ANNEX I - BIS CPSS CORE PRINCIPLES - ASSESSMENT AND RECOMMENDATIONS MATRIX

RELEVANT FACTORS		STANDARDS	STATUS IN THE COUNTRY[1]	RECOMMENDATIONS
LARGE VALUE PAYMENTS CLEARING AND SETTLEMENT (SIPS)		CPSS Core principles		
Legal basis		I. The system should have a well-founded legal basis under all relevant jurisdictions.	• Completeness and reliability of framework legislation; • Enforceability of laws and of contracts in all relevant circumstances; • Clarity of timing of final settlement especially when there is an insolvency (e.g., a participant's insolvency should not raise problems of revocability of payments); • Legal recognition of netting arrangements; • Existence of any zero hour or similar rules; • Enforceability of security interests provided under collateral arrangements and of any relevant repo agreements; • The legal structure should not inhibit the use of payment system technology. For example, laws and rules designed for paper-based processes should not create impediments or disincentives for electronic transfers. • A legal framework that would support electronic processing of payments (e.g., electronic records should be accepted as evidence in a court of law); • Relevant provisions of banking and central banking law; • Relevance of laws outside the domestic jurisdiction; ……	
Risk control		II. The system's rules and procedures should enable participants to have a clear understanding of the system's impact on each of the financial risks they incur through participation in it.	• Are the rules and procedures clear, comprehensive and up-to-date? • Do they explain the system design, its timetable and risk management procedures? • Do they explain the system's legal basis and roles of the parties? • Are they readily available? • Do they explain where there is discretion and how it is exercised; • Do they set out decision and notification procedures and timetables for handling abnormal situations? • Is there any organised participant training and monitor the performance of participants as evidence of their understanding?	

[1] ***Refer to the CPSS Core Principles Report and the Bank-Fund Guidance Note for FSAP assessments for a complete list of criteria.***

ANNEX I - BIS CPSS CORE PRINCIPLES - ASSESSMENT AND RECOMMENDATIONS MATRIX

RELEVANT FACTORS		STANDARDS	STATUS IN THE COUNTRY[1]	RECOMMENDATIONS
			• The system should provide clear, full and timely information to participants including information to support the tools for managing credit and liquidity risks.	
Risk control		III. The system should have clearly defined procedures for the management of credit and liquidity risks, which specify the respective responsibilities of the system operator and the participants and which provide appropriate incentives to manage and contain those risks.	***Credit risks (not all assessment criteria need to be in place)*** • system designs in which credit risk between participants does not arise (e.g. in real-time gross settlement systems); • Access criteria; • Credit limits (bilateral or multilateral) to cap exposures; • Loss-sharing arrangements and/or "defaulter pays" arrangements; • No unwinding procedures should be in place. ***Liquidity risks*** • Management of payment queues • Provision of intraday credit (which means credit risk issues for the lender, e.g. the central bank) • Throughput guidelines (e.g. intra-day proportion of payments) • Position (receiver or sender) limits • Tools for systems with deferred net settlement, used to comply with CP V. ***General tools*** • Rules addressing the consequences of a participants' defaults; • Information systems to support the tools for managing credit and liquidity risks; • Clear, full and timely (ideally real-time) financial information to participants; • Timely monitoring by the system operator. ***Incentives:*** • Formula for loss-sharing – for example if it reflects the scale/nature of controllable positions with the failed institution; • Pricing.	
Risk Control		IV. The system should provide prompt final settlement on the day of value, preferably during the day and at a minimum at the end of the day.	• Clarity in the system rules and procedures that a payment accepted by the system for settlement cannot be removed from the settlement process; (e.g., settlement cannot be considered final until there is no further possibility that the payment will be unwound); • Clearly defined and legally effective moment of final settlement;	

ANNEX I - BIS CPSS CORE PRINCIPLES - ASSESSMENT AND RECOMMENDATIONS MATRIX

RELEVANT FACTORS		STANDARDS	STATUS IN THE COUNTRY[1]	RECOMMENDATIONS
			• Ensuring that the interval between the system's acceptance of a payment and the payment's final settlement at least never lasts overnight and preferably is much shorter; • Ensuring that operating hours and the settlement processes are strictly enforced. ……	
Risk control		V. A system in which multilateral netting takes place should, at a minimum, be capable of ensuring the timely completion of daily settlements in the event of an inability to settle by the participant with the largest single settlement obligation.	Ensuring that additional financial resources are available to meet this contingency. These usually involve a combination of the following: – a pool of collateral (cash or securities), appropriately valued; – committed lines of credit. • The amount of such additional resources needs to be determined in relation to: – maximum individual settlement obligation; – whether the system meets or exceeds the minimum standard (i.e. whether the system is designed to withstand an inability to settle by the participant with the largest single settlement obligation or to withstand a more widespread inability to settle); • Alternatively, the need to control liquidity risk in this context can be avoided by the use of an alternative system design (e.g. RTGS or some types of hybrid design) that does not give rise to the concerns addressed by Core Principle V.	
Risk control		VI. Assets used for settlement should preferably be a claim on the central bank; where other assets are used, they should carry little or no credit risk.	If other assets are used, check: • the creditworthiness of the issuer of the settlement asset; • how readily the asset can be transferred into other assets; • size and duration of involuntary exposures to the issuer; • risk controls, if any. Also, if the settlement asset is not a claim on the central bank of issue, then analyze.	
Operational reliability		VII. The system should ensure a high degree of security and operational reliability and should have contingency arrangements for timely completion of daily processing.	***General*** • The system should meet the security policies and operational service levels agreed by the system operator and participants, and relevant legal constraints, system rules, risk management procedures, business requirements, or international, national or industry-level standards; • The system's security and operational reliability depend on both central system and participants components; the participants have responsibilities for security and operational	

ANNEX I - BIS CPSS CORE PRINCIPLES - ASSESSMENT AND RECOMMENDATIONS MATRIX

RELEVANT FACTORS		STANDARDS	STATUS IN THE COUNTRY[1]	RECOMMENDATIONS
			reliability. The system should be formally monitored to ensure the policies and service levels are being met; • Security policies and operational service levels should change over time, in response to market and technological developments; system should be designed and operated to meet such developments; • The system requires adequate numbers of well-trained, competent and trustworthy personnel to operate it safely and efficiently in both normal and abnormal situations; ***Security*** • Security objectives and policies should be established during the design of the system, and reviewed pe riodically. They should appropriate to the payment system, recognising its particular architecture and ownership; • System security should conform to commercially reasonable standards, for example for confidentiality, integrity, authentication, non-repudability, availability and auditability. Security features should be tested regularly; • The system should be subject to regular security risk analyses. The system operator should pro-actively monitor technological advances to keep system's security risk analysis up-to-date. ***Operational reliability*** • Threats to operational reliability arise not just from the failure of central system and participant components, but also from failures of infrastructure services and natural disasters; • The system requires comprehensive, rigorous and well-documented operational and technical procedures; • Changes to the system should be properly documented, authorised, controlled, tested and subject to quality assurance. • The system should be designed with sufficient capacity, which should be monitored and upgraded in advance of business changes; ***Business continuity*** • The system operator should carry out a formal business continuity planning exercise;	

ANNEX I - BIS CPSS CORE PRINCIPLES - ASSESSMENT AND RECOMMENDATIONS MATRIX

RELEVANT FACTORS		STANDARDS	STATUS IN THE COUNTRY[1]	RECOMMENDATIONS
			Simplicity and practicality should be key considerations when designing contingency arrangements; • Business continuity arrangements should be documented and regularly tested. They should include procedures for crisis management and information dissemination; • Business continuity arrangements could include: diversion of payments to another payment system; a second processing site; and/or a "minimum level service".	
Efficiency		VIII. The system should provide a means of making payments, which is practical for its users and efficient for the economy.	**General** • Define objectives (identifying risk and efficiency factors); • Identify user needs and constraints; • Identify system choices and benefits; • Determine social and private costs; • Develop decision choices; **Analytical framework** • Identify efficiency requirements (or conversely identify inefficiencies); • Identify safety requirements; • Evaluate costs (social and private); • Identify resources (social or private); • Determine practical constraints (technology, infrastructure); • Define safety constraints (e.g. applying the Core Principles).	
Access criteria		IX. The system should have objective and publicly disclosed criteria for participation, which permit fair and open access.	• Identify access criteria, if any; • Assess them for their: Justification in terms of safety, Justification in terms of efficiency. • Identify and assess exit/exclusion criteria, if any;	
Corporate governance		X. The system's governance arrangements should be effective, accountable and transparent.	Check if: • Relevant information on the system and its operations is readily available, complete and up to date; • Major decisions are made after consultation with all interested parties and due deliberation; • The high-level decision-making process is prompt and communicated clearly to the system users; • The system consistently attains projected financial results and can explain any differences from those plans; • The system delivers payment services that satisfy customer needs;	

ANNEX I - BIS CPSS CORE PRINCIPLES - ASSESSMENT AND RECOMMENDATIONS MATRIX

RELEVANT FACTORS		STANDARDS	STATUS IN THE COUNTRY[1]	RECOMMENDATIONS
			• The system complies with the other nine Core Principles.	

(*): If the system presents an element that makes it not compliant with the Principle the line should be marked in red (third column). If the system is not compliant at all with the principle the principle in the second column should be marked in red. It the system is partially compliant the principle in the second column should be marked in blue.