EUROPEAN CENTRAL BANK

EUROSYSTEM

Eurosystem assessment methodology for electronic payment instruments, schemes and arrangements

Draft for public consultation

October 2020

Contents

1 General Introduction 3

2 Use of this assessment methodology 4

2.1 Identifying applicable principles and key considerations 4

2.2 Scope of the individual assessments 5

2.3 Self-assessment by the governance body 5

2.4 Oversight report 6

2.5 Observance levels for each principle 7

2.6 Follow-up actions, recommendations and timeframe for addressing each issue of concern 8

3 Other oversight requirements for payment schemes/arrangements 10

3.1 Information about major changes 10

3.2 Major incident reporting 10

3.3 Statistical information 11

4 Applicable principles, key considerations and the resulting assessment questions 12

Principle 1: legal basis 14

Principle 2: governance 16

Principle 3: framework for the comprehensive management of risks 21

Principle 4: credit risk 24

Principle 5: collateral 25

Principle 6: not applicable to a payment scheme/arrangement 26

Principle 7: liquidity risk 26

Principle 8: settlement finality and crediting end users 28

Principle 9: money settlement 29

Principle 10-12: not applicable to a payment scheme/arrangement 31

Principle 13: payment service provider default rules and procedures 31

Principle 14: not applicable to a payment scheme/arrangement 32

Principle 15: general business risk 32

Principle 16: custody and investment risk 33

Principle 17: operational risk 34

Principle 18: access and participation requirements 41

Principle 19: not applicable to a payment scheme/arrangement 44

Principle 20: not applicable to a payment scheme/arrangement 44

Principle 21: efficiency and effectiveness 44

Principle 22: communication procedures and standards 45

Principle 23: disclosure of rules, key procedures and market data 47

Principle 24: not applicable to a payment scheme/arrangement 49

Annex 1: Comparison of PISA with other oversight assessment methodologies 50

1 General Introduction

This assessment methodology complements the "Eurosystem's oversight framework for electronic payment instruments, schemes and arrangements" (the PISA framework) and should be read jointly with the latter. To ensure consistency with the Eurosystem's oversight of payment systems, the CPMI-IOSCO general instructions and practices for conducting an assessment against the principles for financial market infrastructures (PFMI) are also observed for payment scheme/arrangement assessments.[1]

The Eurosystem's oversight requirements for electronic payment instruments, schemes and arrangements are set out in the form of principles included in the PISA framework. This assessment methodology is aimed at ensuring the consistent and harmonised application of these principles by specifying key considerations and assessment questions. The answers provided by the governance body of the respective payment scheme/arrangement to the questions serve as key input for the actual oversight assessment.

The underlying methodology is based on the "Revised assessment methodology for payment systems"[2]. In view of the different scope of the PISA framework, some key considerations and assessment questions were adjusted and streamlined as appropriate, complemented by relevant content from the previous assessment guides for payment schemes and enriched by new requirements which take market developments into account. The PISA assessment methodology thus combines and replaces the guidance that was previously provided in dedicated documents for each payment instrument.[3]

---

1 These instructions and practices are also valid for all assessments of payment systems conducted by the Eurosystem, regardless of the classification of the payment system. Further guidance on definition of scope, fact finding, the structure of the assessment report etc. is contained in "Principles for financial market infrastructures: Disclosure framework and Assessment methodology", Committee on Payment and Settlement Systems (CPMI) and Board of the International Organization of Securities Commissions, (IOSCO) December 2012.

2 See "Revised assessment methodology for payment systems", ECB, June 2018.

3 See "Guide for the assessment of card payment schemes against the oversight standards", ECB, February 2015.

See "Guide for the assessment of credit transfer schemes against the oversight standards", ECB, November 2014.

See "Guide for the assessment of direct debit schemes against the oversight standards", ECB, November 2014.

See "Electronic money system security objectives", ECB, May 2003.

2 Use of this assessment methodology

The PISA framework defines payment scheme functions as well as payment arrangement functions/functionalities. Based on this information, an overseer should determine which functions of a payment scheme, which functions/functionalities of a payment arrangement and which payment instruments fall within the scope of the assessment. The overseer then informs the respective governance body, which may be a legal entity, a part of a legal entity, or several legal entities.

2.1 Identifying applicable principles and key considerations

The assessment methodology provides guidance as to which of the principles and key considerations are applicable. This is indicated by tick boxes as illustrated in Table 1 below. The assessment questions are listed in Section 3 and are organised by key considerations for each of the assessment methodology principles.

When answering the questions, the payment scheme/arrangement should consider, first, whether the respective function/functionality is provided and, if so, whether it applies to the payment instruments used in the scheme. Only if both conditions are fulfilled is the assessment question applicable and only then it should answer for the functions, functionalities and payment instruments concerned.

Table 1

Overview of payment scheme functions, payment arrangement functions/ functionalities and payment instruments

Payment scheme functions	Payment arrangement functions/functionalities	Payment instruments
☒ Governance of a payment scheme ☒ Service provision ☒ Payment guarantee ☒ Processing ☒ Clearing ☒ Settlement	☒ Governance of a payment arrangement ☒ Initiation, facilitation and requests to execute transfers of value ☒ Storage or registering of personalised security credentials ☒ Storage of payment instrument-related data	☒ Payment card ☒ Credit transfer ☒ Direct debit ☒ E-money ☒ Digital payment token ☒ Cash[4]

The assessment methodology also uses footnotes to indicate whether specific key considerations or assessment questions might fall within the remit of other authorities.[5]

As mentioned in the framework, risks that are already overseen in the context of the Eurosystem's oversight of payment systems will not be assessed again against the PISA framework, provided that all relevant aspects of the payment scheme/arrangement have been considered in the context of payment systems

4 Only as a provision of cash/cash placement.

5 These references are not exhaustive as they take into account the status quo at the point of publication.

oversight.[6]Information on the supervisory assessments of payment service providers conducted by the competent authorities will feed into the oversight assessment to the extent that they cover the same requirements set out in the PISA framework.

For instance, if the service provision function (and, possibly, the payment guarantee function) is provided by effectively supervised entities (whether these be the governance body itself or service providers), the lead overseer should consider the results of assessments against the respective regulatory and supervisory frameworks, to the extent relevant.

The lead overseer, in such cases, will consider how best to coordinate with the respective authorities or will ask the governance body to provide the results of a relevant supervisory review.

2.2 Scope of the individual assessments

An assessment exercise, following the requirements of this methodology, typically starts with a kick-off meeting[7] involving the governance body, the lead overseer and, where applicable, other members of the Assessment Group (AG)[8]. The objective is to explain the scope of the assessment, the general approach and the timeline.

The lead overseer informs the governance body whether the assessment will be conducted (a) against all the principles relevant for the type of payment scheme/arrangement (e.g. as a part of a periodic comprehensive review of a payment scheme/arrangement's safety and efficiency) or (b) against one or more individual principles (e.g. in the event of a major change such as the introduction of a new service or as a part of a thematic review across one or more payment schemes/arrangements).[9]

The lead overseers/AG could, at their discretion, pose additional or different assessment questions, or modify these as required, to address the different levels of complexity, the specific design of the payment scheme/arrangement, particular risk factors or other specific circumstances.

2.3 Self-assessment by the governance body

Based on the applicable assessment questions and key considerations, a preliminary self-assessment is submitted by the governance body, together with the relevant

---

6 Annex 1 provides an overview of which expectations of the PISA assessment methodology are also covered by other assessment methodologies used by the Eurosystem for the oversight of payment systems.

7 Physical or virtual.

8 To be established for pan-European schemes or arrangements. Here oversight is conducted under a cooperative oversight arrangement with interested central banks, coordinated by the lead overseer. The lead overseer and interested central banks form the assessment group.

9 See Section 2.2.1.

documentation. The self-assessment should answer each question or outline why a question is not applicable, providing sufficient justification and evidence.

The answers to the questions should consider all the functions of a payment scheme, the functions/functionalities of a payment arrangement and each payment instrument the governing body is responsible for. If the same question is relevant for multiple functions/functionalities/instruments, the answers should clearly indicate how they relate to each of the functions/functionalities/instruments in question.

The assessment questions should not be considered to be prescriptive in terms of solutions, and different solutions may provide an acceptable level of resilience. If the oversight expectation is not followed in the way suggested in the assessment question, the governance body should explain how they mitigate the underlying risk.

2.4 Oversight report

The self-assessment is evaluated by the lead overseer, together with the AG where applicable. The self-assessment based on the questions is a tool which helps the overseer to gather facts to determine whether a payment scheme/arrangement is observing the principles. The self-assessment is not intended to be a checklist – it should inform and guide the judgement of the overseer, not replace it. The lead overseer may ask the governance body additional questions or request further documentation and clarification.

Based on the facts gathered, the lead overseer/AG formulates key conclusions for each principle included in the assessment. The overseer's assessment will be forward-looking and based on sound judgement.

The assessment outcome, recommendations and action plans are presented in an oversight report after the assessment has been completed. The report is shared with the payment scheme/arrangement's governance body for the review and correction of factual mistakes before finalisation by the lead overseer/AG. Additional information provided by the governance body of the payment scheme/arrangement after the cut-off date of the assessment could be accepted by the overseer, but will only be taken into consideration during follow-up on the recommendations of the assessment. Once it has been approved by the overseer's decision-making bodies, the final assessment report will be shared with the payment scheme/arrangement's governance body, which will be asked to develop a plan for addressing any recommendations.

A non-confidential summary of the assessment report and/or its main findings might, at the discretion of the lead overseer, be published, depending on the extent to which this serves the public interest.

When drawing key conclusions for the oversight report, the lead overseer/AG will take the steps below.

1. Summarise the payment scheme/arrangement's practices and achievements, as appropriate.

2. Identify any gaps or shortcomings as they emerge from the facts gathered by the lead overseer/AG.

3. For each gap or shortcoming, describe the essential associated risks or other issues and the implications of observing the principle.

4. For each gap or shortcoming, determine whether it is an issue of concern based on the associated risks, practices and achievements. Issues of concern could include a risk management flaw, a deficiency, or a lack of transparency or effectiveness that needs to be addressed. The lead overseer/AG will distinguish between major and minor issues of concern. Major issues are serious and warrant immediate attention, as they could become critical if not addressed promptly. Minor issues should be addressed in a defined timeframe.

Key conclusions serve as building blocks for rating the level of observance for each principle.

2.5 Observance levels for each principle

In order to assign a rating to each principle, the following observance levels are used[10]:

- **Observed.** The payment scheme/arrangement observes the principle. Any identified gaps or shortcomings are not issues of concern and are minor, manageable and of such a nature that the governance body of the payment scheme/arrangement could consider addressing them in the normal course of its business.

- **Broadly observed.** The payment scheme/arrangement broadly observes the principle. The assessment has identified one or more issues of concern that the governance body of the payment scheme/arrangement should address and follow up on, according to a timeline agreed with the lead overseer/AG.

- **Partly observed.** The payment scheme/arrangement partly observes the principle. The assessment has identified one or more issues of concern that could become serious if not addressed promptly. The governance body of the payment scheme/arrangement should accord a high priority to addressing these issues.

- **Not observed.** The payment scheme/arrangement does not observe the principle. The assessment has identified one or more serious issues of concern that warrant immediate action. The governance body of the payment scheme/arrangement should, therefore, accord the highest priority to addressing these issues.

[10] Aligned with the ratings used for non-systemically important payment systems.

Guidance on the assignment of ratings

The rating assigned reflects the conditions at the moment of assessment and is built on the key conclusions. It reflects the lead overseer/AG's judgement regarding the type or impact of the risks and other issues associated with each identified gap or shortcoming. Planned improvements should be noted in the assessment report, where appropriate, but should not influence the lead overseer/AG's judgement with regard to observance of the principles.

The assessment should note situations in which the observance of a particular principle could not be adequately assessed and should give reasons for this. For example, certain information may not have been provided, or key individuals or institutions may have been unavailable to discuss important issues. Unsatisfied requests for information or meetings should be documented in writing. In such cases, the lead overseer/AG may treat such information gaps as evidence of a concern.

When rating the observance of a principle, lead overseer/AG should consider the following points. For a principle to be observed, any identified gaps or shortcomings should not be issues of concern, meaning that they should be manageable and of such a nature that the governance body of the payment scheme/arrangement could consider addressing them in the normal course of business. When a principle is not observed, the lead overseer/AG should decide on the degree of non-observance. Ratings should take into account not only the number of issues identified but also the level of concern they present. It is important to note that there may be multiple issues presenting differing degrees of concern. In such cases the overseer should, typically, assign to the principle a rating which reflects the overseer's judgement of the severity of the most serious concerns identified (in line with the rating guidelines outlined above).

The lead overseer/AG should, however, ensure that the rating appropriately reflects the circumstances. For example, in some cases the combination of a number of smaller gaps or shortcomings may be an issue of concern. Conversely, where one issue of concern is relevant for more than one principle or key consideration, it should only negatively affect the rating of the most relevant principle/key consideration, rather than all of them.

2.6 Follow-up actions, recommendations and timeframe for addressing each issue of concern

An oversight report should conclude with a clear identification of the issues of concern that need to be addressed, if any. Recommendations for a principle that has not been rated as "observed", or for other noted shortcomings, should address any identified issues of concern – they should serve to improve the payment scheme/arrangement's level of observance of the principle.

The lead overseer/AG should identify the areas in which less than full observance of principles may lead to serious concerns. The lead overseer/AG will identify and

prioritise deficiencies that pose the greatest risks or greatest lack of transparency or lack of effectiveness to the payment scheme/arrangement.

Having identified priority areas, the lead overseer/AG should then suggest the actions needed in each area. The governance body of the payment scheme/arrangement itself is expected to prepare, based on the issues of concern, an action plan for review by the lead overseer/AG. A reasonable timeframe in which an issue of concern should be addressed should also be agreed with the governance body. The lead overseer/AG will monitor the follow-up to the action plan.

Where appropriate, the lead overseer/AG should also provide recommendations that serve to rectify any gaps or shortcomings that are not issues of concern. There is no requirement or specified timeline for implementing these recommendations, and the governance body of the payment scheme/arrangement could consider taking them up in the normal course of its business.

3 Other oversight requirements for payment schemes/arrangements

3.1 Information about major changes

The governance body should inform the lead overseer in good time of any planned major changes to the payment scheme/arrangement. A major change typically represents a change of the design or the functioning of the payment scheme/arrangement, which either significantly alters the setup of the rules or introduces major new business features. Major changes may have a significant impact on the payment schemes/arrangement's risk profile and may have the potential to materially affect the level of observance in relation to the oversight principles if not properly managed. The governance body should submit relevant documentation about the major change to the lead overseer as soon as it is available.

The lead overseer/AG will assess the significance of the change and will confirm that it is a major change and that an assessment is required. Furthermore, the lead overseer/AG will evaluate which principles may be affected by the change and communicate this information to the governance body.

If a change is classified as major by the overseer the governance body will prepare a self-assessment of the change against the principles affected. The overseer will review the self-assessment, taking into consideration the impact on the payment scheme/arrangement, and will provide feedback to the governance body on the implementation of the change. If a need is identified to downgrade the observance level for an oversight principle, the overseer should alert the governance body so that the respective plans can, ideally, be amended before implementation.

3.2 Major incident reporting

Major incidents (as defined in the Eurosystem's oversight framework for major incident reporting for retail payment systems, schemes and arrangements communicated separately to payment scheme/arrangements' governance bodies) should be reported to the lead overseer immediately and additional information should be provided within the timeframe prescribed in the above document. An incident should be classified as "major" if it has caused significant business disruption or interrupted the smooth functioning of the scheme or arrangement, or one of its functions. For example, any major network failure, or a major fraud incident involving the data of a scheme or arrangement, should be reported.

For further details, please refer to the guidance provided separately to the overseen schemes and arrangements by their lead overseer.

3.3 Statistical information

A payment scheme/arrangement's governance body should report to its lead overseer the statistical information required to calculate the thresholds defined in the "Exemption policy of the Eurosystem oversight framework for payment instruments, schemes and arrangements". The overseer may request additional regular or ad hoc statistical reporting in order to monitor developments or particular risks for a payment scheme or arrangement.

4 Applicable principles, key considerations and the resulting assessment questions

Table 2

Overview – adjusted principles of the framework and the key considerations applicable to functions/functionalities/payment instruments

	Payment scheme functions						Payment arrangement functions/functionalities				Payment instrument					
	Governance	Service provisions	Payment guarantees	Processing	Clearing	Settlements	Governance	Initiation, facilitation and requests to execute transfers of value	Storage or registering of personalised security credentials	Storage of payment instrument-related data	Payment cards	Credit transfers	Direct debits	E-money	Digital payment tokens	Cash
Principle 1	**Legal risk**															
KC 1 -5	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
Principle 2	**Governance risk**															
KC 1 -7	☑	☒	☒	☒	☒	☒	☑	☒	☒	☒	☑	☑	☑	☑	☑	☑
Principle 3	**Comprehensive risk management**															
KC 1 - 4	☑	☒	☒	☒	☒	☒	☑	☒	☒	☒	☑	☑	☑	☑	☑	☑
Principle 4	**Credit risk**															
KC 1-2	☒	☒	☑	☒	☑	☑	☒	☒	☒	☒	☑	☑	☑	☑	☑	☑
Principle 5	**Collateral risk**															
KC 1	☒	☒	☑	☒	☑	☑	☒	☒	☒	☒	☑	☑	☑	☑	☑	☑
Principle 7	**Liquidity risk**															
KC 1-3	☒	☒	☑	☒	☑	☑	☒	☒	☒	☒	☑	☑	☑	☑	☑	☑
Principle 8	**Settlement finality and crediting of end user**															
KC 1	☒	☑	☑	☒	☑	☑	☒	☒	☒	☒	☑	☑	☑	☑	☑	☑
Principle 9	**Money settlement risk**															
KC 3- 5	☒☑	☑	☑	☒	☑	☑	☒	☒	☒	☒	☑	☑	☑	☑	☑	☑
Principle 13	**Service provider default**															
KC 1	☑	☑	☑	☒	☑	☑	☒	☒	☒	☒	☑	☑	☑	☑	☑	☑

	Payment scheme functions						Payment arrangement functions/functionalities				Payment instrument					
	Governance	Service provisions	Payment guarantees	Processing	Clearing	Settlements	Governance	Initiation, facilitation and requests to execute transfers of value	Storage or registering of personalised security credentials	Storage of payment instrument-related data	Payment cards	Credit transfers	Direct debits	E-money	Digital payment tokens	Cash
KC 2	☑	☒	☒	☒	☑	☑	☒	☒	☒	☒	☑	☑	☑	☑	☑	☑
Principle 15	**General business risk**															
KC 1	☑	☒	☒	☒	☒	☒	☑	☒	☒	☒	☑	☑	☑	☑	☑	☑
Principle 16	**Custody and investment risk**															
KC 1 -2	☑	☑	☑	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☑	☑	☒
Principle 17	**Operational risk**															
KC 1	☑	☑	☒	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
KC 2	☑	☒	☒	☒	☒	☒	☑	☒	☒	☒	☑	☑	☑	☑	☑	☑
KC 3, 3a	☑	☒	☒	☒	☒	☒	☑	☒	☒	☒	☑	☑	☑	☑	☑	☑
KC 4, 5,7,7a, 8	☑	☑	☒	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
Principle 18	**Access and participation**															
KC 1 - 3	☑	☒	☒	☒	☒	☒	☑	☒	☒	☒	☑	☑	☑	☑	☑	☑
Principle 21	**Efficiency and effectiveness**															
KC 1 -3	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
Principle 22	**Communication**															
KC 1	☑	☑	☒	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
Principle 23	**Disclosure**															
KC 1-3, 5	☑	☑	☑	☒	☒	☒	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
Total principles	**11**	**9**	**10**	**4**	**10**	**10**	**9**	**5**	**5**	**5**	**15**	**15**	**15**	**16**	**16**	**15**

Principle 1: legal basis

A payment scheme/arrangement should have a well-founded, clear, transparent and enforceable legal basis for each material aspect of its activities in all relevant jurisdictions

Payment scheme functions	Payment arrangement functions/functionalities	Payment instruments
☒ Governance of a payment scheme ☒ Service provision ☒ Payment guarantee ☒ Processing ☒ Clearing ☒ Settlement	☒ Governance of a payment arrangement ☒ Initiation, facilitation and requests to execute transfers of value ☒ Storage or registering of personalised security credentials ☒ Storage of payment instrument-related data	☒ Payment card ☒ Credit transfer ☒ Direct debit ☒ E-money ☒ Digital payment token ☒ Cash[11]

Key consideration 1. The legal basis should provide a high degree of certainty for each material aspect of the payment scheme/arrangement's activities in all relevant jurisdictions

Material aspects and relevant jurisdictions

Q.1.1.1. What are the material aspects of the payment scheme/arrangement's activities that require a high degree of legal certainty (for example, the establishment and functioning of a payment scheme/arrangement; the relationship between the different payment scheme/arrangement actors, and the rights and interests of payment service providers/technical service providers/end users; the finality of transfers of value; netting; interoperability; collateral arrangements, suspension and default procedures)?

Q.1.1.2. What are the relevant jurisdictions for each material aspect of the payment scheme/arrangement's activities?

Q 1.1.3. What are the jurisdiction and legal framework governing the establishment and activities of the governance body itself and all the other relevant functions/functionalities of the respective payment scheme/arrangement?

Legal basis for each material aspect

Q.1.1.4. How does the governance body ensure that the legal basis (i.e. the legal framework and the payment scheme/arrangement's rules, procedures and contracts) provides a high degree of legal certainty for each material aspect of the payment scheme/arrangement's activities in all relevant jurisdictions?

[11] Only as a provision of cash/cash placement.

Key consideration 2. A payment scheme/arrangement should have rules, procedures and contracts that are clear, easily understandable, and consistent with the relevant laws and regulations

Q.1.2.1. How has the governance body demonstrated that the payment scheme/arrangement's rules, procedures and contracts are clear and easily understandable?

Q.1.2.2. How does the governance body ensure that the payment scheme/arrangement's rules, procedures and contracts are consistent with the relevant laws and regulations (e.g. through legal opinions or analyses)? Have any inconsistencies been identified and remedied? Are the payment scheme/arrangement's rules, procedures and contracts reviewed or assessed by external authorities or entities?

Q.1.2.3. Do the payment scheme/arrangement's rules, procedures and contracts have to be approved before coming into effect? Are they reviewed periodically or on an event-driven basis? If so, by whom and how?

Key consideration 3. The governance body should be able to articulate the legal basis for the payment scheme/arrangement's activities to the relevant authorities, payment service providers, technical service providers and, where relevant, end users, in a way that is clear and easily understandable

Q.1.3.1. How does the governance body articulate the legal basis for the payment scheme/arrangement's activities to the relevant authorities, payment service providers, technical service providers and end users?

Key consideration 4. A payment scheme/arrangement should have rules, procedures and contracts that are enforceable in all relevant jurisdictions. There should be a high degree of certainty that actions taken by the governance body under such rules and procedures will not be voided, reversed or subject to stays

Enforceability of rules, procedures and contracts

Q.1.4.1. How does the governance body achieve a high level of confidence that the payment scheme/arrangement's rules, procedures and contracts are enforceable in all the relevant jurisdictions identified in Key consideration 1 (for example, through legal opinions and analyses)?

Degree of certainty for rules and procedures

Q.1.4.2. How does the governance body achieve a high degree of certainty that the payment scheme/arrangement's rules, procedures and contracts will not be voided, reversed or subject to stays? Are there any circumstances under which a governance body's actions under the payment scheme/arrangement's rules, procedures or contracts could be voided, reversed or subject to stays? If so, what are those circumstances?

Q.1.4.3. Has a court in any relevant jurisdiction ever held any of the payment scheme/arrangement's relevant activities under its rules and procedures to be unenforceable?

Key consideration 5. A payment scheme/arrangement doing business in multiple jurisdictions should identify and mitigate the risks arising from any potential conflict of laws across jurisdictions

Q.1.5.1. If the payment scheme/arrangement is offered to payment service providers and/or end users in multiple jurisdictions, how does the governance body identify and analyse any potential conflict-of-laws issues? What potential conflict-of-law issues have been identified and analysed by the governance body? How has the governance body addressed any potential conflict-of-law issues?

Principle 2: governance

A payment scheme/arrangement should have governance that is clear and transparent, promotes the safety and efficiency of the payment scheme/arrangement, and supports the objectives of relevant stakeholders

Payment scheme functions	Payment arrangement functions /functionalities	Payment instrument
☒ Governance of a payment scheme ☐ Service provision ☐ Payment guarantee ☐ Processing ☐ Clearing ☐ Settlement	☒ Governance of a payment arrangement ☐ Initiation, facilitation and requests to execute transfers of value ☐ Storage or registering of personalised security credentials ☐ Storage of payment instrument-related data	☒ Payment card ☒ Credit transfer ☒ Direct debit ☒ E-money ☒ Digital payment token ☒ Cash[12]

[12] Only as a provision of cash/cash placement.

Key consideration 1. A governance body should have objectives which place a high priority on the safety and efficiency of the payment scheme/arrangement

Q.2.1.1. What are the payment scheme/arrangement's objectives, and have they been clearly identified? How does the governance body assess the payment scheme/arrangement's performance in meeting its objectives?

Q.2.1.2. In what way do the payment scheme/arrangement's objectives place a high priority on safety and efficiency?

Key consideration 2. A payment scheme/arrangement should have governance documentation which provides clear and direct lines of responsibility and accountability. This documentation should be disclosed to owners, the relevant authorities, payment service providers and (as appropriate) to other stakeholders

Governance

Q.2.2.1. How is the ownership and decision-making process of the payment scheme/arrangement organised? What are the lines of responsibility and accountability within the governance body? How and where is the governance function documented?

Q.2.2.2. How does the governance body monitor the compliance of payment service providers and technical service providers with the full range of formal, standardised and common rules?

Disclosure of governance documentation

Q.2.2.3. How is the governance documentation disclosed to owners, the relevant authorities, payment service providers, technical service providers and other stakeholders?

Q.2.2.4. Are the objectives and major decisions regarding the payment scheme/arrangement communicated in a timely manner (e.g. through reports, statistical analysis, etc.) to payment service providers, technical service providers, owners, operators, overseers, as well as to any risk management and audit functions?

Q.2.2.5. Are the objectives and major decisions regarding the payment scheme/arrangement released through the appropriate channels, depending on the stakeholder concerned (payment service providers, technical service providers, owners and overseers)?

Key consideration 3. The roles and responsibilities in the payment scheme/arrangement's decision-making process should be clearly specified. There should be documented procedures which explain how the process functions, including procedures for identifying, addressing and managing conflicts of interest

Q.2.3.1. What are the roles and responsibilities in the payment scheme/arrangement's decision-making process, and are they clearly specified? Is there a process in place to update these roles and responsibilities regularly and/or on an event-driven basis?

Q.2.3.2. What are the procedures involved in the payment scheme/arrangement's decision-making process (e.g. procedures to identify, address and manage conflicts of interest)? How are these procedures documented and to whom are they disclosed? How frequently are they reviewed?

Key consideration 4. The actors involved in the payment scheme/arrangement's decision-making process should have the skills and incentives required to perform their roles and fulfil their responsibilities

Q.2.4.1. To what extent do the actors involved in the payment scheme/arrangement's decision-making process have the skills and incentives required to perform their roles and fulfil their responsibilities? How does the governance body ensure that this is the case?

Key consideration 5. The roles and responsibilities of the management of the scheme/arrangement's governance body should be clearly specified. The management should have the required experience, mix of skills and integrity needed to discharge its responsibilities with regard to the operation and risk management of the scheme or arrangement

Roles and responsibilities of the management of the payment scheme/arrangement's governance body

Q.2.5.1. What are the roles and responsibilities of the governance body's management, and are these clearly specified?

Q.2.5.2. How are the roles and objectives of the governance body's management defined and evaluated?

Experience, skills and integrity

Q.2.5.3. To what extent does the governance body's management have the appropriate experience, mix of skills and integrity required with regard to the operation and risk management of the payment scheme/arrangement? How does the governance body ensure that this is the case?

Q.2.5.4. What is the process for removing a member of the governance body's management, should this become necessary?

Key consideration 6. The governance body should establish a clear, documented risk management framework which includes the payment scheme/arrangement's risk tolerance policy, assigns responsibility and accountability for risk decisions, and addresses decision-making during crises and emergencies. Governance provisions should ensure that the risk management and internal control functions have sufficient authority, independence, resources and access to the decision-making process of the governance body

Risk management framework

Q.2.6.1. What is the risk management framework that has been established by the governance body? How is it documented?

Q.2.6.2. How does this framework address the payment scheme/arrangement's risk tolerance policy, assign responsibility and accountability for risk decisions (such as limits on risk exposures), and address decision-making in crises and emergencies?

Q.2.6.3. What is the process for determining, endorsing and reviewing the risk management framework?

Authority and independence of the risk management and audit functions

Q.2.6.4. What roles, responsibilities, authority, reporting lines and resources do the risk management and audit functions have?

Q.2.6.5. How does the governance body ensure that there are adequate rules for the adoption and use of risk management models? How are these models and the related methodologies validated?

Q.2.6.6. Are the risk management and audit functions independent from day-to-day operations?

Effective internal control function

Q.2.6.7. How does the governance body ensure that the internal control framework is able to prevent and detect irregularities effectively?

Q.2.6.8. Does the governance body have sufficient powers to enable it to ask for audit reports from payment service providers and technical service providers on issues pertaining to the scheme/arrangement's security policies and measures, capacity monitoring and planning, business continuity, outsourcing and the independence of the control function.

Key consideration 7. The governance body should ensure that the payment scheme/arrangement's design, rules, overall strategy and major decisions appropriately reflect the legitimate interests of payment service providers, technical service providers and other relevant stakeholders. Major decisions should be clearly disclosed to the relevant stakeholders and, where there is broad market impact, the public

Identification and consideration of stakeholder interests

Q.2.7.1: How does the governance body identify and take into account the interests of the payment scheme/arrangement's payment service providers, technical service providers and other relevant stakeholders in its design, rules, overall strategy and major decisions?

Q.2.7.2: How does the governance body take into account the views of the payment scheme/arrangement's payment service providers, technical service providers and other relevant stakeholders in the above decisions? For example, are payment service providers and technical service providers involved in the risk management committee, in user committees or through public consultation? How are conflicts of interest between stakeholders and the governance body identified, and how are they addressed?

Q.2.7.3: Is there a specific dispute resolution procedure in place for payment scheme/arrangement service providers and/or end users for disputes related to the payment scheme/arrangement's rules or other issues? If not, how are disputes handled? If there is a procedure, has it been used already?

Q.2.7.4: Is there a specific dispute resolution procedure to be used by payment service providers and technical service providers that not adhere to the scheme/arrangement (e.g. applicants, former payment service providers and technical service providers) in respect of disputes related to access criteria/denial of access/termination of participation? If not, how are disputes handled? Is there an objective and risk-based procedure and, if so, has it been used already?

Q.2.7.5: What type of consultation arrangement exists? For example, are there any formal or informal consultation arrangements in place?

Q.2.7.6: Is a sufficiently wide range of payment service providers and technical service providers consulted to ensure that they are all fairly represented? Do discussions take place with groups of payment service providers and technical service providers? Are adequate processes in place to review performance, usability, convenience and payment service user satisfaction with the scheme or arrangement?

Disclosure

Q.2.7.7: To what extent does the payment scheme/arrangement disclose major decisions taken by the governance body to the relevant stakeholders and, where appropriate, the public?

Principle 3: framework for the comprehensive management of risks

A governance body should have a sound risk management framework for comprehensively managing a payment scheme/arrangement's legal, credit, liquidity, operational and other risks

Payment scheme functions	Payment arrangement functions/functionalities	Payment instrument
☒ Governance of a payment scheme ☐ Service provision ☐ Payment guarantee ☐ Processing ☐ Clearing ☐ Settlement	☒ Governance of a payment arrangement ☐ Initiation, facilitation and requests to execute transfers of value ☐ Storage or registering of personalised security credentials ☐ Storage of payment instrument-related data	☒ Payment card ☒ Credit transfer ☒ Direct debit ☒ E-money ☒ Digital payment token ☒ Cash[13]

Key consideration 1. A governance body should have in place the risk management policies, procedures and systems that will enable it to identify, measure, monitor and manage the range of risks that arise in or are borne by the payment scheme/arrangement. Risk management frameworks should be subject to periodic review

Risks that arise in or are borne by the payment scheme/arrangement

Q.3.1.1. What types of risk arise in or are borne by the payment scheme/arrangement?

[13] Only as a provision of cash/cash placement.

Risk management policies, procedures and systems

Q.3.1.2. What are the governance body's policies, procedures and controls that enable it to identify, measure, monitor and manage the risks that arise in or are borne by the payment scheme/arrangement?

Q.3.1.3. What risk management systems are used by the governance body to enable it to identify, measure, monitor and manage its range of risks?

Q.3.1.4. How do these systems provide the capacity to aggregate exposures across the payment scheme/arrangement and, where appropriate, other relevant parties, such as the payment scheme/arrangement's payment service providers, technical service providers and end users?

Review of risk management policies, procedures and systems

Q.3.1.5. What are the procedures for developing, approving and maintaining risk management policies, procedures and systems?

Q.3.1.6. How does the governance body assess the effectiveness of risk management policies, procedures and systems?

Q.3.1.7. How frequently are the risk management policies, procedures and systems reviewed and updated by the governance body? How do these reviews take into account fluctuations in risk intensity, changing environments and market practices?

Key consideration 2. A payment scheme/arrangement should provide incentives to payment service providers, technical service providers and, where relevant, end users to manage and contain the risks they pose to the payment scheme/arrangement

Q.3.2.1. What information does the payment scheme/arrangement provide to its payment service providers, technical service providers and, where relevant, end users to enable them to manage and contain the risks they pose to the payment scheme/arrangement?

Q.3.2.2. What incentives does the payment scheme/arrangement provide for payment service providers and technical service providers and, where relevant, end users to monitor and manage the risks they pose to the payment scheme/arrangement?

Q.3.2.3. How does the governance body design its policies and systems so that they are effective in allowing a payment scheme/arrangement's payment service providers, technical service providers and, where relevant, end users to manage and contain the risks they pose to the payment scheme/arrangement?

Key consideration 3. The governance body of a payment scheme/arrangement should regularly review the material risks it bears from and poses to other entities (such as other payment scheme/arrangements, clearing and settlement systems, and payment service providers) as a result of interdependencies, and it should develop appropriate risk management tools to address these risks

Material risks

Q.3.3.1. How does the governance body identify the material risks that it bears from and poses to other entities as a result of interdependencies? What material risks has the governance body identified?

Q.3.3.2: How are these risks measured and monitored? How frequently does the governance body review these risks?

Risk management tools

Q.3.3.3. What risk management tools are used by the governance body to address the risks arising from interdependencies with other entities?

Q.3.3.4. How does the governance body assess the effectiveness of these risk management tools? How does the governance body review the risk management tools it uses to address these risks? How frequently is this review conducted?

Key consideration 4. A governance body should identify scenarios that could potentially prevent the payment scheme/arrangement from being able to carry out its critical operations and providing its services as a going concern

Scenarios that could prevent a payment scheme/arrangement from carrying out its critical operations and providing its services

Q.3.4.1. How does the governance body identify scenarios that could potentially prevent the payment scheme/arrangement from carrying out its critical operations and providing its services? What scenarios have been identified as a result?

Principle 4: credit risk

A payment scheme should effectively measure, monitor and manage its credit exposures to payment service providers and/or end users as well as those arising from its payment, clearing and settlement processes. A payment scheme/ arrangement should maintain sufficient financial resources to fully cover its credit exposure to each payment service provider with a high degree of confidence

Payment scheme functions	Payment arrangement functions/functionalities	Payment instrument
☐ Governance of a payment scheme ☐ Service provision ☒ Payment guarantee ☐ Processing ☒ Clearing ☒ Settlement	☐ Governance of a payment arrangement ☐ Initiation, facilitation and requests to execute transfers of value ☐ Storage or registering of personalised security credentials ☐ Storage of payment instrument-related data	☒ Payment card ☒ Credit transfer ☒ Direct debit ☒ E-money ☒ Digital payment token ☒ Cash[14]

Key consideration 1. A payment scheme should establish a robust framework for managing its credit exposures to its payment service providers and/or end users as well as those arising from its payment guarantee, clearing and settlement functions. Credit exposures may include current exposures and/or potential future exposures

Q.4.1.1. What framework has the payment scheme established for managing credit exposures, including current and potential future exposures, to its payment service providers and/or end users, arising from its payment guarantee, clearing and settlement processes?

Q.4.1.2. How frequently is the framework reviewed to reflect the changing environment, market practices and new products?

Key consideration 2. A payment scheme should identify sources of credit risk, routinely measure and monitor credit exposures, and use the appropriate risk management tools to control risk

Q.4.2.1. How does the governance body identify sources of credit risk in the payment scheme/arrangement? What sources of credit risk has the governance body identified?

Q.4.2.2. How does the payment scheme measure and monitor credit exposures? How frequently does/can the payment scheme/arrangement recalculate these exposures? How timely is the information?

Q.4.2.3. Does the governance body have a complete overview of all existing clearing and settlement arrangements for the payment scheme, including major in-house

[14] Only as a provision of cash/cash placement.

clearing and settlement arrangements? Does the governance body evaluate the credit risks arising from the various clearing and settlement arrangements?

Key considerations 3-7: not applicable to a payment scheme/arrangement

Principle 5: collateral

A payment scheme that requires collateral to manage its or its payment service providers' credit exposures should accept collateral with low credit, liquidity and market risk

Payment scheme functions	Payment arrangement functions/functionalities	Payment instrument
☐ Governance of a payment scheme ☐ Service provision ☒ Payment guarantee ☐ Processing ☒ Clearing ☒ Settlement	☐ Governance of a payment arrangement ☐ Initiation, facilitation and requests to execute transfers of value ☐ Storage or registering of personalised security credentials ☐ Storage of payment instrument-related data	☒ Payment card ☒ Credit transfer ☒ Direct debit ☒ E-money ☒ Digital payment token ☒ Cash[15]

Note: Because of the extensive interactions between the financial risk management and financial resources principles, this principle should be viewed together with Principle 4 for credit risk and Principle 7 for liquidity risk, as appropriate.

Key consideration 1. A payment scheme should generally limit assets used as collateral to those with low credit, liquidity and market risks

Q.5.1.1. How does the payment scheme determine whether a specific asset can be accepted as collateral, including on an exceptional basis? How does the payment scheme determine what qualifies as an exceptional basis? How frequently does the payment scheme adjust these determinations? How frequently does the payment scheme accept collateral on an exceptional basis, and does the scheme apply any limits to its acceptance of such collateral?

Q.5.1.2. How does the payment scheme monitor the collateral posted to ensure it meets the applicable acceptance criteria?

Key considerations 2-6: not applicable to a payment scheme/arrangement

[15] Only as a provision of cash/cash placement.

Principle 6: not applicable to a payment scheme/arrangement

Principle 7: liquidity risk

A payment scheme should measure, monitor and manage its liquidity risk effectively. A payment scheme should maintain sufficient liquid resources in all relevant currencies to meet its payment obligations in a timely manner with a high degree of confidence. This should be under a wide range of potential stress scenarios that should include, but not be limited to, the default of the payment service provider and its affiliates that would generate the largest aggregate liquidity obligation for the payment scheme under extreme, but plausible, market conditions

Payment scheme functions	Payment arrangement functions/functionalities	Payment instrument
☐ Governance of a payment scheme	☐ Governance of a payment arrangement	☒ Payment card
☐ Service provision	☐ Initiation, facilitation and requests to execute transfers of value	☒ Credit transfer
☒ Payment guarantee	☐ Storage or registering of personalised security credentials	☒ Direct debit
☐ Processing	☐ Storage of payment instrument-related data	☒ E-money
☒ Clearing		☒ Digital payment token
☒ Settlement		☒ Cash[16]

Note: Because of the extensive interactions between the financial risk management and financial resources principles, this principle should be viewed together with Principle 4 on credit risk and Principle 5 on collateral, as appropriate.

Key consideration 1. A payment scheme should have a robust framework to manage the liquidity risks arising from its payment service providers, settlement banks, nostro agents, liquidity providers and other entities

Q.7.1.1. What framework does the payment scheme have in place to manage the liquidity risks, in all relevant currencies, arising from its payment service providers, settlement banks, nostro agents, liquidity providers and other entities?

Q.7.1.2. What is the nature and size of the payment scheme's liquidity needs and the associated sources of liquidity risks?

Q.7.1.3. How does the payment scheme take into account the potential aggregate liquidity risk presented by an individual entity and its affiliates, which may play multiple roles in respect of the payment scheme?

[16] Only as a provision of cash/cash placement.

Key consideration 2. A governance body should have effective tools which provide an overview of all clearing, settlement and funding flows relevant to the payment scheme, including major in-house clearing and settlement arrangements

Q.7.2.1. What tools does the governance body have in place to provide an overview of the clearing, settlement and funding flows? How does the governance body mitigate the liquidity risks that exceed its risk appetite?

Q.7.2.2. Does the governance body monitor the liquidity risks of clearing/settlement agents, in line with its overall risk appetite?

Q.7.2.3. How frequently is the framework for managing liquidity exposures reviewed to reflect the changing environment, market practices and new products?

Q.7.2.4. What incentives do the rules and procedures of the payment scheme provide for the management and containment of liquidity risk? For example, are incentives provided through the ongoing monitoring and analysis of the credit and liquidity risks that payment service providers and/or payment service users pose to the payment scheme?

Key consideration 3. If a payment scheme offers a guarantee function, it should maintain sufficient liquid resources to meet the guarantee obligations with a high degree of confidence. This should be under a wide range of potential stress scenarios that should include, but not be limited to, the default of the payment service provider and its affiliates that would generate the largest aggregate payment obligation in extreme, but plausible, market conditions

Q.7.3.1. How does the payment scheme determine the amount of liquid resources required to meet the obligations deriving from the guarantee function? What potential stress scenarios (including, but not limited to, the default of the payment service provider and its affiliates that would generate the largest aggregate payment obligation under extreme, but plausible, market conditions) does the payment scheme use to make this determination?

Q.7.3.2. What is the estimated size of the liquidity shortfall that the payment scheme would need to cover?

Key considerations 4-10: not applicable to a payment scheme

Principle 8: settlement finality and crediting end users

A payment scheme should define clear rules for final settlement

Payment scheme functions	Payment arrangement functions/functionalities	Payment instrument
☐ Governance of a payment scheme ☒ Service provision ☒ Payment guarantee ☐ Processing ☒ Clearing ☒ Settlement	☐ Governance of a payment arrangement ☐ Initiation, facilitation and requests to execute transfers of value ☐ Storage or registering of personalised security credentials ☐ Storage of payment instrument-related data	☒ Payment card ☒ Credit transfer ☒ Direct debit ☒ E-money ☒ Digital payment token ☒ Cash[17]

Key consideration 1. A payment scheme should clearly define the point after which the transfer of value instructions or other obligations may no longer be revoked by a payment service provider and the payee/payer will be credited/debited. A technical service provider should complete settlement no later than the end of the value day

Point of settlement finality

Q.8.1.1. At what point is the transfer of value final, meaning that it is irrevocable and unconditional? Is the point of finality defined and documented? How and to whom is this information disclosed?

Q.8.1.2. How do the payment scheme's legal framework and rules, including the applicable insolvency law(s), acknowledge the discharge of a transfer of value or other obligations between payment service providers or among payment service providers and end users?

Q.8.1.3. How does the payment scheme demonstrate that there is a high degree of legal certainty that finality will be achieved in all relevant jurisdictions (e.g. by obtaining a well-reasoned legal opinion)?

Intraday settlement

Q.8.1.4. If settlement takes place through multiple-batch processing, what is the frequency of the batches and within what timeframe are they processed? What happens if a payment service provider does not have sufficient funds or securities at the time of settlement – are transactions entered in the next batch? If so, what is the status of those transactions and when would they become final for payment service providers?

[17] Only as a provision of cash/cash placement.

Revocability and irrevocability of transactions

Q.8.1.5. How does the payment scheme define the point at which transfer of value instructions or other obligations may not be revoked by a payment service provider or end user? How does the payment scheme prevent the unilateral revocation of accepted and unsettled transfer of value instructions or other obligations after this time?

Q.8.1.6. Under what circumstances can an instruction or obligation that has been accepted be revoked (e.g. R-transactions)? How can an instruction be revoked? Who is permitted to revoke transfer of value instructions?

Principle 9: money settlement

If central bank money is not used for the money settlement of the obligations of the end users or the payment service providers of a payment scheme, the governance body should minimise and strictly control the credit and liquidity risk arising from the use of commercial bank money

Payment scheme functions	Payment arrangement functions /functionalities	Payment instrument
☐ Governance of a payment scheme ☒ Service provision ☒ payment Guarantee ☐ Processing ☒ Clearing ☒ Settlement	☐ Governance of a payment arrangement ☐ Initiation, facilitation and requests to execute transfers of value ☐ Storage or registering of personalised security credentials ☐ Storage of payment instrument-related data	☒ Payment card ☒ Credit transfer ☒ Direct debit ☒ E-money ☒ Digital payment token ☒ Cash[18]

Key considerations 1-2: not applicable to a payment scheme

[18] Only as a provision of cash/cash placement.

Key consideration 3. If a payment scheme settles in commercial bank money it should monitor, manage and limit the credit and liquidity risks arising from commercial settlement banks. In particular, a payment scheme should establish and monitor its settlement banks' adherence to strict criteria that take account of, among other things, their regulation and supervision, creditworthiness, capitalisation, access to liquidity and operational reliability. A payment scheme should also monitor and manage the concentration of credit and liquidity exposures to its commercial settlement banks

Q.9.3.1. How does the governance body monitor the settlement banks' adherence to the criteria it uses for selection? For example, how does the governance body evaluate the banks' regulation, supervision, creditworthiness, capitalisation, access to liquidity and operational reliability?

Q.9.3.2. How does the governance body monitor, manage and limit the credit and liquidity risks arising from commercial settlement banks? How does the governance body monitor and manage the concentration of credit and liquidity exposures to these banks?

Q.9.3.3. How does the governance body assess its potential losses and liquidity pressures, as well as those of its payment service providers, in the event of the failure of its largest settlement bank?

Key consideration 4. If a payment scheme performs money settlements on its own books, it should minimise and strictly control its credit and liquidity risks

Q.9.4.1. If a payment scheme conducts money settlements on its own books, how does it minimise and strictly control its credit and liquidity risks?

Key consideration 5. The payment scheme's governance body's legal agreements with any settlement banks should state clearly when transfers on the books of individual settlement banks are expected to occur, that transfers should be final when effected, and that funds received should be transferable as soon as possible, at the latest by the end of the value day (and ideally intraday), to enable the payment scheme and its payment service providers to manage credit and liquidity risks

Q.9.5.1. Do the payment scheme's governance body's legal agreements with its settlement banks state when transfers occur, that transfers are final when effected,

and that funds received are transferable as soon as possible and at the latest by the end of the value day?

Principle 10-12: not applicable to a payment scheme/arrangement

Principle 13: payment service provider default rules and procedures

A payment scheme should have effective and clearly defined rules and procedures for managing the default of a payment service provider. These rules and procedures should be designed to ensure that a payment scheme can take timely action to contain losses and liquidity pressures and, thereby, continue to meet its obligations

Payment scheme functions	Payment arrangement functions/functionalities	Payment instrument
☒ Governance of a payment scheme (KC 1, KC2) ☒ Service provision[19] ☒ Payment guarantee (KC1) ☐ Processing ☒ Clearing ☒ Settlement	☐ Governance of a payment arrangement ☐ Initiation, facilitation and requests to execute transfers of value ☐ Storage or registering of personalised security credentials ☐ Storage of payment instrument-related data	☒ Payment card ☒ Credit transfer ☒ Direct debit ☒ E-money ☒ Digital payment token ☒ Cash[20]

Key consideration 1. A payment scheme should have rules and procedures in place which enable the payment scheme and/or the other payment service providers to continue to meet their obligations (including those resulting from guarantees and R-transactions) in the event of the default of a payment service provider

Rules and procedures for the default of a payment service provider

Q.13.1.1. Do the payment scheme's rules and procedures clearly define a default event (including the financial and the operational default of a payment service provider) and the method used to identify a default? How are these events defined?

Q.13.1.2. How do the payment scheme's rules and procedures address the obligations of the payment scheme and/or the other payment service providers in the event of the default of a payment service provider (e.g. when it comes to payment

[19] Where applicable, since most aspects are covered by existing supervisory requirements for payment service providers.

[20] Only as a provision of cash/cash placement.

guarantees and/or reverse transactions affecting the defaulting payment service provider)?

Key consideration 2. A payment scheme should be well prepared to implement its default rules and procedures, including any appropriate discretionary procedures provided for in its rules

Q.13.2.1. Does the governance body have internal plans in place which clearly delineate roles and responsibilities in the event of a default? What are these plans?

Q.13.2.2. What kind of communication procedures does the governance body have in place to contact all relevant stakeholders – including regulators, supervisors and overseers – in a timely manner?

Q.13.2.3: How frequently are internal plans for dealing with a default reviewed? Who is in charge of these plans?

Key considerations 3-4: not applicable to payment scheme/arrangement

Principle 14: not applicable to a payment scheme/arrangement

Principle 15: general business risk

A payment scheme/arrangement should identify, monitor and manage its general business risk and it should hold sufficient liquid net assets funded by equity to cover potential general business losses. This would allow it to continue operations and provide services as a going concern if such losses were to materialise

Payment scheme functions	Payment arrangement functions/functionalities	Payment instrument
☒ Governance of a payment scheme ☐ Service provision ☐ Payment guarantee ☐ Processing ☐ Clearing ☐ Settlement	☒ Governance of a payment arrangement ☐ Initiation, facilitation and requests to execute transfers of value ☐ Storage or registering of personalised security credentials ☐ Storage of payment instrument-related data	☒ Payment card ☒ Credit transfer ☒ Direct debit ☒ E-money ☒ Digital payment token ☒ Cash[21]

[21] Only as a provision of cash/cash placement.

Key consideration 1. A payment scheme/arrangement should have robust management and control systems to identify, monitor and manage general business risks, including losses due to poor execution of business strategy, negative cash flows, or unexpected and excessively large operating expenses

Q.15.1.1. How does the payment scheme/arrangement identify its general business risks? What general business risks has the governance body identified?

Q.15.1.2. How does the payment scheme/arrangement monitor and manage general business risks on an ongoing basis?

Key considerations 2-5: not applicable to a payment scheme/arrangement

Principle 16: custody and investment risk

A payment scheme should safeguard its end users' assets and minimise the risk of losses on these assets or delayed access to them. A payment scheme should invest in instruments that carry minimal credit, market and liquidity risks

Payment scheme functions	Payment arrangement functions/functionalities	Payment instrument
☒ Governance of a payment scheme	☐ Governance of a payment arrangement	☐ Payment card
☒ Service provision	☐ Initiation, facilitation and requests to execute transfers of value	☐ Credit transfer
☒ Payment guarantee	☐ Storage or registering of personalised security credentials	☐ Direct debit
☐ Processing	☐ Storage of payment instrument-related data	☒ E-money
☐ Clearing		☒ Digital payment token
☐ Settlement		☐ Cash[22]

Key consideration 1. A payment scheme should hold its own assets, as well as those of its payment service providers and/or its end users, at supervised and regulated entities that follow robust accounting practices, effective safekeeping procedures and internal controls to fully protect the assets

Q.16.1.1. If the payment scheme uses custodians, how does the payment scheme/arrangement select its custodians? What are the specific selection criteria the payment scheme/arrangement uses, including the supervision and regulation of these entities? How does the payment scheme monitor the custodians' adherence to these criteria?

[22] Only as a provision of cash/ cash placement.

Q.16.1.2. How does the payment scheme verify that these entities follow robust accounting practices, effective safekeeping procedures and internal controls that fully protect its own and its payment service providers' assets?

Key consideration 2. A payment scheme should have prompt access to its assets and the assets of its payment service providers and/or end users, when required

Q.16.2.1. How has the payment scheme established that there is a sound legal basis underpinning its enforcement of its interest or ownership rights in assets held in custody?

Q.16.2.2. How does the payment scheme ensure that it has prompt access to its assets, including securities that are held with a custodian in another time zone or legal jurisdiction, in the event of the default of a payment service provider and/or end user?

Key considerations 3-4: not applicable to a payment scheme

Principle 17: operational risk

Payment schemes/arrangements, payment services providers and technical service providers should identify the plausible sources of operational risk, whether internal or external, and mitigate impact by implementing appropriate systems, policies, procedures and controls. Systems should be designed to ensure a high degree of security and operational reliability and should have adequate, scalable capacity. Business continuity management should aim for timely recovery of operations and the fulfilment of the obligations of the payment scheme/arrangement, the payment services providers or the technical service providers, including in the event of a wide-scale or major disruption

Payment scheme functions	Payment arrangement functions/functionalities	Payment instrument
☒ Governance of a payment scheme All KCs ☒ Service provision[23] (KC 1 Q.1,2,3 KC 4-8) ☐ Payment guarantee ☒ Processing (KC 1, Q.17.2, KC 4-8) ☒ Clearing (KC 1, Q.17.2, KC 4-8) ☒ Settlement (KC 1, Q.17.2, KC 4-8)	☒ Governance of a payment arrangement All KCs ☒ Initiation, facilitation and requests to execute transfers of value KC 1, Q.1,2,3 KC 4-8 ☒ Storage or registering of personalised security credentials KC 1 Q.1, 2; KC 4-8 ☒ Storage of payment instrument-related data KC 1 Q.1, 2 KC 4-8	☒ Payment card ☒ Credit transfer ☒ Direct debit ☒ E-money ☒ Digital payment token ☒ Cash[24]

[23] Where applicable, since most aspects are covered by existing supervisory requirements for payment service providers.

[24] Only as a provision of cash/cash placement.

Key consideration 1. A payment scheme/arrangement should establish a robust operational risk management framework with appropriate systems, policies, procedures and controls in place to identify, monitor, and manage operational risks

Identification of operational risk

Q.17.1.1. What are the payment scheme/arrangement's policies and processes for identifying the plausible sources of operational risks? How do the payment scheme/arrangement's processes identify plausible sources of operational risks, whether these risks arise from internal sources (e.g. the arrangements of the payment scheme/arrangement itself, including human resources), from payment service providers and technical service providers, or from external sources?

Q.17.1.2. What sources of operational risks has the payment scheme/arrangement identified? What single points of failure in its operations has the payment scheme/arrangement identified? Does the payment scheme/arrangement collect and analyse up-to-date information on fraud data and operational and security incidents.

Comprehensive risk management framework

Q.17.1.3. Does the risk management framework deal with all aspects relevant for the functioning of the payment scheme/arrangement? Aspects may include:

- organisational, personnel, infrastructural and technical issues;
- the impact and likelihood of internal and external security threats;

existing or potential safeguards such as technical controls and insurance.

Q.17.1.3: Does the risk management framework consider the aspects below?

- All operational aspects of the payment scheme/arrangement (e.g. end user devices, accepting devices, the issuing process for personalised security credentials, the operation of accepting devices, communication network facilities, acquiring transactions, clearing and settlement, the risk profiles of payment service providers and technical service providers, and mandate management)
- All technological solutions and platforms used, the application architecture, the programming techniques and routines, as well as all payment channels taken into account
- All types and variations of payment instruments provided within the payment scheme/arrangement (e.g. credit/debit, Core/B2B/Inst) and all types of transactions (e.g. first, one-off, recurrent, final) supported by the payment scheme/arrangement?

Management of operational risk

Q.17.1.3. How does the payment scheme/arrangement monitor and manage identified operational risks? Where are these systems, policies, procedures and controls documented?

Policies, processes and controls

Q.17.1.4. What policies, processes and controls does the payment scheme/arrangement employ in order to ensure that operational procedures are implemented appropriately? To what extent do the payment scheme/arrangement's systems, policies, processes and controls take into consideration the relevant international, national and industry-level operational risk management standards?

Q.17.1.5. What human resources policies does the payment scheme/arrangement have in place to hire, train and retain qualified personnel, and how do such policies mitigate the effects of high rates of personnel turnover or key-person risk? How do the payment scheme/arrangement's human resources and risk management policies address fraud prevention?

Q.17.1.6. How do the payment scheme/arrangement's change management and project management policies and processes mitigate the risk of changes and major projects inadvertently affecting the smooth functioning of the payment scheme/arrangement? Does this process include security reviews?

Key consideration 2. The governance body should clearly define roles and responsibilities for addressing operational risk and should endorse the payment scheme/arrangement's operational risk management framework. Systems, operational policies, procedures and controls should be reviewed, audited and tested both periodically and after significant changes

Roles, responsibilities and framework

Q.17.2.1. How has the governance body defined and documented key roles and responsibilities in respect of operational risk management?

Q.17.2.2. Does the governance body explicitly review and endorse the payment scheme/arrangement's operational risk management framework? How frequently does the board review and endorse this framework?

Review, audit and testing

Q.17.2.3. How does the payment scheme/arrangement review, audit and test its systems, policies, procedures and controls, including its operational risk management arrangements with payment service providers and technical service providers? How frequently does the payment scheme/arrangement conduct these reviews, audits and tests?

Q.17.2.4: To what extent, where relevant, is the payment scheme/arrangement's operational risk management framework subject to external audit?

Key consideration 3: A payment scheme/arrangement should have clearly defined operational reliability objectives and should have policies in place that are designed to achieve those objectives

Q.17.3.1: What are the payment scheme/arrangement's operational reliability objectives, whether qualitative or quantitative? Where and how are they documented? How does the governance body monitor the availability of the payment scheme/arrangement's key services?

Q.17.3.2. What policies are in place, with the aim of achieving the payment scheme/arrangement's operational reliability objectives, to ensure that the payment scheme/arrangement takes appropriate action as needed?

Q17.3.3. Are all incidents logged, reported, systematically investigated and appropriately followed up?

Key consideration 4. A payment scheme/arrangement should ensure that it has adequate scalable capacity to handle increasing stress volumes and to achieve its service-level objectives

Q.17.4.1. How does the payment scheme/arrangement review, audit and test the scalability and adequacy of its capacity to handle, as a minimum, projected stress volumes? How frequently does the payment scheme/arrangement conduct these reviews, audits and tests?

Q.17.4.2. How are situations in which operational capacity is neared or exceeded addressed?

Key consideration 5. A payment scheme/arrangement should have comprehensive physical and information security policies that address all potential vulnerabilities and threats

Physical security

Q.17.5.1. What are the payment scheme/arrangement's policies and processes, including change management and project management policies and processes, for addressing the plausible sources of physical vulnerabilities and threats on an ongoing basis?

Q.17.5.2. Do the payment scheme/arrangement's policies, processes, controls and testing appropriately take into consideration the relevant international, national and industry-level standards as well as the relevant legislation with regard to physical security?

Information security

Q.17.5.3. What are the payment scheme/arrangement's policies and processes, including change management and project management policies and processes, for addressing the plausible sources of information security vulnerabilities and threats to the payment scheme/arrangement, the payment service providers, the technical service providers and the end users on an ongoing basis?

Q.17.5.4. Do the payment scheme/arrangement's policies, processes, controls and testing appropriately take into consideration the relevant international, national and industry-level standards as well as the relevant legislation with regard to information security?

Q.17.5.5. Are operational service levels and security policies for the appropriate domains (e.g. security management, protection of sensitive data or devices during manufacturing or generation, the distribution of end user devices, the initiation and processing of transactions, clearing and settlement, business continuity and outsourcing) and all payment channels well documented?

Q.17.5.6. Does the payment schemes/arrangement's security policy ensure data privacy, integrity and authenticity (e.g. electronic mandates) and the confidentiality of secrets (e.g. personalised security credentials) when data are processed, stored or exchanged? Is end-to-end encryption applied when sensitive data are exchanged? Does the scheme or arrangement require all payment service providers and technical service providers to comply with these procedures? Are there effective contingency plans in place in the event of operational secrets or sensitive payment information being revealed or compromised?

Q.17.5.7. Are there effective and secure procedures in place for the initialisation, personalisation and delivery of end-user devices, the generation and delivery of secrets (e.g. personalised security devices) or e-mandates, access to the payment

service (e.g. online banking), the payment initiation process, the validation of payment orders, the transaction phase (including return transactions and the cancellation of mandates) and the dematerialisation of paper mandates?

Q.17.5.8. Does the design, manufacturing or generation of end user payment devices, accepting devices and other technical devices guarantee an adequate degree of security, in line with the security policies of the payment scheme/arrangement?

Q.17.5.9. Are the activities of payers and payees adequately monitored (in line with the payment scheme/arrangement's security policy), in order to facilitate a timely reaction to fraud and any risks posed by fraudulent activities? Are there appropriate measures in place to limit the impact of fraud?

Q.17.5.10. Does the payment scheme/arrangement monitor technological developments relevant to the functioning and security of the payment scheme/arrangement, especially with regard to fraud techniques (for both internal and external fraud), the evolution of the characteristics and features of the payment instrument, the optional services and the initiation channel?

Key consideration 7. A governance body should identify, monitor and manage the risks that key payment service providers, critical technical service providers and utility providers might pose to operations within the payment scheme/arrangement

Risks to the payment scheme/arrangement's own operations

Q.17.7.1. What risks to its operations has the payment scheme/arrangement identified arising from its key payment service providers, its critical technical service providers and its utility providers? How and to what extent does the payment scheme/arrangement monitor and manage these risks?

Q.17.7.2. If the payment scheme/arrangement has outsourced services which are critical to its operations, how and to what extent does it ensure that the operations of a critical technical service provider meet the same reliability and contingency requirements they would need to meet if they were provided internally?

Key consideration 7.a. The payment scheme/arrangement's business impact analyses should clearly identify those operations that are crucial for the smooth functioning of the payment scheme/arrangement. Effective and comprehensive contingency plans should be in place to deal with any disaster or incident that would jeopardise the availability of the payment scheme/arrangement. The adequacy of these plans should be tested and reviewed regularly

Q.17.7.a.1. Do the payment scheme/arrangement's business impact analyses clearly identify the operations that are crucial for the smooth functioning of the payment scheme/arrangement? Are there effective and comprehensive contingency plans in place to deal with any disaster or incident that would jeopardise the availability of the payment scheme/arrangement? Is the adequacy of these plans tested and reviewed regularly?

Key consideration 8. A payment scheme/arrangement should establish an effective cyber resilience framework, with appropriate governance measures in place to manage cyber risk

Q.17.8.1. Has the governance body identified the payment scheme/arrangement's critical operations and supporting assets? Are appropriate measures in place to protect them from, detect, respond to and recover from cyber-attacks? Are these measures regularly tested?

Q.17.8.2. Does the payment scheme/arrangement have a sound level of situational awareness of cyber threats?

Q.17.8.3. Does the governance body ensure that there is a process of continuous learning and evolving that enables it to adapt its cyber resilience framework to the dynamic nature of cyber risks in a timely manner, as required?

Principle 18: access and participation requirements

A payment scheme/arrangement should have objective, risk-based and publicly disclosed criteria for participation, which permit fair and open access.

Payment scheme functions	Payment arrangement functions/functionalities	Payment instrument
☒ Governance of a payment scheme ☐ Service provision ☐ Payment guarantee ☐ Processing ☐ Clearing ☐ Settlement	☒ Governance of a payment arrangement ☐ Initiation, facilitation and requests to execute transfers of value ☐ Storage or registering of personalised security credentials ☐ Storage of payment instrument-related data	☒ Payment card ☒ Credit transfer ☒ Direct debit ☒ E-money ☒ Digital payment token ☒ Cash[25]

Notes: It should be noted that payment scheme/arrangements are subject to the constraints of the local laws and policies of the jurisdiction in which the payment scheme/arrangement operates – these laws may prohibit or require the inclusion of certain categories of licensed payment service providers. This principle should be viewed together with Principle 21 on efficiency and effectiveness, as well as other principles, as appropriate.

Key consideration 1. A governance body should allow for fair and open access to the payment scheme/arrangement, including by payment service providers which adhere directly and, where relevant, indirectly to the scheme, based on reasonable risk-related participation requirements

Participation criteria and requirements

Q.18.1.1. What are the payment scheme/arrangement's criteria and requirements for participation (e.g. operational, financial and legal requirements)?

Q.18.1.2. How do these criteria and requirements allow for fair and open access to the payment scheme/arrangement, including by payment service providers which adhere directly and, where relevant, indirectly to the scheme, based on reasonable risk-related participation requirements?

[25] Only as a provision of cash/cash placement.

Key consideration 2. Participation requirements should be justified in terms of the safety and efficiency of the payment scheme/arrangement and the markets it serves. They should be tailored to and commensurate with the payment scheme/arrangement's specific risks and they should be publicly disclosed. Subject to it maintaining acceptable risk control standards, a payment scheme/arrangement should endeavour to set requirements that have the least restrictive impact on access possible under the circumstances

Justification and rationale for participation criteria

Q.18.2.1. How are the requirements for participation in the payment scheme/arrangement justified in terms of the safety and efficiency of the payment scheme/arrangement and its role in the markets it serves. How are they tailored to and commensurate with the payment scheme/arrangement's specific risks?

Q.18.2.2. Are there any participation requirements that are not risk-based but required by law or regulation? If so, what are these requirements?

Q.18.2.3. Are all classes of payment service provider subject to the same access criteria? If not, what is the rationale for the different criteria (e.g. size or type of activity, additional requirements for payment service providers that act on behalf of third parties, and additional requirements for payment service providers that are non-regulated entities)?

Least restrictive access

Q.18.2.4. How are the access restrictions and requirements reviewed to ensure that they have the least restrictive impact on access possible under the circumstances, in a manner which is consistent with maintaining acceptable risk controls? How frequently is this review conducted?

Disclosure of criteria

Q.18.2.5. How is participation criteria, including restrictions in participation, publicly disclosed?

Key consideration 3. A payment scheme/arrangement should monitor compliance with its participation requirements on an ongoing basis. It should have clearly defined and publicly disclosed procedures for facilitating the suspension and orderly exit of any payment service providers or technical service providers that breach, or no longer meet, the participation requirements

Monitoring compliance

Q.18.3.1. How does the governance body monitor the ongoing compliance of payment service providers and technical service providers with the participation criteria? How are the payment scheme/arrangement's policies designed to ensure that the information it uses to monitor compliance with participation criteria is timely and accurate?

Q.18.3.2. What are the payment scheme/arrangement's policies for conducting enhanced surveillance of, or imposing additional controls on, payment service providers or technical service providers whose risk profile has deteriorated?

Suspension and orderly exit

Q.18.3.3. What are the payment scheme/arrangement's procedures for managing the suspension and orderly exit of payment service providers or technical service providers that breach, or no longer meet, the participation requirements?

Q.18.3.4. How are the payment scheme/arrangement's procedures for managing the suspension and orderly exit of payment service providers or technical service providers disclosed to the public?

Principle 19: not applicable to a payment scheme/arrangement

Principle 20: not applicable to a payment scheme/arrangement

Principle 21: efficiency and effectiveness

A payment scheme/arrangement should be efficient and effective in meeting the requirements of the payment service providers, end users and the markets it serves.

Payment scheme functions	Payment arrangement functions/functionalities	Payment instrument
☒ Governance of a payment scheme ☒ Service provision ☒ Payment guarantee ☒ Processing ☒ Clearing ☒ Settlement	☒ Governance of a payment arrangement ☒ Initiation, facilitation and requests to execute transfers of value ☒ Storage or registering of personalised security credentials ☒ Storage of payment instrument-related data	☒ Payment card ☒ Credit transfer ☒ Direct debit ☒ E-money ☒ Digital payment token ☒ Cash[26]

Key consideration 1. A payment scheme/arrangement should be designed to meet the needs of its payment service providers, its technical service providers and the end users it serves, in particular with regard to the products provided, the use of technology and procedures

Q.21.1.1. How does the payment scheme/arrangement determine whether its design (including the individual functions, functionalities, services and products) takes into account the needs of its payment service providers, its technical service providers and the markets it serves?

Q.21.1.2. How does the payment scheme/arrangement determine whether it is meeting the requirements and needs of its payment service providers, its technical service providers and its end users, and will continue to meet those requirements as they change (e.g. through the use of feedback mechanisms)?

[26] Only as a provision of cash/cash placement.

Key consideration 2. A payment scheme/arrangement should have clearly defined goals and objectives. These should be measurable and achievable, including in the areas of minimum service levels, risk management expectations and business priorities

Q.21.2.1. What are the payment scheme/arrangement's goals and objectives as far as the effectiveness of its operations is concerned?

Q.21.2.2. How does the payment scheme/arrangement ensure that it has clearly defined goals and objectives that are measurable and achievable?

Q.21.2.3. To what extent have the goals and objectives been achieved? What mechanisms does the payment scheme/arrangement use to measure and assess this?

Key consideration 3. A payment scheme/arrangement should use established mechanisms for the regular review of its efficiency and effectiveness

Q.21.3.1. What processes and metrics does the payment scheme/arrangement use to evaluate its efficiency and effectiveness?

Q.21.3.2. How frequently does the payment scheme/arrangement evaluate its efficiency and effectiveness?

Principle 22: communication procedures and standards

A payment scheme/arrangement should use, or at least accommodate, relevant internationally accepted communication procedures and standards in order to facilitate the efficient transfer of value between end users

Payment scheme functions	Payment arrangement functions/functionalities	Payment instrument
☒ Governance of a payment scheme ☒ Service provision ☐ Payment guarantee ☒ Processing ☒ Clearing ☒ Settlement	☒ Governance of a payment arrangement ☒ Initiation, facilitation and requests to execute transfers of value ☒ Storage or registering of personalised security credentials ☒ Storage of payment instrument-related data	☒ Payment card ☒ Credit transfer ☒ Direct debit ☒ E-money ☒ Digital payment token ☒ Cash[27]

Note: This principle is not applicable if the use of a particular communication standard is required by law.

[27] Only as a provision of cash/cash placement.

Key consideration 1. A payment scheme/arrangement should use, or at least accommodate, internationally accepted communication procedures and standards

Communication procedures

Q.22.1.1. Does the payment scheme/arrangement use an internationally accepted communication procedure and, if so, which one(s)? If not, how does the payment scheme/arrangement accommodate internationally accepted communication procedures?

Q.22.1.2. If the payment scheme/arrangement engages in cross-border operations, how do the payment scheme/arrangement's operational procedures, processes and systems use or otherwise accommodate internationally accepted communication procedures for cross-border operations?

Communication standards

Q.22.1.3. Does the payment scheme/arrangement use an internationally accepted communication standard and, if so, which one(s)? If not, how does the payment scheme/arrangement accommodate internationally accepted communication standards?

Q.22.1.4. If the payment scheme/arrangement engages in cross-border operations, how do the payment scheme/arrangement's operational procedures, processes and systems use or otherwise accommodate internationally accepted communication standards for cross-border operations?

Q.22.1.5. If no international standard is used, how does the payment scheme/arrangement accommodate systems that translate or convert message formats and data from international standards into their domestic equivalent and vice versa?

Principle 23: disclosure of rules, key procedures and market data

A payment scheme/arrangement should have clear and comprehensive rules and procedures and it should provide sufficient information to enable payment service providers, technical service providers and end users to reach an accurate understanding of the risks, fees and other material costs they incur by participating in/making use of the payment scheme/arrangement. All relevant rules and key procedures should be publicly disclosed, bearing in mind those rules and procedures which, if disclosed, could pose a threat to the security of a scheme or arrangement. The latter should only be disclosed to scheme or arrangement stakeholders on a "need to know" basis.

Payment scheme functions	Payment arrangement functions/functionalities	Payment instrument
☒ Governance of a payment scheme ☒ Service provision ☒ Payment guarantee ☐ Processing ☐ Clearing ☐ Settlement	☒ Governance of a payment arrangement ☒ Initiation, facilitation and requests to execute transfers of value ☒ Storage or registering of personalised security credentials ☒ Storage of payment instrument-related data	☒ Payment card ☒ Credit transfer ☒ Direct debit ☒ E-money ☒ Digital payment token ☒ Cash[28]

Note: In the context of this principle, information should be disclosed to the extent that it would not risk prejudicing the security and integrity of the payment scheme/arrangement or divulging commercially sensitive information.

Key consideration 1. A payment scheme/arrangement should adopt clear and comprehensive rules and procedures which should be fully disclosed to payment service providers and technical service providers. Relevant rules and key procedures should also be disclosed to end users and/or publicly disclosed. Sensitive information should only be disclosed on a "need to know" basis

Rules and procedures

Q.23.1.1. What documents comprise the payment scheme/arrangement's rules and procedures? How are these documents disclosed to payment service providers and technical service providers?

Q.23.1.2. How does the payment scheme/arrangement ensure that its rules and procedures are clear and comprehensive?

[28] Only as a provision of cash/cash placement.

Disclosure

Q.23.1.3. What information is included in the payment scheme/arrangement's rules and procedures on the procedures it would follow in the event of non-routine, albeit foreseeable, events?

Q.23.1.4. How and to whom does the payment scheme/arrangement disclose the processes it follows when changing its rules and procedures?

Q.23.1.5. How does the payment scheme/arrangement disclose relevant rules and key procedures to end users and/or the public?

Key consideration 2. A payment scheme/arrangement should provide clear descriptions of the system's design and operations, as well as the rights and obligations of the payment scheme/arrangement's payment service providers, technical service providers and end users, so that they can assess the risks associated with participating in/making use of the payment scheme/arrangement

Q.23.2.1. Which documents contain information on the payment scheme/arrangement's design and operations?

Q.23.2.2. How and to whom does the governance body disclose the payment scheme/arrangement's design and operations?

Q.23.2.3. What information does the payment scheme/arrangement provide to its payment service providers and technical service providers about their rights, their obligations and the risks associated with participating in the payment scheme/arrangement?

Key consideration 3. A payment scheme/arrangement should provide all the necessary and appropriate documentation and capacity building to ensure that payment service providers, technical service providers and end users understand the payment scheme/arrangement's rules and procedures and the risks associated with participating in it/making use of it

Q.23.3.1. How does the payment scheme/arrangement ensure that the payment service providers/technical service providers/end users understand the payment scheme/arrangement's rules, procedures and the risks associated with participating in it/making use of it?

Q.23.3.2. Is there any evidence that the methods described above facilitate an understanding of the payment scheme/arrangement's rules, procedures and the risks associated with participating in it/making use of it?

Q.23.3.3. If the governance body identifies payment service providers or technical service providers whose behaviour demonstrates a lack of understanding of the payment scheme/arrangement's rules, procedures and the risks associated with participating, what remedial action does it take?

Key consideration 5. The payment scheme/arrangement should regularly disclose to the lead overseer and, where relevant, its payment service providers and technical service providers, how it addresses the principles of payment scheme/arrangement oversight. The payment scheme/arrangement should also, as a minimum, disclose basic data on transaction volumes and values

Q.23.5.1. When did the payment scheme/arrangement last answer the questions relating to an oversight assessment applicable to it? Has this assessment been updated following material changes to the payment scheme/arrangement and its environment?

Q.23.5.2. What quantitative information does the payment scheme/arrangement disclose to the public? How often is this information updated?

Q.23.5.3. What other information does the payment scheme/arrangement disclose to the public?

Q.23.5.4. How does the payment scheme/arrangement disclose this information to the public? In which language(s) are the disclosures provided?

Principle 24: not applicable to a payment scheme/arrangement

Annex 1: Comparison of PISA with other oversight assessment methodologies

Table 3

Comparison of the PISA assessment methodology with the PFMI and the assessment methodology for retail payment systems

		Payment schemes						Payment arrangements		Payment systems		
		Governance	Service provision	Payment guarantee	Processing	Clearing	Settlement	Governance	Functionalities	SIPS	PIRPS	ORPS
SIPS Regulation										☑		
Principle 1	Legal risk										☑	☑
KC 1 -5		☑	☑	☑	☑	☑	☑	☑	☑		KC 1-5	KC 1-5
Principle 2	Governance risk										☑	☑
KC 1 -7 *		☑	☒	☒	☒	☒	☒	☑	☒		KC 2, 7	`KC 2
Principle 3	Comprehensive risk management										☑	☑
KC 1 – 4		☑	☒	☒	☒	☒	☒	☑	☒		KC 1	KC 1
Principle 4	Credit risk										☒	☒
KC 1-2		☒	☒	☑	☒	☑	☑	☒	☒			
Principle 5	Collateral risk										☒	☒
KC 1		☒	☒	☑	☒	☑	☑	☒	☒			
Principle 7	Liquidity risk										☒	☒
KC 1-3		☒	☒	☑	☒	☑	☑	☒	☒			
Principle 8	Settlement finality and crediting of end user										☑	☑
KC 1		☒	☑	☑	☒	☑	☑	☒	☒		KC 1,3	KC 1,3
Principle 9	Money settlement risk										☑	☒
KC 3- 5		☒	☑	☑	☒	☑	☑	☒	☒		KC 1-5	KC 1-5
Principle 13	Service provider default										☑	

		Payment schemes						Payment arrangements		Payment systems		
		Governance	Service provision	Payment guarantee	Processing	Clearing	Settlement	Governance	Functionalities	SIPS	PIRPS	ORPS
KC 1		☑	☑	☑	☒	☑	☑	☒	☒		KC 1-3	KC 1,2
KC 2		☑	☒	☒	☒	☑	☑	☒	☒			
Principle 15	General business risk										☑	☒
KC 1		☑	☒	☒	☒	☒	☒	☑	☒		KC1-5	
Principle 16	Custody and investment risk											☒
KC 1 -2		☑	☑	☑	☒	☒	☒	☒	☒			
Principle 17	Operational risk											☑
KC 1		☑	☑	☒	☑	☑	☑	☑	☑		KC 1,3,5	KC 1,3,5
KC 2		☑	☑	☒	☑	☑	☑	☑	☑			
KC 3		☑	☑	☒	☑	☑	☑	☑	☑			
KC 4, 5,7,7a, 8		☑	☑	☒	☑	☑	☑	☑	☑			
Principle 18	Access and participation										☑	☑
KC 1 – 3		☑	☒	☒	☒	☒	☒	☑	☒		KC 1-3	KC 1, 3
Principle 21	Efficiency and effectiveness											☑
KC 1 -3		☑	☑	☑	☑	☒	☒	☑	☑		KC 1	KC 1
Principle 22	Communication											☒
KC 1		☑	☑	☒	☑	☒	☒	☑	☑		KC 1	KC 1
Principle 23	Disclosure										☑	☑
KC 1-3, 5		☑	☑	☑	☒	☒	☒	☑	☑		KC 1,2,4	KC 1,2,4
Total Principles		11	9	10	4	10	10	9	5		12	9

Table 3 above shows how the PISA principles differ from the respective principles in the PFMI and compares the key considerations with those applicable for retail payment systems. For principles highlighted in green, the content is more or less identical to that for the respective key considerations of the PFMI, yellow indicates some modifications and grey indicates that the key considerations and/or the assessment questions have been substantially reduced. It should be noted that some principles and key considerations are only applicable if there is a payment guarantee, while others – for the clearing and settlement functions – are only applicable in respect of scheme-wide risks or if the function is not a payment system subject to Eurosystem oversight.

Postal address 60640 Frankfurt am Main, Germany
Telephone +49 69 1344 0
Website www.ecb.europa.eu

For specific terminology please refer to the ECB glossary (available in English only).