which is the methodology used for risk analysis?

7.5.3 Do the security assessment and the risk analysis take into account market and technology developments in order to be kept up to date?

7.5.4 Is the outcome of the security assessment and the risk analysis regularly reported to the system owner/board and the system overseer?

7.6 The system is subject to a continuous independent security review.

- 7.6.1 Are security policies, procedures and their implementation subject to review by, for example, internal and/or external auditors or the relevant overseer?
- 7.6.2 Are there any IT auditors in the Internal Audit department?

Operational reliability

7.7 Operational and technical procedures are comprehensive, rigorous and well documented.

- 7.7.1 Are operational and technical procedures formally and well documented by the system operator and the participants and available? If yes, in which format (e.g. in service level agreements)?
- 7.7.2 Are there arrangements to monitor the operational reliability when the responsibility for information processing has been outsourced?
- 7.7.3 Do hardware, software and communication vendors contractually provide maximum response times in case of failure?
- 7.7.4 Has the system operator specified required service levels, alternate routings and contingency arrangements in its contracts with the telecommunications providers?
- 7.7.5 Are any losses of payment instructions anticipated as a result of technical failures?
- 7.7.6 Are there arrangements to ensure the awareness of participants of operational risks they might incur through participation in the system?
- 7.7.7 What procedures are applied to make the system operator aware of the availability of the participants' system components during normal business hours?

7.8 Changes are properly tested, authorised and documented.

- 7.8.1 Are significant system changes (including the components belonging to the system participants and any relevant third party) authorised, tested, subject to quality assurance by the relevant parties, and adequately documented? Is this done on a separate development platform/mainframe in order to avoid any adverse impact on the production system? Does this development platform comply with the same levels of security as the production system? Can changes be reversed, if necessary?

- 7.8.2 Are system changes subject to a security review which is independent from the actual system operator?
- 7.8.3 Are there admission tests for prospective participants?
- 7.8.4 Are there periodical tests for existing participants?
- 7.8.5 Are there admission tests for indirect participants? Is there any responsibility for the relevant direct participants?

7.9 Capacity requirements are incorporated in the design of the system, monitored and upgraded when necessary.

- 7.9.1 Is capacity taken into account in the design of the system, in order to ensure the operational reliability of the system? Is the capacity of the system regularly monitored and upgraded when appropriate? Does the system operator carefully plan for any changes of volumes or business patterns so that the required levels of payment throughput and speed are maintained?

7.10 The system should be administered and operated by an adequate number of well-trained staff.

- 7.10.1 Is an adequate number of well-trained, competent and trustworthy staff to operate the system safely and efficiently in both normal and abnormal situations in place?

7.11 Operational and security incidents are reported, recorded, analysed and followed-up appropriately.

- 7.11.1 What is the system's track record in terms of availability?
- 7.11.2 Are all incidents logged, reported, systematically investigated, and appropriately followed-up?
- 7.11.3 What were the most severe incidents until now and what measures have been taken to prevent them from reoccurring?

Business Continuity - Key questions for prominently important payment systems (notably PIRPS)

7.12 Business continuity arrangements ensure that the agreed service levels are met in the event of the malfunctioning of one or more of the system components/in the event of a variety of plausible scenarios and commensurate with the importance of system.

7.12.1 Are there business continuity objectives?

7.12.2 Are those objectives in line with the service level agreed with participants?

7.13 Business continuity arrangements are documented and regularly tested.

7.13.1 Are business continuity objectives, arrangements and procedures (including, for example, hardware and network equipment, staff, data replication, recovery time, testing, residual risks) documented and endorsed by senior level managers? Which scenarios do the planned business continuity arrangements include (e.g. the failure of each of the central components, the failure of participants' components)?

7.13.2 At what frequency are business continuity plans updated, verified and tested? Are they well documented? Have tests shown that the business continuity arrangements work at times of stress?

7.14 Business continuity arrangements include crisis management, information dissemination, and analysis of residual risks.

7.14.1 Are there crisis management and information dissemination procedures (including, for example, the rapid formation of multi-skilled crisis management teams, escalating procedures, decision-making responsibilities, measures to inform the overseers, etc.)?

7.14.2 Is there a back-up for the place of operation (back-up site, second processing site)?

7.14.3 If there is a second processing site, what is the distance to the primary site? What is the difference in the risk profile of the two sites? Does the second site have identical software, hardware and telecommunications to the prime site? How quickly is it operational and ready to start processing?

7.14.4 Which measures have been taken by the system owner/operator to protect against the failure of an infrastructure service provider (such as the power supply or telecommunications)?

7.14.5 Has the system operator/owner considered whether the participants should have a secondary site and, if so, what are the conclusions?

Business Continuity –Key questions for systemically important payment systems (large-value and retail SIPS):

See synopsis of the key issues on “business continuity” at the beginning of Core Principle VII and “Guide for the assessment against the business continuity oversight expectations for SIPS” (Annex).

8. Core Principle VIII

The system should provide a means of making payments which is practical for its users and efficient for the economy.

Key issues

1. The system continuously meets the needs (e.g. technology, operating hours and procedures, technical performance, business continuity) of the users (meaning both the system's participants and their customers for payment services), and procedures are in place to review and update the service level.
2. The needs of all types of users are considered in the design of the system and its evolution (e.g. by way of cooperation, consultation and coordination of plans).
3. Resources are allocated efficiently.
4. The pricing policy (cost recovery method, market based pricing, subsidised pricing) is communicated clearly to participants.

Key questions

8.1 The system continuously meets the needs (e.g. technology, operating hours and procedures, technical performance, business continuity) of the users (meaning both the system's participants and their customers for payment services) and procedures are in place to review and update the service level.

- 8.1.1 Have objectives of the system been identified, i.e. has the business case been presented?
- 8.1.2 Is there any indication that the service delivered does not serve the need of users? For example: frequent complaints by users.
- 8.1.3 Have any user problems or issues arisen over the last three years?
- 8.1.4 What are the arrangements to meet the information needs of users?
- 8.1.5 Is the design of the system coherent with the needs of the relevant economy/economies in terms of quality (time of execution, types of services, reliability and security, price, etc.) according to an end-to-end approach?

8.2 The needs of all types of users are considered in the design of the system and its evolution (e.g. by way of cooperation, consultation and coordination of plans).

- 8.2.1 Is there a procedure to regularly monitor and take stock of the needs of all types of current and potential users?
- 8.2.2 Are services tailored to the specific needs of different user profiles? Does the system recognise the difference in user/participant requirements and provide for these differences?
- 8.2.3 Does the system take due account of the evolving structure of the euro area market and conventions?

8.3 Resources are allocated efficiently.

- 8.3.1 Is there a procedure to record and analyse operational performances?
- 8.3.2 Does the system have technical or operational problems? Can it cope with the level of demand?
- 8.3.3 Does it persistently have high excess capacity?
- 8.3.4 Does it have long or variable processing times or high levels of returned payments?
- 8.3.5 Are payments held in queues because the participants do not have adequate access to intraday liquidity to allow payments to be settled promptly?
- 8.3.6 Is the queuing mechanism flexible to avoid that participants have to hold very high levels of intraday liquidity?
- 8.3.7 Are there any constraints (e.g. technology, infrastructure, organisation and resources) which affect the efficiency of the system?
- 8.3.8 Does system provide the participants with adequate incentives to pay promptly?
- 8.3.9 Describe any policies, mechanisms or analyses aimed at enhancing or ensuring system efficiency on a continuous basis.
- 8.3.10 Are there indications that improved safety measures in the system increase the cost or the complexity of use of the system, giving the participants in the system incentives or even leading the participants to settle relevant payments in alternative, perhaps less secure systems?
- 8.3.11 Does the system owner/operator make use of market disciplines (e.g. applying the principles of an open market economy with free competition) where possible and appropriate to increase the

efficiency of the system? In this context, has the system owner/operator issued requests for proposals and/or made the decision on the provision of services (e.g. telecommunication services) subject to the outcome of public tender procedures?

- 8.3.12 Is a cost methodology used?
- 8.3.13 Which costs are taken into account? Do the relevant costs include the total resources used by the system and its users in providing the payment services, taking also into account any indirect costs to users, such as the processing costs of the central system, the processing costs of the system's participants, and the opportunity costs of participants of holding liquidity and collateral? Does the system take into account the current and prospective costs of inputs, such as labour (including skilled labour) and technology? Are the costs of providing payment services signalled as clearly as possible to participants?
- 8.3.14 Based on the methodology used, how cost-efficient is the system? Are the costs high, possibly reflected in charges, compared to systems with similar services elsewhere? Are the costs for the setting-up or the operation of the system excessively high when a participant joins or leaves the system?
- 8.3.15 Has a formal (or informal) cost/benefit analysis been conducted or are there plans for the one to be conducted? If yes, provide details.
- 8.3.16 What is the basis for the prices charged to users?
- 8.3.17 Is there any sort of subsidising or cross-subsidising with other systems? If yes, are all participants aware of these subsidies?
- 8.3.18 Has the owner/operator of the system disclosed the rationale for its pricing policy?
- 8.3.19 Does the system apply message standards that are compatible with other systems that are relevant to participants?
- 8.3.20 Has the system been benchmarked against systems operating in comparable economies?

8.4 The pricing policy (cost recovery method, market based pricing, subsidised pricing) is communicated clearly to participants.

- 8.4.1 Is there a formal pricing policy? What are the market elements taken into consideration when defining it?
- 8.4.2 Is the basis for pricing and related policies available to users and the public?

- 8.4.3 Are the participants involved in the formulation of the pricing policy and/or in the determination of prices?

9. Core Principle IX

The system should have objective and publicly disclosed criteria for participation, which permit fair and open access.

Key issues

1. Criteria for access/exit are clearly and explicitly stated and disclosed publicly.
2. Procedures for access/exit are clearly specified in the rules and disclosed to participants and applicants.
3. Criteria of access/exit are objective, based on appropriate risk and efficiency considerations, and do not unduly restrict competition amongst participants.
4. Criteria fulfilment is monitored on a regular basis.

Key questions

9.1 Criteria for access/exit are clearly and explicitly stated and disclosed publicly.

- 9.1.1 What are the access/exit criteria for the system? Do exit criteria cover both suspension/exclusion/orderly withdrawal of a participant and voluntary exit of a participant?
- 9.1.2 Where are access/exit criteria laid down, and are they disclosed?
- 9.1.3 What is the participant structure (banks, non-financial institutions, others (please, specify))?
- 9.1.4 If the system allows for forms of participation other than direct participation, to what extent is this type of access actually used?

9.2 Procedures for access/exit are clearly specified in the rules and disclosed to participants and applicants.

- 9.2.1 Are there specific access and exit procedures? If so, where are they laid down and are they disclosed? Who (e.g. management, board of directors) applies them?

9.3 Criteria of access/exit are objective, based on appropriate risk and efficiency considerations, and do not unduly restrict competition amongst participants.

9.3.1 In case there is a differentiation made in access/exit criteria for different types of participants, how do these relate to the differences in risk profiles and/or on the basis of what efficiency considerations have they been defined and justified? Are they based on risk measures such as capital ratios, risk ratings or other indicators? Do they include factors such as minimum payment volumes? Is access possible on restricted terms (e.g. no access to intraday credit)?

9.3.2 What is the fee structure for participation in the system, and how does it affect the access of participants, especially for those who send/receive limited volumes?

9.4 Criteria fulfilment is monitored on a regular basis.

9.4.1 Who monitors the continued fulfilment of access criteria by existing participants and at what frequency?

9.4.2 If access criteria are related to risk indicators (e.g. ratings), to what extent do the criteria allow the risk indicators to fall below the level required to permit initial access?

10. Core Principle X

The system's governance arrangements should be effective, accountable and transparent.

Key issues

1. Governance arrangements are clearly specified.
2. Governance arrangements are transparent.
3. Management of the system operator is fully accountable for its performance vis-à-vis the system owner and the wider financial community, and lines of responsibility are clearly specified.
4. Major decisions are taken after consultation with at least all relevant stakeholders.
5. Objectives and major decisions are disclosed by the owners to operators, users, overseers, and any other relevant stakeholders.
6. Governance is effective in that management has incentives, appropriate tools and skills needed to achieve stated objectives for the system, its participants and the public more generally.

Key questions

10.1 Governance arrangements are clearly specified.

- 10.1.1 Are the ownership of the system, the decision-making procedures (hierarchical set-up, entities involved in decision-making), the operational functions, and the control functions (audit, oversight) clear and documented (please describe)?
- 10.1.2 Is there a specific dispute resolution procedure to be used by participants for disputes related to the implementation of procedures or other issues? If not, how are disputes handled? If yes, has it been used already?
- 10.1.3 Is there a specific dispute resolution procedure to be used by non-participants (e.g. applicants, former participants) for disputes related to the access/exit criteria? If not, how are disputes handled? If yes, has it been used already?
- 10.1.4 Is there a dispute resolution procedure in place for potential disputes of the owner and the operator of the system?

10.2 Governance arrangements are transparent.

- 10.2.1 Is relevant information on the system and its operations (e.g. reports on the system) complete and up to date and readily available to participants?
- 10.2.2 Are the ownership, board and management structure of the system, the process via which board members are appointed, the basic organisational structure, the general principles of risk management and the internal control system, and the basic decision-making procedures made transparent to the public in an easily understandable way (via a website, brochures, letters, information on demand)?
- 10.2.3 In the case of central bank-owned or jointly-owned systems, have the owner and/or operator function and the regulatory function been clearly separated?
- 10.2.4 In the case of privately-owned systems, have clear and transparent policies been adopted to avoid conflicts of interests of directors who are employed by participants and, for example, who may represent organisations that compete with each other?

10.3 Management of the system operator is fully accountable for its performance vis-à-vis the system owner and the wider financial community, and lines of responsibility are clearly specified.

- 10.3.1 How is it ensured that management is held accountable for performance of the system (e.g. is the work of the management subject to audit, oversight, or reviews by the board)? Towards which entity does the system manager/operator have to justify/explain the performance of the system, the compliance with the internal rules and with the external regulatory framework, major decisions and actions, and the adequacy of new developments (e.g. reports to the board of the institution or/and to shareholders)?
- 10.3.2 Are their clear lines of responsibility and accountability within the organisation? How is the effectiveness and enforceability of controls on management ensured (independence of audit, of oversight – for systems managed by central banks – adequacy of reporting, existence of “non-executive independent” members of the board)? Do reporting arrangements exist that assess the actions of senior management against the strategic objectives?
- 10.3.3 Are there arrangements to ensure the accountability of the performance of the system when the information processing has been outsourced?
- 10.3.4 Are risk management and audit functions in place that are independent of those responsible for the day-to-day operations and that concern themselves with, for example, legal, financial, operational security risks?

10.4 Major decisions are taken after consultation with at least all relevant stakeholders.

- 10.4.1 How are the users and other interested parties (e.g. audit, oversight) associated? For what type of issues do consultations take place?
- 10.4.2 What type of consultation arrangement exists? For example, do formal or informal consultation arrangements exist?
- 10.4.3 If meetings are arranged, do they take place multilaterally or bilaterally and how often do they take place?
- 10.4.4 Is the range of users consulted sufficiently wide to ensure that all users are fairly represented? Do discussions with user groups take place?
- 10.4.5 Do the majority of users usually accept decisions which are agreed by the user representatives?

10.5 Objectives and major decisions are disclosed by the owners to operators, users, overseers, and any other relevant stakeholders.

- 10.5.1 Do written strategic objectives and plans to achieve them exist?
- 10.5.2 Are the objectives and major decisions regarding the system timely communicated (e.g. through reports, statistical analysis, etc.) to users, owners, operators, overseers, and any risk management and audit functions that are independent of those responsible for the day-to-day operations?
- 10.5.3 Are the objectives and major decisions regarding the system released through appropriate channels depending on the concerned stakeholder (users, owners, overseers)?

10.6 Governance is effective in that management has incentives, appropriate tools and skills needed to achieve stated objectives for the system, its participants and the public more generally.

- 10.6.1 Do business plans exist? Are projected financial results attained? For example, is there a check by controlling or audit?

- 10.6.2 What mechanisms are used to ensure that management has the incentives, tools and skills necessary to realise the system's objectives and to act in the interest of stakeholders? Are there requirements that management at all levels is appropriately qualified and supervises the system and its operations competently?
- 10.6.3 Does the system comply – at least broadly – with the other relevant Core Principles? If not, have plans been developed by the system owner/operator to address issues/problems identified within a reasonable time frame?
- 10.6.4 Are the governance arrangements (as described in responses to key questions 10.1, 10.3, 10.4 and 10.5) subject to an audit process for ensuring that they are properly and effectively applied? Is an independent auditor entitled to perform that audit?