OVERSIGHT OF PAYMENT AND SECURITIES SETTLEMENT SYSTEMS

POLICY AND PROCEDURES

ISSUED: 5 DECEMBER 2001

TABLE OF CONTENTS

1. INTRODUCTION

The purpose of the policy and procedures is to set out the Banque centrale du Luxembourg (BCL) oversight of payment and securities settlement systems and other related mechanisms.

The competence of the BCL in this field is laid down in the circular BCL 2001/163 of 23 February 2001 ("La surveillance par la Banque centrale des systèmes de paiement et de règlement des opérations sur titres au Luxembourg").

The BCL's oversight mission, aiming to promote the smooth operation of payment and securities settlement systems and hence the stability and integrity of the financial infrastructure, can be described as being in proportion to its assessment of systemic risks or the respective level of efficiency.

The BCL considers the following to be key features of oversight in its application:

- knowledge and understanding of the various systems and their interrelationships,
- BCL recognition of important systems, operators[1] and technical agents[2],
- the application of the BIS Committee on Payment and Settlement Systems Core Principles for Systemically Important Payment Systems (hereafter Core Principles) and other recommendations and standards, relating to payment, securities settlement and other mechanisms,
- self-assessment conducted by operators and/or technical agents,
- the use of independent key functions for compliance, internal audit and risk management where relevant,
- good records and/or easy access to information when required,
- monitoring relevant changes in the business environment and assessing impact on systems as such relate to efficiency and stability and,
- the use of routine and ad hoc inspections.

2. 'SYSTEMS'

2.1. PAYMENTS

A payment system (PS) is an arrangement, which allows the users of the system to transfer funds. In today's rapidly changing financial markets, which have witnessed significant

[1] An operator is the central system organisation providing products and services.

[2] A technical agent is a supplier of service where an operator has located a significant portion of its operational or IT infrastructure or where several payment- or securities settlement-related operational or IT infrastructures are centralised.

growth and change, central banks, in the main, focus on PSs handling large-value payments. They have played an active role in the design and operation of such PSs, concentrating on the development of real-time gross settlement systems, which are considered to be the safest and most efficient PSs for large-value payments. It is widely understood that PSs are a critical component of the infrastructure of global financial markets.

Central to payment activities are the arrangements that facilitate the transfer of funds between the participants (those intermediaries which connect directly to the central operator or to each other). It is these arrangements, which constitute a PS. They include the networks, which link participants, the message routing systems, and the infrastructure contracts, rules and procedures. In particular, a PS requires:

- agreed standards for, and mechanisms of transmitting, payment messages between participants and, as such, an agreement on the technical standards of the infrastructure;
- an agreed procedure of settling claims between participants, usually in the form of a safe settlement asset and,
- commonly agreed operating procedures and rules covering, for example, admission, and fee structures.

The two main mechanisms in Luxembourg are those providing for net settlement and gross settlement and which are commonly referred to as LIPS-Net and LIPS-Gross. There are other payment mechanisms for both retail and wholesale transactions.

2.1.1. NET SETTLEMENT

LIPS-Net is a net settlement capability, which settles several times throughout the day. Sypal-Gie, the operator, an economic interest group, including banks active in domestic business, the Post Office and the BCL, is responsible for the management and development of LIPS-Net and the Centre de Transfers Electroniques (CETREL) is the technical agent. The BCL is the settlement agent.

2.1.2. GROSS SETTLEMENT

LIPS-Gross is based on a different architecture and is a real-time gross settlement capability (RTGS). RTGS-L Gie, the operator, an economic interest group, including Luxembourg-based banks and the BCL; the BCL is the technical agent and the settlement agent. It aims in particular at large-value payments and settles payments individually in an ongoing process as they are received in the system. In addition LIPS-Gross is a component of TARGET (Trans-European Automated Real-time Gross settlement Express Transfer System), enabling Luxembourg participants to exchange payments with TARGET participants, currently around 5,000, in the European Union.

2.1.3. OPMs

There are a number of other payment mechanisms[3] (OPMs), which have a direct or indirect impact on the main payment systems for gross and net settlement; these include credit card, debit card and electronic- payment and electronic-money to name a few. These mechanisms are changing as deregulation and new technologies create new solutions. Accordingly, the BCL regards these mechanisms and any developments as being important for reasons of efficiency and stability and as such these and new similar systems are subject to oversight.

2.2. SSSs – EMBEDDED, SSSs – OTHER, AND CCPs

Increasingly, national and international securities settlement and central counterparty systems are recognised as being critical components of global markets. Significant increases in securities settlement volumes, gross and net, and increasing cross-border business, raise concerns that any disruption of post-trade securities processing mechanisms has the potential to spill over to any PS used by a securities settlement system (SSS). This concern is increased when an SSS is directly engaged in funds transfer and the provision of PS-related activities in the domestic market. Further relevance it attached when such systems are engaged in fund transfer and the PS-related activities of other European System of Central Bank (ESCB) members or beyond.

The law of 1 August 2001, pertaining to the circulation of securities and other fungible instruments provides a statutory basis for book-entry clearing, settlement and custody of securities. In essence, the Clearstream Banking Luxembourg (CBL) settlement process is based on book-entry DvP in which credit risk is negated by the simultaneous exchange of cash against securities.

CBL has evolved and developed its services and today has four distinctive capabilities, providing:

- services for the transfer of collateral for monetary policy operations/TARGET liquidity,
- DvP settlement and depository, as an ICSD, for Eurobonds and other international instruments[4] as well as providing DvP settlement via links to a number of domestic markets. This includes funds transfer via cash correspondent banks in, amongst others, all EU markets (CBL also places and borrows funds in the currencies of those markets),
- DvP settlement for domestic government debt settlement,
- DvP settlement for domestic securities and,
- via Clearstream Banking Frankfurt (CBF), DvP settlement for domestic German securities.

Given these findings four distinct securities settlement channels can be identified within Luxembourg and these are securities processing:

---

[3] Other payment mechanisms are defined as those which currently exist e.g. credit and debit card, etc. or new payment- or securities settlement-related products and services which may appear in future.

[4] See Appendix 3 for explanation of cross-border settlement channels.

- in the domestic market where funds transfer is not simultaneous with securities processing,
- resulting in DvP settlement with the simultaneous exchange of funds and securities title of domestic securities,
- the transfer of collateral for monetary policy operations/TARGET liquidity and,
- DvP settlement with the simultaneous exchange of funds and securities title of internationally issued securities (including ESCB member countries).

These can be summarised to two distinct categories and these are systems:

- where funds transfer and securities transfers are embedded in the same mechanism[5] and where the BCL and/or other ESCB NCBs are participating. For the purposes of this paper these are referred to as securities settlement systems embedded with payments systems or SSSs Embedded, because they have a direct impact on PSs in Luxembourg and/or the Eurozone and,
- in which securities are processed independently from the transfer of funds, and for the purposes of this paper are described as other securities settlement systems or SSSs - Other.

2.2.1. SSSs - EMBEDDED

An SSS - Embedded is defined broadly as the full set of institutional arrangements, procedures and rules for the primary and secondary market and the confirmation, clearance and DvP settlement of securities trades (and derivatives if relevant), the safekeeping of securities and any related services. While not an exhaustive list, such arrangements include distribution, pre-settlement matching, pre-advised payments, settlement of securities against payment, securities borrowing and lending, tripartite repo, technical overdraft facilities or the mobilisation or use of securities as collateral or pledge.

Within this definition, the SSS - Embedded will:

- settles securities against funds, DvP, in EUR and/or other currencies,
- provide services for the transfer of collateral for monetary policy operations/TARGET liquidity and,
- provide services that ultimately result in the settlement of payment obligations or the adjustment of the account or accounts of one or more participant in an authorised PS.

2.2.2. SSSs - OTHER

SSSs – Other are defined as the full set of institutional arrangements, procedures and rules for the primary and secondary market and the confirmation, clearance and settlement of securities trades, the safekeeping of securities and any related services. In such systems, securities are processed independently from funds where the cash leg is settled first. Within this definition such a system must:

- have three or more participants, at least two of which are banks,

[5] Often covered by relevant law.

- ultimately result in securities settlement in EUR and,
- ultimately result in the settlement of payment obligations through adjustments to the account or accounts of one or more participant in an authorised PS.

2.2.3. CCPs

A central counterparty (CCP) is defined as the full set of institutional arrangements, procedures and rules for clearing and novation (the legal process which replaces the contract between a buyer and seller with two contracts between the buyer and the CCP and the seller and the CCP). In a CCP, the management and redistribution of counterparty risk is achieved by establishing rules on who will bear the losses that occur in case a participant will default. Within this definition a CCP must:

- have three or more participants, at least two of which are credit institutions,
- operate mechanisms which result in the redistribution of counterparty risk and which require EUR-denominated or other settlement assets to be pledged and/or settled and,
- ultimately result in the settlement of payment obligations through adjustments to the account or accounts of one or more participant in an authorised PS.

There are no clearing and central counterpary organisation or utility based in Luxembourg at this time. In the event that an operator was recognised, these policies and procedures would apply.

3. OVERSIGHT

3.1. DEFINITION

Oversight shares with prudential supervision the objective of financial stability. However, while prudential supervision conducts its surveillance at the institutional level, oversight looks at systems. In the context of the BCL oversight, the use of the term system refers to the general organisation of all categories of system in Luxembourg, their interrelationship and their relationship to similar systems in the Eurozone.

Given this, the BCL's oversight role requires the widest interpretation of system in this regard.

3.2. OVERVIEW

BCL's oversight is concerned with the integrity of the financial infrastructure and its role can be described as being in proportion to its assessment of the systemic risks posed by the various PSs and SSSs. Since the main focus is systemic risk or other factors giving rise to systemic risk, the BCL's oversight concentrates on systems, which individually or cumulatively involve large amounts of funds for payments or against payment securities settlement. Similarly oversight involves operators where the participants do, or have the potential to, incur significant involuntary exposures to one another when engaged in payment, or against payment securities settlement, activities. It is also concerned where problems could have system-wide consequences, even if the values involved do not give rise to major systemic risks. BCL oversight is essentially concerned with many different elements of risk. Such risks and the BCL's concerns need to be identified, quantified and understood by the various constituencies, which comprise the system. As well as the concern for the operator and its operational and IT infrastructure, oversight needs to involve the understanding of the legal framework governing the system. Further, oversight involves the understanding of participant contracts, operator rules, operating procedures and environment, and the reviewing of proposals for changes in same. In addition, it involves the monitoring of changes in the scale or nature of the payments, or where relevant the securities processed against payment and changes to operator management procedures.

Where necessary the BCL may propose changes to the rules, design or operational methods of an operator, or to the environment in which it provides service (e.g. the legal framework), in order to eliminate, reduce or better manage risks. A central aim is to achieve prompt final settlement, using a safe asset in order to minimise the duration of financial exposures between participants, particularly where large amounts are being processed.

Oversight must necessarily evolve to reflect changes in the business environment and the dynamics and patterns of payment and securities flows through the various operators. The growing dependence of banking and capital markets, including operators, on IT and telecommunications networks increases the potential risks which could arise in the event of the failure of computer systems and architecture. There is therefore an increased interest in this potential new source of operational risk in terms of oversight.

The BCL is not involved in nor does it monitor day-to-day operational aspects of an operator or seek to resolve day-to-day operational problems unless the BCL is itself operationally involved[6]. The role and duty of the BCL is to establish that the operator has taken all reasonable steps to ensure the robustness of their business activities.

It should be appreciated that reducing operational risk means addressing technical reliability and redundancy, back-up facilities and contingency plans, security measures and internal controls. Oversight is intended to ensure that operators recognise these issues and address them and further aim to identify common dependencies, e.g. the use of and reliance on particular technologies, which might constitute a single point of failure for a number of users. As an example the increasing reliance on outsourcing, or segregation, by use of subsidiaries (to a non-financial institution), for parts of the operator infrastructure (e.g. the use of a telecommunications network or operations provider). While there are obvious advantages to outsourcing, it carries its own risks; there may, for example, be several financial institutions, operators and technical agents, in Luxembourg, Europe and/or overseas, which use the same supplier, resulting in a potential exposure with the concentration of risk. The BCL has an interest in any concentration in the use of third party infrastructure suppliers by any constituencies involved in the system. A relevant example is S.W.I.F.T., the Belgian-based international organisation, which provides communication network services to many financial institutions, operators and their participants world-wide. Similarly, Clearstream Services (CS), which is the provider of service to CBL and CBF.

Legal uncertainty or unexpected legal judgements can increase the potential for systemic risk. In the event that the recipient of a payment is required to return funds to the payer because a court judges that the payment is not final, the recipient may have a financial exposure. So too in securities processing, settlement issues arise which give rise to legal uncertainty; legal judgements may increase the potential for risk and which may have a consequential impact on an operator. Accordingly, oversight may require that the BCL cooperates with other bodies to identify and where possible, initiate changes to Luxembourg or EU law in order to eliminate them. The implementation of the Settlement Finality Directive is a good example of such need, leading to the reduction of such legal uncertainty.

3.3. BCL OVERSIGHT

3.3.1. GUIDING AXIOMS

Oversight in its application is based on the following guiding axioms:

3.3.1.1. PRAGMATIC AND MODERN OVERSIGHT STYLE

The BCL is adopting a modern, efficient and cost effective approach to oversight.

[6] This is the case with RTGS-L Gie and LIPS-Gross and Sypal-Gie and LIPS-Net and with monitory policy operations or liquidity aspects of TARGET where CBL is involved.

3.3.1.2. TRANSPARENCY

The authorities, system constituencies and the public at large should understand the oversight process.

3.3.1.3. ACCOUNTABILITY AND CLEAR ROLES AND RESPONSIBILITIES

Each authority must be accountable for its actions, so each must have unambiguous and well-defined responsibilities. The BCL believes that the roles and responsibilities of the relevant authorities and key players should be set out in a clear and concise way.

3.3.1.4. AVOID DUPLICATION

There is a need to avoid duplication of resources; this is necessary to avoid confusion, inefficiency and wasted time.

3.3.1.5. REGULAR INFORMATION EXCHANGE

The regular exchange of information between system constituencies and authorities will ensure that all can fulfill their obligations as efficiently and effectively as possible.

3.3.1.6. KNOWLEDGE EXCHANGE

Co-operation between the BCL and the operator's and technical agent's internal and external auditor is considered appropriate for reasons of efficiency and to avoid unnecessary duplication.

3.3.1.7. CONSCIOUSNESS OF REGULATORY CREEP

The BCL is aware of the evolving nature of oversight and is conscious of the phenomenon commonly referred to as 'regulatory creep'. Accordingly, the BCL in pursuit of its oversight mission will endeavour to maintain an appropriate balance between oversight and operator and technical agent compliance costs.

3.4. OVERSIGHT OBJECTIVES

3.4.1. IN RELATION TO SYSTEMS

In the context of oversight, the use of system requires a broad interpretation. It is therefore necessary to set appropriate objectives and these are:

- the smooth operation and efficiency of payment and securities settlement systems and related mechanisms, which contributes to the integrity of the financial infrastructure,
- to identify systems and related mechanisms, whether existing or new, and recognise those systems which are subject to oversight,
- to examine and determine the relationships between constituents,
- to examine the legal and regulatory framework within which the system operates and,
- to monitor changes to the system and its constituents.

3.4.2. IN RELATION TO OPERATORS/TECHNICAL AGENTS

It is also necessary to set appropriate objectives for the oversight of operators/technical agents:

- to determine if policies, practices, procedures, and internal controls are adequate,
- to determine if members of the governing body and executive management are operating in conformance with the established guidelines,
- to determine the scope and adequacy of the audit function,
- to determine the overall quality of the legal and regulatory framework and products and services and how that quality relates to the soundness of the system,
- to determine compliance with laws and regulations and,
- to initiate corrective action when policies, practices, procedures, or internal controls are deficient or when violations of laws or regulations have been noted.

3.5. LEGAL AND PRACTICAL ASPECTS OF THE OVERSIGHT OF A SYSTEM, OPERATOR/TECHNICAL AGENT

3.5.1. BCL'S ROLE UNDER LUXEMBOURG LAW AND EU TREATIES AND PROTOCOLS

The law of 12 January 2001, implementing the EU's settlement finality directive, gives the BCL formal responsibilities for payment and securities settlement systems[7]. The BCL will have regard to financial stability (in Luxembourg and the Eurozone) in all cases when determining whether or not to include such systems, operators and/or technical agents for consideration in terms of recognition.

3.5.2. RECOGNITION

3.5.2.1. DEFINITION

Recognition is an internal mechanism of the BCL, used to facilitate the oversight process.

3.5.2.2. PROCESS

The BCL has defined the following criteria in respect of recognition of systems, operators and technical agents:

- systems in which the BCL or another ESCB NCB participates,
- systems which are of systemic importance at EU and international level, defined by the function provided by the system, importance in ESCB monetary operations, transaction volumes, value, etc.,

[7] System is defined in the widest sense as explained in 3.1. above.

- systems which are of systemic importance at the national level, defined by the function provided by the system, importance in economic, trade and public terms, transaction volumes, value, etc. and,
- systems which require to be monitored for efficiency (cost, investment, competitiveness, speed and risk).

The BCL will assess the operator's/technical agent's:

- financial resources,
- default arrangements,
- rules, which make clear certain key aspects of its business activities and,
- arrangements for monitoring and enforcing compliance with its rules.

3.5.2.3. COMPLIANCE

The BCL will review the performance of operators/technical agents with the requirements as defined by the BCL in conformance with its policy and procedures.

3.5.2.3.1. REQUEST FOR INFORMATION BY BCL OFFICIALS

In the event that BCL needs to review matters with operators/technical agents, it may issue a request for information.

3.5.2.3.2. CONCERNS/INCIDENTS

In the event that an incident occurs within the operator/technical agent, it will inform the BCL; the BCL may require explanation by the operator/technical agent or convene a meeting.

It should be noted that an incident can include such items as complaints, claims, IT systems failures, or any other situations, which could give rise to oversight requirements.

3.5.2.3.3. CORRESPONDENCE

In the event that the BCL remains concerned over such incidents or where the operator/technical agent delays or fails to take appropriate steps, the BCL may issue correspondence stating its requirements and setting a deadline for response and/or action as the case may be.

3.5.2.3.4. COMMUNICATION

In the event that the BCL is required to take formal action and given its requirement for public disclosure, the BCL may make appropriate public statements.

3.6. BCL'S ROLE IN RESPECT OF OPERATORS AND TECHNICAL AGENTS

3.6.1. ADMISSION AND TERMINATION CRITERIA

Financial risks may result from the participation of unqualified or unsound intermediaries. Access to operators/technical agents should therefore be restricted to certain categories of financial institutions, typically banks, or where other organisations are admitted their use of services provided by operators/technical agents should be explained. At the same time, public authorities have a strong interest that operators/technical agents as public utilities have access criteria that are explicitly specified and disclosed to all interested parties. Restrictions on access to operators/technical agents should be based on objective criteria, including risk criteria. Operators/technical agents should in particular take into account the financial and legal soundness of the applicant.

The rules and procedures should also provide for the orderly termination of participation, at the request of a participant and for the exclusion and/or suspension of a participant.

3.6.2. CORPORATE GOVERNANCE

Governance arrangements are the rules and procedures governing the relationships between the operator's/technical agent's management, its governing body, its owners and other relevant stakeholders.

The BCL is interested in such rules and procedures since they constitute the structure through which the operator's/technical agent's objects are set, how they are achieved and how performance is monitored.

3.6.2.1. ACCOUNTABILITY AND TRANSPARENCY

The operator's/technical agent's governance arrangements should be effective, accountable and transparent to the owners, stakeholders and participants in order to allow all interested parties to have access to information about decisions affecting business activities and how they are taken.

3.6.2.2. MANAGEMENT, ADMINISTRATION AND CONTROL

Members of the governing bodies should be able to demonstrate their professional respectability. Governance arrangements should provide for objective and independent control over management, which must be exercised by at least two persons who are authorised effectively to determine general business policy and where appropriate for the day-to-day operations of operators/technical agents. These persons shall have the stature and necessary professional experience.

The BCL should be informed in advance of any nomination, departure or change in rank of the aforementioned members (governing body and management) and may request all necessary information concerning the professional respectability and experience of these members.

Further, all legal cases brought against the operator/technical agent should be notified to the BCL.

3.6.2.3. OWNERSHIP

The operator/technical agent must inform the BCL of the identities of its owners or members, whether direct or indirect, whether physical persons or legal entities, and keep this information updated. The operator/technical agent should further inform the BCL of any major changes in its corporate structure.

An operator/technical agent, proposing to acquire participating interests in a legal entity, directly or via a subsidiary should first inform the BCL.

3.6.3. ORGANISATION

The BCL places significant reliance on operators/technical agents to ensure that risks are properly and widely defined, understood and communicated. Accordingly the BCL requires that specific functions be established for risk management, compliance and internal audit where relevant and that such functions have the resources, experience and are empowered to achieve their respective tasks.

3.6.3.1. COMPLIANCE

The compliance officer stands at the crossroads between auditing, internal control and management's legal responsibilities, and is to some extent the guardian of operator/technical agent code of conduct. The compliance officer acts completely independently and is responsible for supplying operator/technical agent executive management with all the necessary information on whether their decisions comply with the law, the professional rules and regulations and with the internal policies and procedures or with those of the regulatory authorities.

3.6.3.2. INTERNAL AUDIT

Internal audit is an independent function within the operator/technical agent with the purpose of examining the risks the operator/technical agent faces, to review the adequacy of controls in place to protect it from those risks, and to verify that the internal controls are working as intended.

3.6.3.3. RISK MANAGEMENT

The purpose of the risk management function is the systematic and comprehensive identification, compilation, limitation and control of all risks the operator/technical agent is exposed to by virtue of its activities. This process includes the parent and subsidiary, branch and representative offices where such have a bearing on risk and potentially an impact on payment and payment-related systems and financial stability.

3.6.4. EXTERNAL AUDIT

The operator/technical agent must assign the task of auditing the annual accounts to a duly licensed external auditor. The external auditor has to be appointed by the governing body of the operator/technical agent. The BCL should be informed in respect of auditor selection or change prior to formal approval.

3.7. MECHANISM FOR AVOIDING REGULATORY CREEP

It is recognised that oversight and prudential supervision can result in direct costs for the operator/technical agent. Authorisation procedures, inspections and interviews as well as reporting requirements take up management time and may be regarded as a business cost for an operator/technical agent. In a globalising market, risks can change in nature and significance and there is a danger that regulators will demand more and more information with subsequent increase in cost for the operator/technical agent. The BCL recognises this phenomenon commonly referred to as 'regulatory creep'. Accordingly, the BCL in pursuit of its oversight mission will endeavour to maintain an appropriate balance between oversight and operator/technical agent cost. In essence, the operator/technical agent, which is responsible for the definition, analysis, monitoring and control of risks, will ensure the following:

- risks are clearly defined, monitored controlled and managed,
- responsibilities for risk categories are assigned,
- appropriate procedures are in place and training given as appropriate,
- appropriate reporting is defined and reports made available in electronic or physical form on the dates agreed. Wherever possible exception reporting techniques may be considered,
- changes in the operator/technical agent, in terms of governance, location, diversification, outsourcing, operating procedures, management, among others will be advised in advance to the BCL,
- new risks or business exposures and procedures for mitigating same will be advised to the BCL and,
- in pursuit of its oversight mission, the BCL will call on all means of control and monitoring it deems fit; this particularly during significant environmental change or adverse market conditions.

3.8. SPECIFIC EXAMPLES OF MEANS OF CONTROL AND MONITORING

In order to enable the BCL to fulfil its oversight mission, aiming at ensuring the smooth functioning of systems, the following should be regarded as indicative of requirements rather than an exhaustive list:

- the operator/technical agent should provide the BCL with all documents and figures which the BCL may request in the context of its oversight mission,
- the BCL may ask the operator/technical agent for a regular and/or ad-hoc statistical and oversight reporting in relation to his activities,
- the operator/technical agent should allow the BCL to proceed to on-site inspections at the location [offices]of the operator/technical agent,
- the operator/technical agent should submit to the BCL on request certain types of documents or communications prior to public disclosure,
- the operator/technical agent should submit to the BCL its rules and procedures and any subsequent changes,

- the BCL may ask the operator/technical agent to extend the mandate of the external auditor, in relation to the assessment of the annual accounts, to aspects of the soundness and the efficiency of the operator/technical agent and report on it in the auditors long form report,
- the operator/technical agent shall provide the BCL with the reports, analytical and interim reports and written observations issued by the external auditor,
- the BCL may ask the operator/technical agent to provide legal opinions on specific aspects to be defined by the BCL,
- the BCL may ask an operator/technical agent to provide external (auditor) reports in respect of the activities and/or the functioning of such an operator/technical agent,
- the costs related to the external (auditor) reports and the provision of legal opinions should be at the sole expenses of the operator/technical agent,
- the BCL requires to be informed, by the operator/technical agent, of all major operational changes. It may request to inspect the books, accounts, registers and all other deeds and documents of the operator/technical agent, including management letters and internal audit reports and,
- the BCL requires to be informed about all operational incidents.

3.8.1. INFORMATION GATHERING AND EXCHANGE

The BCL will obtain and exchange information on and with operators/technical agents via information supplied, reports and meetings.

3.8.2. BCL USE INSPECTIONS

Whereas, the oversight process can be regarded asone of self-assessment conducted by the operator/technical agent, the BCL may:

- arrange meetings with the operator's/technical agent's compliance, internal audit and risk management functions and,
- use routine and ad hoc inspection in the event of, for example, an infringement or unforeseen event.

3.8.3. BCL REQUIREMENTS IN RESPECT OF EXTERNAL AUDITOR

The BCL may ask operators/technical agents to provide external (auditor) reports in respect of the activities and/or the functioning of such an operator/technical agentand to include particular items during routine or ad hoc audits or reviews.

3.8.4. BCL REQUIREMENTS IN RESPECT OF LEGAL OPINION

In such circumstances as needs dictate the BCL may ask the operator/technical agent for an independent legal opinion. Such opinions may be required in respect of system requirements where such relates to an operator/technical agent, or be in connection with a specific product or service, contract or agreement or other such factor. The provision of such legal opinion will be at the sole expense of the operator/technical agent.

4. THE SYSTEM

The system is defined as having five distinct components and these are the:

- the operator,
- participants,
- technical agents and suppliers,
- rules and contracts and,
- legal and regulatory environment.

4.1. THE SYSTEM - BCL OVERSIGHT

4.1.1. LIST OF RECOGNISED OPERATORS AND TECHNICAL AGENTS

The BCL maintains a list of recognised systems, operators and technical agents and will maintain up to date information on them. See Appendix 1 for list.

4.1.2. RECOGNISED OPERATOR'S LIST OF PARTICIPANTS

Participant lists should be updated by the operator and sent to the BCL on request.

4.1.3. RECOGNISED TECHNICAL AGENT'S LIST OF PARTICIPANTS

Participant lists should be updated by the technical agent and sent to the BCL on request.

4.1.4. SUPPLIERS

Lists of uppliers deemed to be providing essential services in the conducting of an operator's/technical agent's business should be provided to the BCL on request. Suppliers include cash correspondent and depository banks, other securities settlement systems, central securities depositories, important suppliers of IT hardware or architecture services, or other financial intermediaries as used by the operator/technical agent. Suppliers' lists should be updated and sent to the BCL on request.

4.1.5. CONTRACTS AND RULES

Contracts necessary for the efficient functioning of the operator/technical agent e.g. contracts with participants, suppliers, insurance companies and guarantor syndicates and IT hardware or architecture providers, among others should be provided to the BCL on request.

Rules include procedures, which govern the efficient functioning of the operator/technical agent and include participants' handbooks, product and services instructions, and suppliers' operating manuals among others to be advised by the operator/technical agent.

Rules and contract information will be supplied in an updated form on request to the BCL.

4.1.6. LEGAL AND REGULATORY ENVIRONMENT

The BCL maintains records pertaining to the legal and regulatory environment in Luxembourg, European Union, etc.

In the event that the operator's/technical agent's legal and regulatory environment extends beyond the above mentioned areas, the operator/technical agent may be required to provide:

- lists of all such legal and regulatory environments and,
- legal opinion that operator/technical agent rules and contracts as defined and listed above comply with requirements in those legal and regulatory environments and that such are enforceable in event of a claim or dispute.

5. OPERATORS AND TECHNICAL AGENTS

The operator is the central organisation, providing products and services to participants, often using technical agents and suppliers and operating in a legal and regulatory environment which can be wider than the home state, e.g. the Eurozone.

Technical agents are deemed to be important for reasons of efficiency or stability and as such subject to oversight. A technical agent is a supplier of service where an operator has located a significant portion of its operational or IT infrastructure or where several payment- or securities settlement-related operational or IT infrastructures are centralised.

For operators/technical agents, particular emphasis is placed on admissions, governance, products and services, IT, risk and risk mitigation, business continuity and external audit.

5.1. ADMISSION AND TERMINATION CRITERIA RELATING TO PARTICIPANTS

5.1.1. ADMISSION

Operator/technical agent access criteria should encourage competition between participants, without compromising operator/technical agent safety. Acceptance criteria should be based on:

- the provision of a level playing field and,
- creditworthiness of the institution where relevant.

Restricting access should be assessed by:

- safety,
- efficiency and,
- commercial reality.

5.1.2. TERMINATION

In the event that a participant's access to the operator/technical agent is to be terminated at the request of the participant or for non-compliance, this must be done in an orderly way.

5.2. GOVERNANCE

Governance is an important mechanism in the efficient operation of private and public sector entities. For systemically important systems and the operators/technical agents, which support them, effective, accountable and transparent governance is particularly important. This is because:

- there are normally only a few such entities in a country,
- the services they provide involve high values or,
- they give rise to interdependence among participants.

Governance issues will be different dependent upon whether operators/technical agents are:

- owned and/or operated by the BCL,
- privately owned, or
- jointly owned.

These points and others are covered in more detail in the following sections.

5.2.1. ACCOUNTABILITY AND TRANSPARENCY

The governance arrangements should be effective and key consideration should be given to transparency, accountability and objective and independent oversight and control over management.

5.2.1.1. ACCOUNTABILTY

The following requirements are to be met. The operator/technical agent should have:

- explicit strategic objectives and plans for achieving them,
- regular meetings of the governing body,
- audit, compliance and risk management functions, independent of management responsible for day-to-day operations,
- design of risk management (rules and procedures) and,
- design of internal control systems.

5.2.1.2. TRANSPARENCY

The following requirements are to be met in respect of the operator/technical agent. Public disclosure of:

- bye-laws,
- details of governing body (size, membership, qualifications and experience),

- executive management structure with clear lines of responsibility and accountability within the organisation and appropriate management controls, together with arrangements for their enforcement,
- basic organisation structure (functions and hierarchy),
- published annual report,
- detailed information on products and services,
- media releases and other information and,
- information via a web site where possible.

5.2.2. GOVERNING BODY

The governing body of an operator/technical agent should be accountable to its owners and to the wider community of participants and this means justifying major decisions and actions to these parties. It is important that those served by the operator/technical agent should be able to influence its overall objectives and performance. Representation on the governing body is one such means. Privately owned operators/technical agents may have a governance structure resembling that of a cooperative, with the governing body drawn from the owners, participants or suppliers (in some cases the same financial institution is owner and customer of, and supplier to, the operator). Operators/technical agents owned by participants may need to make special efforts to seek the views of a wide range of users, particularly if a small number of large participants or owners dominate the decision making process because of voting rules being attached to transaction volumes or values. In such situations governance arrangements may need to give special consideration to the role of small participants.

Shareholders or participants often nominate members of the governing body and as such they may have conflicts of interest in the execution of their duties because:

- they represent organisations that compete with other owners, participants or suppliers and,
- the interests of the operator/technical agent may not coincide with those of the member of the governing body's employer.

Members of a governing body are placed in a position of trust by the operator's/technical agent's owners, and this is covered by Luxembourg law. The governing body is responsible for safeguarding the interests of the operator/technical agent through the lawful, informed, efficient, and able administration of the institution. In the exercise of their duties, members of the governing body are governed by Luxembourg law in respect of operator/technical agent business activities, as well as by common law, which imposes a liability on directors of all organisations.

A governing body of an operator/technical agent may include one or more advisory directors. Advisory directors generally do not vote but may provide additional information or advice to the voting members of the governing body. Given this, it is important that the governing body of the operator/technical agent meets the following requirements:

- the governing body's role and responsibilities should be clearly set out in the bye-laws and/or in additional information supplied to the owners,

- the governing body should appoint a chairperson and one or more deputy,
- the governing body shall comprise appropriately qualified and experienced directors,
- the members of the governing body shall sit as individuals and act in the best interests of the operator/technical agent,
- members should be appointed for a specified period,
- the members of the governing body are required to exclude themselves from debates and decisions where they have or could be perceived to have a conflict of interest and,
- the members of the governing body should represent the interests of the participants as well as the owners.

5.2.2.1. AUDIT COMMITTEE

Where appropriate operators/technical agents may choose to constitute an audit committee as part of its governance. In such cases, the audit committee monitors compliance with operator/technical agent policies and procedures, and reviews internal and external audit reports.

5.2.2.2. NOMINATION OF MEMBERS TO THE GOVERNING BODY

The initial members of the governing body are elected by the shareholders at a meeting held before operators/technical agents are authorised to commence business. Thereafter, in the event of a vacancy, the position is filled at the next general meeting. General meetings are to be held at least annually on a day specified in the operator/technical agent by-laws. The directors hold office for a stated tenure until their successors are nominated.

Various laws govern the election, number, qualifications, liability, and removal of members of the governing body, as well as the disclosure requirements for members outside business interests.

The following is required:

- a formal nomination process is to be used to screen candidates for membership of the governing body,
- there should be criteria for nomination to membership of the governing body, including specific requirements, and where relevant, criteria which would define ineligibility for membership, e.g. a person responsible for the participant or supplier relationship with the operator/technical agent and,
- The owners approve nominations and therefore voting arrangements should be subject to appropriately documented procedures.

5.2.2.3. MEMBERS OF THE GOVERNING BODY'S DUTIES AND RESPONSIBILITIES

The type and degree of supervision required of a governing body, in ensuring operators/technical agents are soundly managed, involve reasonable business judgment and competence and sufficient time to become informed about operator/technical agent affairs. Members of the governing body ultimately are responsible for the soundness of operators/technical agents. If negligence is involved, a member may be personally

liable. The responsibility of members to supervise operator's/technical agent's affairs may not be delegated to the active executive management or anyone else where such are deemed necessary. Members may delegate to executive management certain authority, but not the primary responsibility of ensuring that the operator/technical agent is run in a sound and legal manner.

The member's role is to provide a clear framework of objectives and policies. This framework is often accomplished through the use of strategic plans and budgets. The strategic plan would discuss long-term, and in some cases, short-term goals and objectives as well as how progress toward their achievement will be measured. The objectives and policies should cover all areas of operator's/technical agent's business activities. The governing body is responsible for establishing the policies that govern and guide the day-to-day activities of operators/technical agents, so they should review and approve them from time to time. These policies are primarily intended to ensure that the risks undertaken by the operator/technical agent are prudent and are being properly managed. This means that the governing body must have a fundamental understanding of the various types of risks associated with different aspects of operator/technical agent business e.g. credit risk, liquidity risk, or operational risk, and define the types of risks operators/technical agents will undertake. Some of the more important areas in which policies and objectives must be established include investments, lines of credit, lending, asset and liability management, profit planning and budgeting, capital planning, and personnel. Members are also responsible for implementing policies and procedures required by law or regulation, such as Bank Secrecy.

In particular, members of the governing body should:

- have a clear understanding of their obligations and liabilities,
- have sufficient expertise and integrity and ensure that there are experienced staff in key positions,
- ensure that adequate policies, practices and procedures related to the different activities of the operator/technical agent are established and complied with including;
    - the promotion of high ethical and moral standards,
    - systems that accurately identify and measure all material risks and adequately monitor and control such risks,
    - adequate internal controls, organisation structures and accounting procedures,
    - the evaluation of the quality of assets and their proper recognition and measurement,
    - 'know your customer' rules that prevent the operator/technical agent being used intentionally or unintentionally by criminal elements and,
    - the promotion of a positive attitude in respect of control functions,
- ensure that appropriate management control systems are established,

- ensure that statutory and regulatory directives, including directives regarding solvency and liquidity are observed,
- ensure that the interest of depositors and other creditors as well as owners are observed,
- have clearly stated duties and responsibilities in written form and, where remuneration is provided for, such duties and responsibilities should be a part of a formal contract and,
- provide a list of directorships in other organisations.

5.2.2.4. DAY-TO-DAY MANAGEMENT

Privately owned operators/technical agents may have a co-operative style governance structure, with the governing body drawn from the owners, participants or suppliers. In such circumstances the governing body meets only occasionally and is not directly involved in the day-to-day management of the operator/technical agent. Where relevant, one of the governing body's most important duties is to select and appoint officers qualified to administer operators'/technical agents' affairs effectively and soundly.

Where relevant, the governing body will ensure the following:

- power is delegated to at least two managers with equal powers,
- the management is fit and proper to administer the day-to-day affairs and activities of the operator/technical agent,
- the management's duties and responsibilities are clearly stated,
- management at all levels are appropriately qualified and supervise the operator/technical agent competently,
- where relevant management contracts and remuneration are approved by the governing body,
- budgets are prepared and submitted to the governing body for approval,
- duties and responsibilities or decision-making limits, e.g. spending and investment which are not part of the delegated authority are clearly stated and,
- relevant and appropriate policies, e.g. finance, human resources, IT, etc., are in place having been approved by the governing body.

5.2.2.5. CHANGES TO EXECUTIVE MANAGEMENT

The governing body is also responsible for removing officers who do not meet reasonable standards of honesty, competency, executive ability, and efficiency. The responsibility for selecting executive management also entails retaining them and ensuring that competent successors can be promoted or hired to fill unanticipated voids.

Executive management resigning from an operator/technical agent should be subject of exit interviews by the governing body to establish the reasons for their departure.

Changes to the executive management require to be approved by the governing body.

5.2.2.6. AWARENESS OF THE FINANCIAL CONDITION AND MANAGEMENT POLICIES

A management information system (MIS) provides the information, necessary to manage an operator/technical agent effectively. MIS should have clearly defined guidelines, policies, practices, standards, and procedures for the operator/technical agent, which should be incorporated in the development, maintenance, and use of MIS throughout the operator's/technical agent's organisation.

All levels of operator/technical agent management and staff use MIS to monitor various aspects of operations, up to and including its overall risk-management process. Therefore, MIS should be supportive of operator/technical agent long-term strategic objectives. At the other extreme, everyday financial accounting systems also are used to ensure that basic control is maintained over financial record keeping activities. Since numerous decisions are based on MIS reports, appropriate control procedures must be set up to ensure that information is correct and relevant.

5.2.3. OWNERSHIP

Operator/technical agent ownership structures are often different.

It is important that an operator/technical agent provides fair and open access, and as such it is important that owners with significant stakes are not able to gain undue advantage in terms of the business affairs or activities of the operator/technical agent.

The operator/technical agent will maintain lists of owners or members, whether direct or indirect, whether physical persons or legal entities, and keep this information updated. As such the operator/technical agent should provide the BCL with:

- regular and updated lists of direct owners or members,
- list of owners of all institutions with a stake of 10% or more in the operator/technical agent and,
- any changes in its corporate structure in term of direct or indirect owners.

5.2.4. PARENT COMPANY AND SUBSIDIARIES

The legal structure of an operator/technical agent can take on different forms, it may have a single legal entity and location or it may have several categories of legal entity in several countries. It is important that the legal structure is transparent, particularly setting out arrangements where different legal entities are interdependent e.g. subsidiaries where one is the supplier of service to one or more subsidiaries in the same group.

In particular the operator/technical agent should have in updated form and available to the BCL on request:

- a description of all legal entities, their status (e.g. bank, service provider, branch, representative office, shell company, etc.),
- owners and percentage stake,
- where there is an interdependence, what services are provided, pricing mechanisms

deployed, investment arrangements, e.g. IT hardware and software, premises, risk and risk mitigation procedures etc.,

- list identifying person(s) responsible for each legal entity,
- relevant information pertaining to the legal establishment of each legal entity, date established, operational date if different to date of establishment, business license number or other identifiers and,
- nature of business, and parameters appropriate to gauging size of each entity e.g. headcount, business statistics, accounts, etc.

5.3. PRODUCTS AND SERVICES

5.3.1. CURRENT PRODUCTS AND SERVICES

Operators/technical agents may offer a range of products and services (these include added value and risk elimination or mitigation) to participants. Products and services provided by the operator/technical agent should be well documented and clearly describe what is being offered to ensure that participants understand their obligations, e.g. instruction cut-off times or deadlines, the operator's/technical agent's obligations e.g. issue of reports and information, the fee structure and other relevant information. This information can be in several forms.

In particular the operator/technical agent should have in updated form:

- clear product and service documentation,
- understandable agreements for their use,
- transparent fee schedules or price lists and billing information,
- user friendly participant handbooks or operating manuals and,
- participant training programmes.

5.3.2. NEW PRODUCT REVIEW

The policies of an operator/technical agent should also provide for effective review of any new products being considered. An operator/technical agent should not acquire a meaningful position in a new product or service until executive management and all relevant personnel[8] understand the product and can integrate it into the risk measurement and control systems of the operator/technical agent.

In particular the operator/technical agent should:

- have policies which define the terms 'new product' and 'meaningful position' consistent with its size, complexity, and sophistication,
- include efficiency initiatives such as straight-through processing (STP),
- not be hesitant to define an instrument as a new product e.g. adding a new equity or

[8] Including those in internal control, legal, compliance, risk management, accounting, and auditing functions.

bond settlement link. Small changes in the current product service e.g. change in instruction processing deadlines or settlement time-scales can greatly alter their risk profiles and may justify designation as a new product,

- analyse all of the relevant risks involved in an instrument and assess how well the product or activity achieves specified objectives,
- include a description of the relevant accounting guidelines and identify the procedures for measuring, monitoring, and controlling the risks involved and,
- integrate new products fully into current products.

5.4. IT

The growing dependence of banking and capital markets, including operators/technical agents, on IT and telecommunications networks increases the potential risks which could arise in the event of the failure of computer systems and architecture. There is therefore an increased interest in this potential new source of operational risk in terms of oversight.

In particular the operator/technical agent should:

- have good documentation and change management procedures,
- adopt and implement relevant, international, national and industry level standards, guidelines and recommendations wherever possible,
- have adequate numbers of well trained, competent and trustworthy staff and management,
- ensure adequate training in respect of business requirements, operational needs and risk management in both normal and abnormal situations,
- ensure that the implications for security and operational reliability are well understood and addressed. This is particularly relevant where new technologies are deployed e.g. TCP/IP, private IP networks and public internet,
- protect intellectual property rights, or ensure adequate user rights, particularly when using third party contractors or suppliers and,
- ensure adequate screening of staff, contractors and consultants and put in place appropriate supervision and checks on quality with regard to robustness and security.

5.5. RISK AND RISK MITIGATION

The processing of instructions by a securities processing and funds transfer mechanism often involves several stages during which the rights and obligations of the buyer and the seller are significantly different. At the stage at which the transfer becomes final, that is, an irrevocable and unconditional transfer, the obligation is discharged. Final transfer of a security by the seller to the buyer constitutes delivery, and final transfer of funds from the buyer to the seller constitutes payment. When delivery and payment have occurred, the settlement process is complete.

Many settlement systems have associated registries in which ownership of securities is listed in the records of the issuer. Registrars typically assist issuers in communicating with

securities owners about corporate actions, dividends, and so forth. Securities may be registered in the name of a broker-dealer or custodian rather than that of the ultimate investor. The efficiency of the registration system has implications for the clearing and settlement process because it determines the ease and speed with which full legal title to securities can be transferred. Full legal title may not be obtained until ownership is listed in a registry, and thus finality in the settlement process may not be achieved until registration is complete.

It is therefore essential to fully understand risks[9] arising in the payment and securities settlement process, particularly when the operator/technical agent uses multiple suppliers and contractual arrangements for funds transfer and securities deliveries in non-domestic markets, involving several legal and regulatory environments.

5.5.1. RISK ANALYSIS

The following categories are relevant to the analysis and understanding of risks:

- participant involvement,
- supplier involvement,
- the products and services provided (including operational and IT infrastructure),
- the rules and contracts used and,
- the legal and regulatory environment.

5.5.2. RISK MITIGATION

Risk mitigation procedures require to be documented for each risk category and should include:

- the description of risk mitigation procedures in relation to the categories described in 5.5.1. above,
- known exposures,
- persons responsible for particular categories of risk,
- risk limits and approval process (including escalation procedures) and,
- mechanism by which risk and risk mitigation process is reviewed e.g. in respect of ongoing risk reduction programmes, new products or services, IT, contract changes, etc.

5.5.3. CREDIT RISK

Credit exposures between participants arise in an operator/technical agent in which there is a delay between the receipt of cash and final settlement by the operator/technical agent and the delivery of securities with good title. It is necessary therefore to ensure that risks are clearly understood by participants, the operators/technical agents and suppliers where relevant.

[9] See definitions of risk in Appendix 3.

The following points require particular attention and explanation if required:

- where the use of the settlement asset is other than central bank money,
- the use of and arrangements with cash correspondent banks where required,
- the granting and administration of lines of credit and overdraft facilities where used,
- the use of and arrangements with depository banks where required,
- the use of and arrangements with PSs, payment-related or other similar mechanisms such as SSSs and/or CCPs where required,
- granting and administration of securities lending for fails management and other uses where used,
- primary market distribution and mechanisms and,
- conflicts of law or contestable contractual arrangements with participants and/or suppliers, e.g. cash correspondents, depository banks, etc.

5.5.4. LIQUIDITY RISK

Liquidity problems have the potential to create systemic problems, particularly if they occur at a time when securities prices are changing rapidly and failures to meet obligations when due are more likely to create concerns about solvency. In the absence of a strong linkage between delivery and payment, the emergence of systemic liquidity problems at such times is especially likely. The fear of a loss of the full principal value of securities or funds could induce some participants to withhold deliveries and payments, which, in turn, may prevent other participants from meeting their obligations.

The following points require particular attention and explanation if required:

- if the operator is not based on DvP or where the DvP mechanism is contestable how are such risks managed and what is the potential for failure and,
- if the operator is based on DvP are arrangements sufficiently robust, e.g. where cash correspondent or depository banks or contractual arrangements with other suppliers are required?

5.5.5. RISK OF SUPPLIER BANK FAILURE

In addition to the risks associated with counterparties, participants in an operator may face the risk of a cash correspondent or depository bank failure (if used by the operator). The failure of any supplier that provides cash accounts to settle payment obligations or which administers securities for participants could disrupt settlement and result in significant losses and liquidity pressures for those participants. The impact on participants would be particularly severe if all participants were required to use the same supplier of service to the operator/technical agent.

The following points require particular attention and explanation if required:

- in the event that the operator uses cash correspondent or depository banks are participants required to use a single supplier,
- how is the operator/technical agent and its participants impacted by failure of

insolvency of a supplier and,

- what contingency arrangements exist?

5.5.6. CUSTODY RISK

Risk may arise from the safekeeping and administration of securities and financial instruments on behalf of others. Users of custodial services face risk from the potential loss of securities in the event that the holder of the securities becomes insolvent, acts negligently or commits fraud.

The following points require particular attention and explanation if required:

- where securities are administered domestically does the operator/technical agent conduct physical checks,
- where securities are administered in another country by a locally based SSS – Embedded, SSS – Other, CSD or by a depository bank, what arrangements are made to protect the operator/technical agent and its participants from negligence, fraud or insolvency,
- where securities are administered non-domestically does the operator/technical agent conduct physical checks,
- are arrangements for administering securities contestable (in the event of negligence, fraud or insolvency) from a legal or contractual point of view and,
- are quality checks carried on suppliers and what arrangements are made for improvement, corrective action or replacement?

5.5.7. OPERATIONAL RISK

Operational risk is the risk of unexpected losses as a result of deficiencies in operational and IT infrastructures, internal controls, human error and management failure. It can reduce the effectiveness of other measures the operator/technical agent takes to manage risk, for example by impairing the ability of the operator/technical agent to complete settlement, perhaps creating liquidity pressures for itself or its participants, or by hampering the ability of the operator/technical agent to monitor and manage its credit exposures. Possible operational failures include errors or delays in processing, IT computer and communications outages, insufficient capacity or fraud by staff.

The following points require particular attention and explanation if required:

- what mechanisms are in place to monitor operational and IT infrastructure performance and how are outages analysed, reported and recorded,
- are cut-off times met and how if used are concessions granted and approved,
- do delays in IT or operational infrastructure processing take place and how are they analysed, reported and recorded,
- is the operational and IT infrastructure capabilities scaleable, what limits are defined and what action is needed to extend them e.g. to double the capability of the IT or operational capability,
- are operating procedures documented and subject to change controls,

- are participant instructions authenticated or are procedures established to allow for alternative mechanisms to be used in event of failure,
- are instructions taken by telephone or general fax and if so how are they authenticated,
- are operating rules as set out in participant literature, operating manual, handbooks, agreements, etc. strictly adhered to and where concessions are granted how are such approved and recorded,
- what manuals of procedure are available to staff and is training given,
- what mechanisms are used to prevent fraud,
- are records of errors kept,
- do claims arise and are there procedures for administering, analysing, reporting and recording them and,
- when staff are recruited are security checks carried out.

5.5.8. LEGAL RISK

Legal risk is the risk that a party will suffer a loss because laws or regulations do not support the rules of the operator/technical agent, the performance of related settlement arrangements, or the property rights and other interests held. Loss and legal risk can also arise if the application of these laws and regulations is uncertain. For example, legal risk encompasses the risk a counterparty faces from an unexpected application of a law that renders contracts illegal or unenforceable. It includes the risk of loss resulting from a delay in the recovery of funds or securities or a freezing of positions. In a cross-border context, the laws of more than one jurisdiction apply or can potentially apply to a transaction, conduct or relationship. Counterparties may face loss resulting from the application of a different law than expected, or had specified in a contract, by a court in a relevant jurisdiction. Legal risk thus exacerbates other risks, such as market, credit or liquidity risk, relating to the integrity of transactions.

The following points require particular attention and explanation if required:

- where the operator/technical agent provides settlement, custody, safekeeping services in non-domestic legal and regulatory environments have conflicts of law been thoroughly evaluated to eliminate the potential for contesting contractual arrangements with participants and/or suppliers, e.g. cash correspondents, depository banks etc. and,
- are contractual arrangements contestable in the event of negligence, fraud or insolvency from a legal or regulatory point of view?

5.5.9. SYSTEMIC RISK

Systemic risk is the risk that the inability of one institution to meet its obligations when due will cause other institutions to fail to meet their obligations when due. The possibility that the liquidity and credit problems precipitated by these failures to perform will disrupt financial markets and impair the functioning of payment and settlement operators/technical agents is of particular concern. An operator/technical agent can create significant credit, liquidity and other risks for its participants. PSs, SSSs - Embedded and SSSs – Other or other financial institutions often depend critically on an

operator/technical agent because of their use of securities as collateral in their own risk management procedures.

Market liquidity in securities markets is dependent on confidence in the safety and reliability of an operator/technical agent because traders will be reluctant to deal if they doubt that the trade will settle. Thus it is important that operator/technical agent mechanisms be appropriately risk managed in order that such are not a source of systemic disturbances to securities markets and other payment and settlement operators/technical agents.

The following points require particular attention and explanation if required:

- how does the operator/technical agent assess issues arising that could lead to systemic risk, e.g. operational and IT infrastructure failure, loss of suppliers, major fraud, etc. and,
- is the operator/technical agent aware of participant arrangements in event that critical failure or natural disaster impacts the operator/technical agent?

5.5.10. FINANCIAL RISK

Financial Risk - The ability of the operator/technical agent to be financially viable. This risk concerns the financial strength of operators/technical agents and if its capital is sufficient to meet the on-going operational and strategic investment needs of the participants, markets and other organisations.

The following points require particular attention and explanation if required:

- are costs managed and investment decisions subject to good housekeeping and business practices,
- are there vulnerabilities, e.g. participant revenues may be vulnerable to business changes, competition, market efficiencies, participant cost-cutting,
- does the operator/technical agent evaluate the impact of alternative business scenarios, e.g. bear market, loss of key customers, significant investment caused by business volume increase (scalability can be expensive where system is near limits) and,
- does the operator/technical agent have access to funds in times of need.

5.5.11. HUMAN RESOURCE RISK

The nature of operator/technical agent activities requires specialist knowledge in certain areas of business e.g. management, legal, operations and IT management and staff. In order to ensure an adequate knowledge base at all times, staff retention, training, succession plans and formalised procedures (for knowledge exchange) form an essential requirement of the business activities of the operator/technical agent. Any sudden or prolonged and significant loss of management or experienced staff gives rise to an increased potential for operational risk.

The following points require particular attention and explanation if required:

- are qualified resources readily available and able to be attracted if needed,

- are remuneration and benefit packages competitive,
- is the operator/technical agent impacted by business changes, e.g. severe competitive pressures, market downturn, loss of business, mergers, etc., which give rise to problems of morale, high absenteeism or above normal staff turnover,
- are procedures and other relevant documentation (management, operational, and IT) for knowledge exchange comprehensive and up to date,
- are statistics available which measure the experience base (length of experience of staff leaving versus new starts), recruitment performance, open positions, staff turnover, reasons for leaving, dismissals etc. and,
- does the operator/technical agent have effective staff and management training programmes?

5.5.12. REPUTATIONAL RISK

Given its role, the good reputation and standing of an operator/technical agent is essential to the safeguarding that of Luxembourg (and the Eurozone). It is essential that operators/technical agents conform to best practice and project an image of integrity and stability. Accordingly an operator/technical agent should adhere to international standards, working closely with and supporting industry groups and standards committees.

The following points require particular attention and explanation if required:

- does the operator/technical agent have a good standing and enjoy a good reputation,
- what steps does the operator/technical agent take to maintain and/or build its reputation,
- how is the operator/technical agent perceived by its participants, suppliers, media, regulators, etc.,
- what mechanisms and procedures are used by the operator/technical agent to maintain/build its reputation,
- has the operator/technical agent suffered from situations that have damaged its reputation and what corrective actions were taken and to what effect and,
- does the operator/technical agent use mechanisms to measure its standing and reputation, e.g. media coverage analysis, participant questionnaires, surveys, etc?

5.6. BUSINESS CONTINUITY

The purpose of the business continuity arrangements of an operator/technical agent is to strive to ensure that service levels are met in the event of one or more components (operational units, premises, hardware, software, etc.) failing. It is important to establish plausible scenarios for failure and plans and procedures and carry out formal exercise. Such scenarios could include failure of each of the central components of the operator/technical agent, those of participants and any infrastructural services used. External and internal threats should be reviewed and the impact assessed.

In particular the operator/technical agent should:

- set and review the operational and IT infrastructure security objectives and policies,
- identify the operational and IT infrastructure's functions, components, boundaries and areas of responsibility, identify possible threats, and their magnitude (impact and likelihood),
- identify existing or potential safeguards (such as physical devices, security software and organisational or operational procedures),
- identify any residual risks and vulnerabilities,
- constantly review update securities policies and objectives,
- implement appropriate safeguards as identified by the risk analysis process,
- use of fault tolerant or duplicated hardware,
- conduct regular preventative maintenance of all relevant computer and telecommunications components,
- make available on-site supplies of spare hardware and telecommunications components,
- use internally generated or uninterrupted power supplies and an independent water supply, fire detection and extinguishing systems,
- have available clear and up-to-date documentation of procedures and technical documentation at the prime and any contingency sites, procedures for taking regular copies of data, and copies of software when it is changed, critical components of which should be stored off the prime site,
- have procedures for the exchange of data by physical media (disks, tape, paper) in the event of a telecommunications failure, procedures for disabling certain system functions or participants, or starting or stopping certain processes out of sequence and,
- ensure, when a new software, hardware or telecommunications component is implemented, the retention for a short period of the capability to revert to the old technology and procedures.

5.7. OPERATOR/TECHNICAL AGENT RELATIONSHIPS WITH PARTICIPANTS

The operator/technical agent has an obligation to ensure that participants fully understand their relationship with and obligations to the operator/technical agent in the conducting of business.

In particular the participants should:

- understand fully the contracts and agreements they enter into with the operator/technical agent,
- where relevant, understand contracts and agreements the operator/technical agent has with suppliers, e.g. credit institutions, cash correspondent and depository banks insofar as participants are impacted,

- understand the mechanisms (products, services, support, etc.) of the operator/technical agent which can be effected via a variety of means, e.g. handbooks, operating manuals, product literature web site etc.,
- understand fully the risk management and risk mitigation procedures of the operator/technical agent and therefore any risk issues they may create or be exposed to in their relationship with the operator/technical agent and,
- benefit from support and training in respect of products and services and understanding of risk and risk mitigation.

5.7.1. ACCOUNT OPENING

The participant should be requested to apply in writing when opening an account or accounts within the operator/technical agent and there should be documented procedures and checks prior to operator/technical agent acceptance and implementation.

5.7.2. ACCOUNT CLOSING

Participants closing accounts should be required to provide reasonable period of notice prior to closing an account number or numbers and provide reasons for closure.

5.7.3. PARTICIPANT COMPLAINTS AND CLAIMS

In the event that a participant makes a formal complaint or where a financial claim is made for operator/technical agent error, negligence or other reason then these must be subject to formal procedure, appropriately recorded, reviewed and resolved within a reasonable timeframe.

5.8. OPERATOR/TECHNICAL AGENT RELATIONSHIPS WITH SUPPLIERS

The operator/technical agent has an obligation to ensure that suppliers, e.g. a cash correspondent or depository bank, fully understand their relationship with and obligations to the operator/technical agent in the conducting of business.

In particular the participants should:

- understand fully the agreements they enter into with the operator/technical agent,
- where relevant, understand agreements the operator/technical agent has with participants insofar as the suppliers are impacted,
- understand the mechanisms (products, services, support, etc.) of the operator/technical agent where the supplier is supporting directly or indirectly such mechanisms,
- understand fully the risk management and risk mitigation procedures of the operator/technical agent and therefore any risk issues they may create or be exposed to in their relationship with the operator/technical agent and,
- provide clearly documented procedures, explaining products and services supplied, risks involved and risk mitigation methods.

5.8.1. SUPPLIER CLAIMS

In the event that a supplier makes a formal complaint or where a financial claim is made for operator/technical agent error, negligence or other reason then these must be subject to formal procedure, appropriately recorded, reviewed and resolved within a reasonable timeframe.

5.9. OPERATOR/TECHNICAL AGENT - USE OF CONTRACTS AND RULES

Rules and contracts can be defined in a number of ways and it is important that all mechanisms which are used to form legal or contractual process and rules and procedures are appropriately documented and understood by relevant constituencies, e.g. participants, suppliers, governing body, executive management, etc.

5.9.1. CONTRACTS AND AGREEMENTS

The following categories of contracts and agreements are relevant:

- contracts and agreements with 'external' organisations, e.g. participants, cash and depository banks, other PSs, payment-related or other similar mechanisms, etc., which form a direct and essential mechanism for the provision of service in whole or in part and which are used to specify the responsibilities and scope or limitations of the operator/technical agent, i.e. what the operator/technical agent is responsible for or not as the case may be,
- contracts and agreements which form a direct and essential mechanism for the provision of service but which are 'internal' e.g. between two subsidiaries owned (or part-owned) by the operator/technical agent,
- contracts and agreements used by the operator/technical agent to mitigate risk, e.g. insurance, syndicates, etc.
- contracts and agreements with strategic and other suppliers i.e. where there is a high dependence on the continuing supply of services, e.g. IT suppliers, information providers, etc. and,
- contracts and agreements with members of the governing body, other groups or committees, executive management and/or key employees.

5.9.2. RULES AND PROCEDURES[10]

The following categories of rules and procedures are relevant:

- rules and procedures required to be used by 'external' organisations, e.g. participants, cash correspondent and depository banks, SSSs - Embedded, and SSSs - Other, etc., which form a direct and essential mechanism for the provision of service in whole or in part and which are used to specify the responsibilities and scope or limitations of the operator/technical agent, i.e. what the operator/technical agent is responsible for or not as the case may be,

[10] Rules and procedures are often included in participant handbooks, supplier operating manuals, product operating instructions, etc.

- rules and procedures which form a direct and essential mechanism for the provision of service but which are 'internal', e.g. between two subsidiaries owned (or part owned) by the operator/technical agent,
- rules and procedures which are used in the provision of products and services, IT and other 'internal' mechanisms which are required to ensure the smooth functioning of the operator/technical agent and,
- rules and procedures relating to the appropriate and effective governance of the operator/technical agent, e.g. bylaws, policies, employee handbooks, code of ethics, etc.

5.10. OPERATOR/TECHNICAL AGENT DEPENDENCE ON THE LEGAL AND REGULATORY ENVIRONMENT

Operators/technical agents normally conduct business within a national legal and regulatory environment although the EU, using various directives, is seeking to harmonise the environment in which operators/technical agents conduct business. Given this, it is important that the precise mechanism, including contract law or laws by which the operator/technical agent conducts business is precisely defined, documented and understood. (i.e. in a national environment or in the event where more than one legal or regulatory environment has an impact, e.g. the Eurozone.)

The following should be clearly understood:

- the national legal framework impacting the operator/technical agent,
- the national regulatory framework for same,
- other relevant national laws, e.g. employment, company, common, etc.,
- the EU legal framework impacting the operator/technical agent,
- the EU regulatory framework impacting the operator/technical agent and,
- other relevant EU directives, e.g. employment, banking, etc.

5.11. INDUSTRY STANDARDS AND CAPITAL MARKET BODIES

Standards committees and groups and industry bodies have a major role to play in shaping and influencing the services and development of an operator/technical agent. It is important that the views and needs of these bodies are recognised and understood by the operator/technical agent. These associations or groups have very different, and occasionally, contradictory needs and it is important that these groups are handled in a consistent and professional manner.

The following points are made in this regard:

- relevant groups should be listed and categorised by the operator/technical agent and responsibility assigned for the relationship and,
- such listings should be updated regularly and supplied to the BCL along with any reports, which would be informative of market issues or developments.

6. CORE PRINCIPLES

Operators/technical agents must be able to meet the Core Principles or give reasons for non-compliance or corrective action plans where relevant. The Core Principles are outlined in section 6.1. below (see also Appendix 4 for list) and should be applied to payment and security settlement systems wherever possible. Further, the BCL has defined its responsibilities in applying the Core Principles and these are outlined in 6.2. below. Further, as such relates particularly to SSSs – Embedded and SSSs – Other, recommendations and standards adopted by the BCL, relating to payment, securities settlement and other mechanisms.

6.1. OPERATOR/TECHNICAL AGENT REQUIREMENTS

6.1.1. LEGAL BASIS

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

Careful attention should be given to:

- the completeness and reliability of the framework legislation,
- the enforceability of laws and of contracts in all relevant circumstances,
- the clarity of timing of final settlement especially when there is an insolvency,
- the legal recognition of netting arrangements, the existence of any zero hour or similar rules,
- the enforceability of securities interests provided under collateral arrangements and of any relevant repurchase agreements,
- a legal framework that would support electronic processing of payments,
- the relevant provisions of banking and central banking law and,
- the relevance of laws outside the domestic jurisdiction.

6.1.2. RULES AND PROCEDURES

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.

The following points are considered relevant in this context.

Participants need to understand the risks they bear. An operator/technical agent should therefore have rules and procedures that:

- are clear, comprehensive and up to date,
- explain the system design, its timetable and risk management procedures,
- explain the system's legal basis and roles of the parties, are readily available and,

- explain where there is discretion and how it is exercised, set out decision and notification procedures and timetables for handling abnormal situations.

It may also be useful to organise participant training and monitor the performance of participants as evidence of their understanding.

6.1.3. RISK MANAGEMENT

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

The effective management of credit and liquidity risks is at the heart of designing safe mechanisms. The appropriate tools and incentives depend on the type of system design. Accordingly, the following points are relevant:

6.1.3.1. TOOLS FOR MANAGING CREDIT RISKS

- using system designs in which credit risk between participants does not arise e.g. in RTGS systems,
- access criteria based on creditworthiness,
- credit limits (bilateral or multilateral) to cap exposures and,
- loss-sharing arrangements and/or defaulter pays arrangements.

6.1.3.2. TOOLS FOR MANAGING LIQUIDITY RISKS

- management of payment and securities queues,
- provision of intraday liquidity (which means credit risk issues for the lender, e.g. the operator, central bank)
- throughput guidelines,
- position (receiver or sender) limits and,
- tools described under 7.1.5. below for systems with deferred net settlements,

6.1.3.3. GENERAL TOOLS

- information systems to support the tools for managing credit and liquidity risks,
- clear, full and timely (ideally real-time) financial information to participants and,
- timely monitoring by the operator/technical agent.

6.1.3.4. POSSIBLE INCENTIVES TO MANAGE THESE RISKS

- formula for loss-sharing, e.g. if it reflects the scale/nature of controllable positions with the failed institution and,
- pricing.

6.1.4. SETTLEMENT

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.

The following points are considered relevant in this context.

Promptness of final settlement of the day of value entails:

- clarity in the rules and procedures that a payment or security accepted by the system for settlement cannot be removed from the settlement process,
- a clearly defined and legally effective moment of final settlement,
- ensuring that the interval between the acceptance of a payment and security instruction and the final settlement at least never lasts overnight and preferable is much shorter and,
- ensuring that operating hours and the settlement processes are strictly observed.

6.1.5. MULTILATERAL NETTING

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.

A system that combines multilateral net settlement with deferral of settlement needs to be protected against liquidity risk arising from an inability to settle on the part of one or more participants.

6.1.5.1. ADDITIONAL FINANCIAL RESOURCES

This can be achieved by ensuring that additional financial resources are available to meet this contingency. These usually involve a combination of the following:

- committed lines of credit and,
- a pool of collateral (cash or securities – appropriately valued, including haircut) that supports them fully.

6.1.5.2. ADDITIONAL RESOURCES

The amount of such additional resources needs to be determined in relation to:

- the maximum individual settlement obligation and,
- whether the operator/technical agent meets or exceeds the minimum standard i.e. whether the operator/technical agent can withstand an inability to settle by the participant with the largest single settlement obligation or to withstand a more widespread inability to settle.

6.1.5.3. ALTERNATIVE DESIGN

Alternatively, the need to control liquidity risk in this context can be avoided by the use of an alternative design, e.g. RTGS (or some types of hybrid design).

6.1.6. SETTLEMENT ASSETS

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

The most satisfactory settlement asset for systemically important systems is a claim on the central bank issuing the relevant currency. The BCL fully supports and advocates the implementation of this core principle as soon as possible. Where other assets are used, considerations relevant to meeting this Core Principle are:

- the purpose of the arrangement,
- 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 and,
- risk controls, if any.

6.1.7. SECURITY AND RELIABILITY

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

The operator/technical agent should consider the following issues in relation to security and operational issues.

6.1.7.1. GENERAL

- the operational and IT infrastructure should meet the security policies and operational service levels agreed by the system operator/technical agent and participants, and relevant legal constraints, rules, risk management procedures, business requirements, or international, national or industry-level standards,
- the operational and IT infrastructure's security and operational reliability depend on both the central platform and participants' components; the participants have responsibilities for security and operational reliability. The operational and IT infrastructure 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; the operational and IT infrastructure should be designed and operated to meet such developments and,
- the operational and IT infrastructure requires adequate numbers of well-trained, competent and trustworthy personnel to operate it safely and efficiently in both normal and abnormal situations.

6.1.7.2. SECURITY

- security objectives and policies should be established during the design of the operational and IT infrastructure, appropriate to the operator/technical agent and reviewed periodically,
- operational and IT infrastructure security should conform to commercially reasonable standards, e.g. for confidentiality, integrity, authentication, non-repudiability, availability and auditability. Security features should be regularly tested and,
- the operational and IT infrastructure should be subject to regular security risk analysis. The operator/technical agent should proactively monitor technological advances to keep the operational and IT infrastructure's security risk analysis up to date.

6.1.7.3. OPERATIONAL RELIABILITY

- threats to operational reliability arise not just from failure of the central platform and participant components, bot also from features of the operational and IT infrastructure services and natural disasters,
- the operational and IT infrastructure 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 and,
- the operational and IT infrastructure should be designed with sufficient capacity, which should be monitored and upgraded in advance of business changes.

6.1.7.4. BUSINESS CONTINUITY

- the operator/technical agent should carry out a formal business continuity planning exercise. Simplicity and practicality should be key considerations when designing contingency arrangements, and
- business continuity arrangements should be documented and regularly tested. They should include procedures for crisis management and information dissemination.

Business continuity arrangements should include: diversion of payments to another payment system, use of alternate cash correspondent, physical file transfer arrangements, loss of domestic agent bank or SSS - Embedded or SSS - Other.

6.1.8. PRACTICAL AND EFFICIENT PAYMENT

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

Several steps are involved in establishing an efficient system (this section refers to the creation of a new operator/technical agent). They include identifying the general objectives, needs and constraints, and establishing an analytical framework for gauging efficiency, using various possible methods of analysis.

6.1.8.1. GENERAL

- define objectives, identifying risk and efficiency factors,
- identify the needs and constraints or participants and users more widely,
- identify operational and IT infrastructure choices and benefits,
- determine social and private costs and,
- develop decision choices.

6.1.8.2. ANALYTICAL FRAMEWORK

- identify efficiency requirements,
- identify safety requirements, evaluate costs (social and private),
- identify resources (social and private),
- determine practical constraints (technology, infrastructure) and,
- determine safety constraints (e.g. application of Core Principles).

6.1.8.3. METHODS

- cost benefit and other structural analysis,
- involvement of participants in discussions,
- methodology for data collection and analysis and,
- identify data sources (archived data, economic data, samples or estimates).

6.1.9. ACCESS

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

Access criteria should encourage competition among participants, without compromising operator/technical agent safety. Criteria that restrict access should be assessed for:

- justification in terms of safety,
- justification in terms of efficiency and,
- where consideration should be given to adopting forms of risk management which have the least restrictive impact on competition that circumstances permit.

6.1.10. GOVERNANCE

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

The following points are considered relevant in this context.

6.1.10.1. GOVERNANCE TOOLS

The operator/technical agent should have:

- written strategic objectives and plans for achieving them,
- reporting arrangements that assesses the actions of senior management against the strategic objectives,
- clear lines of responsibility and accountability within the organisation and appropriate management controls, together with arrangements for their enforcement,
- requirements that management at all levels is appropriately qualified and supervises the system and its operations competently, and
- risk management, audit and compliance functions independent of those responsible for day-to-day operations.

6.1.10.2. INTERNAL AND EXTERNAL AUDIT

Audit is a means of providing independent assurance to an operator's/technical agent's management or governing body of the effectiveness of operator/technical agent internal control system and operational efficiency. The auditor's scope should also include:

- governance arrangements,
- security controls and,
- procedures for managing risk.

Auditors are either internal (usually staff employed by the operator/technical agent) and this function should be independent of the management, and the functions and activities it audits, or external, appointed by the operator/technical agent (in accordance with legal or regulatory requirements). The external auditor should include an assessment of the quality of internal audit's testing of controls.

6.2. BCL REQUIREMENTS

The BCL responsibilities in applying the Core Principles are as follows:

6.2.1. OBJECTIVES AND PUBLIC DISCLOSURE

The central bank should define clearly its objectives in respect of systems (and operators) and should disclose publicly its role and major policies and procedures with respect to systemically important systems.

These policy and procedures cover this requirement.

6.2.2. ENSURE COMPLIANCE WITH CORE PRINCIPLES

The central bank should ensure that the systems it operates comply with the Core Principles

The BCL will require operator/technical agents to comply with the Core Principles as covered by these policy and procedures.

6.2.3. OTHER OPERATORS

The central bank should oversee compliance with the Core Principles by systems it does not operate and it should have the ability to carry out this oversight.

The BCL will:

- identify operators/technical agents subject to oversight. These include all operators/technical agents whether or not the BCL is a direct participant where such are deemed by the BCL to be relevant to efficiency and stability,
- operators/technical agent and participants will be made aware of the BCL's decision to exercise oversight,
- operators/technical agent not deemed to be systemically important will be re-examined from time to time to assess the relevance of changes in their activities or operating environment,
- reviewing and evaluating the design and operation of each operator/technical agent,
- evaluating a proposed new operator/technical agent at the design stage to minimise the cost of compliance,
- evaluating operators/technical agent continuously and,
- ensuring that action is taken to remedy any deficiencies in compliance.

For operators/technical agents, the BCL will carry out its oversight role via this policy and procedures.

6.2.4. CO-OPERATION WITH OTHER CENTRAL BANKS, AND RELEVANT DOMESTIC OR FOREIGN AUTHORITIES

The central bank in promoting system (and operator) safety and efficiency through the Core Principles should co-operate with other central banks and with other relevant domestic or foreign authorities.

The BCL co-operates with other NCBs within the ESCB[11] and with other NCBs as necessary. Further, the BCL is open for dialogue with other domestic and foreign authorities. See section 7. below.

[11] Article 14 of the Protocol on the Statute of the European System of Central Banks and of the European Central Bank and the MoU on specific arrangements for co-operation and information sharing in Stage Three of Economic and Monetary Union (EMU) in relation to large-value payments.

7. COOPERATION

The BCL, as an integral part of the ESCB, cooperates with other national central banks and the ECB in the execution of the objectives and tasks of the ESCB. The BCL remains open for cooperation arrangements with other national and international authorities.

The BCL has signed a Memorandum of Understanding on cooperation between payment systems overseers and banking supervisors in Stage Three of Economic and Monetary Union.

APPENDICES

1 RECOGNISED SYSTEMS, OPERATORS AND TECHNICAL AGENTS

BCL oversight is concerned with the following:

1.1. SYSTEMS

1.1.1. PSs

- Gross settlement,
- Net settlement and,
- Other payment mechanisms.

1.1.2. SSSs - EMBEDDED

- the transfer of collateral for monetary policy operations/TARGET liquidity,
- DvP settlement of international securities,
- DvP settlement of government debt securities and,
- DvP settlement of domestic Luxembourg securities.

1.1.3. SSSs - OTHER

- non DvP settlement of Luxembourg equities.

1.1.4. CCPs

There are no systems or operators requiring to be assessed at this time.

1.2. RECOGNISED OPERATORS

The following operators and technical agents are recognised and subject to oversight.

1.2.1. RECOGNISED OPERATORS - PSs

1.2.1.1. IN WHICH THE BCL PARTICIPATES

The BCL is a participant in the following operators, which have been notified by the BCL to the European Commission and are subject to BCL oversight and self-regulation.

- RTGS-L Gie (LIPS-Gross) and,
- Sypal-Gie (LIPS-Net).

1.2.1.2. OTHER RECOGNISED OPERATORS

- Other payment mechanisms subject to ongoing review, where their operators have been recognised by the BCL will be subject to oversight.

1.2.2. RECOGNISED OPERATORS - SSSs - EMBEDDED

1.2.2.1. IN WHICH THE BCL PARTICIPATES

The BCL is a participant in CBL, which has been recognised by the BCL and is subject to oversight. This includes the following activities:

- CBL as a provider of services for the transfer of collateral for monetary policy operations/TARGET liquidity,
- CBL for international securities settlement,
- CBL for domestic government debt settlement and,
- CBL for domestic Luxembourg securities.

Note: CI as a PSF and CBL as a credit institution are also subject to prudential supervision.

1.2.3. RECOGNISED OPERATORS – SSSs - OTHER

There are no recognised other securities settlement systems operators in Luxembourg at this time.

1.2.4. RECOGNISED OPERATORS – CCPs

There are no recognised central counterparty system operators in Luxembourg at this time.

1.2.5. RECOGNISED TECHNICAL AGENTS

The following technical agents are recognised by the BCL and are subject to oversight:

- BCL for RTGS-L Gie and LIPS-Gross,
- CETREL for Sypal-Gie and LIPS-Net,
- CETREL for other operational and IT infrastructure services of importance and,
- Clearstream Services for operational and IT infrastructure services (supplied to CBL and CBF).

1.2.6. OPMs

There are a number of other payment mechanisms in Luxembourg, which are subject to oversight and ongoing review and assessment in respect of operator/technical agent recognition.

2 DEFINITION AND EXPLANATION OF SECURITIES SETTLEMENT RISKS[12]

2.1. CREDIT RISK

Credit risk is the risk of loss from default by a participant, typically as a consequence of its insolvency. Two types of credit risk are usefully distinguished: pre-settlement risk and settlement risk.

Pre-settlement risk is also called replacement cost risk, that is, the risk of loss of unrealised gains on unsettled contracts with the defaulting participant. Settlement risk is sometimes termed principal risk, the risk of the loss of securities delivered or payments made to the defaulting participant prior to detection of the default. Settlement risk also involves liquidity risk that arises on the settlement date, as discussed below.

The risk of loss of unrealised gains is termed the replacement cost component of credit risk. A failure to perform on the part of one party to the transaction will leave the solvent counterparty with the need to replace, at current market prices, the original transaction. When the solvent counterparty replaces the original transaction at current prices, however, it will lose the gains that had occurred on the transaction in the interval between the time of the trade and the default. The unrealised gain, if any, on a transaction is determined by comparing the market price of the security at the time of default with the contract price. The seller of a security is exposed to a replacement cost loss if the market price is below the contract price, while the buyer of the security is exposed to such a loss if the market price is above the contract price. Because future securities price movements are uncertain at the time of the trade, both counterparties face replacement cost risk. The magnitude of replacement cost risk depends on the volatility of the security price and the amount of time that elapses between the trade date and the settlement date. Compressing the time between trade execution and settlement can reduce the replacement cost component of credit risk. Implementing legally binding trade netting systems may also reduce it.

Another form of credit risk arises in connection with contracts scheduled to settle on the date on which a counterparty default may occur. On such contracts, the non-defaulting counterparty may be exposed to principal risk, that is, the risk that the seller of a security could deliver but not receive payment or that the buyer could make payment but not receive delivery. If either of these events occurred, the entire principal value of the transaction would be at risk, hence the term principal risk. Both the buyer and the seller of a security may be exposed to principal risk. The buyer is at risk if it is possible to complete payment but not receive delivery, and the seller is at risk if it is possible to complete delivery but not receive payment. Principal risk can be eliminated through use of a DvP mechanism. A DvP mechanism links a payment system and a securities settlement system to ensure delivery occurs if and only if payment occurs. CCPs are sometimes used to mitigate principal risk. Principal risk in systems is analogous to what is termed cross-currency settlement risk (Herstatt risk) in foreign exchange settlements. Principal risk is of particular importance

[12] Largely extracted from CPSS - IOSCO paper on Recommendations for securities settlement systems January and October 2001.

because it involves the full value of securities transferred, and in the event of default it may entail credit losses so sizeable as to create systemic problems.

2.2. LIQUIDITY RISK

Liquidity risk includes the risk that the seller of a security who does not receive payment when due may have to borrow or liquidate assets to complete other payments. It also includes the risk that the buyer of the security does not receive delivery when due and may have to borrow the security in order to complete its own delivery obligation. Thus, both parties to a securities trade are exposed to liquidity risk on the settlement date. The costs associated with liquidity risk depend on the liquidity of the markets in which the affected party must make its adjustments: the more liquid the markets, the less costly the adjustment.

Liquidity problems have the potential to create systemic problems, particularly if they occur at a time when securities prices are changing rapidly and failures to meet obligations when due are more likely to create concerns about solvency. In the absence of a strong linkage between securities settlement systems and payment systems, the emergence of systemic liquidity problems at such times is especially likely, as the fear of a loss of the full principal value of securities or funds could induce some participants to withhold deliveries and payments. In turn, this may prevent other participants from meeting their obligations.

2.3. RISK OF SETTLEMENT BANK FAILURE

In addition to the risks associated with counterparties, participants in a securities settlement system may face the risk of a settlement bank failure. The failure of any bank that provides cash accounts to settle payment obligations for securities settlement system participants could disrupt settlement and result in significant losses and liquidity pressures for those participants. The impact on securities settlement system participants would be particularly severe if all securities settlement system participants were required to use the same settlement bank. Thus, when use of a single settlement bank is required, it is usually the central bank of issue or a limited purpose bank with strong risk controls and access to sizeable financial resources. Alternatively, the risk of settlement bank failure may be controlled and diversified by allowing securities settlement system participants to choose among multiple private settlement banks.

2.4. CUSTODY RISK

Risk may arise from the safekeeping and administration of securities and financial instruments on behalf of others. Users of custodial services face risk from the potential loss of securities in the event that the holder of the securities becomes insolvent, acts negligently or commits fraud. Even if there is no loss of the value of the securities held by the custodian or sub-custodian, the ability of participants to transfer the securities might temporarily be impaired. Custody risk is particularly important for indirect participants in securities settlement systems whose securities are held in custody by direct participants, but securities settlement systems pose custody risk, too.

2.5. OPERATIONAL RISK

Operational risk is the risk of unexpected losses as a result of deficiencies in operators and controls, human error or management failure. It can reduce the effectiveness of other measures the settlement operator takes to manage risk, for example by impairing the operator's ability to complete settlement, perhaps creating liquidity pressures for itself or its participants, or by hampering the operator's ability to monitor and manage its credit exposures. Possible operational failures include errors or delays in processing, IT system outages, insufficient capacity or fraud by staff.

2.6. LEGAL RISK

Legal risk is the risk that a party will suffer a loss because laws or regulations do not support the rules of the securities settlement system, the performance of related settlement arrangements, or the property rights and other interests held through the settlement operator. Loss and legal risk can also arise if the application of these laws and regulations is uncertain. For example, legal risk encompasses the risk a counterparty faces from an unexpected application of a law that renders contracts illegal or unenforceable. It includes the risk of loss resulting from a delay in the recovery of funds or securities or a freezing of positions. In a cross-border context, the laws of more than one jurisdiction apply or can potentially apply to a transaction, conduct or relationship. Counterparties may face loss resulting from the application of a different law than expected, or had specified in a contract, by a court in a relevant jurisdiction. Legal risk thus exacerbates other risks, such as market, credit or liquidity risk, relating to the integrity of transactions.

2.7. SYSTEMIC RISK

Systemic risk is the risk that the inability of one institution to meet its obligations when due will cause other institutions to fail to meet their obligations when due. The possibility that the liquidity and credit problems precipitated by these failures to perform will disrupt financial markets and impair the functioning of payment and settlement operators is of particular concern. Securities settlement systems can create significant credit, liquidity and other risks for their participants. PSs and clearing systems for other financial instruments often depend critically on securities settlement systems because of their use of securities as collateral in their own risk management procedures.

Market liquidity in securities markets is dependent on confidence in the safety and reliability of settlement operators because traders will be reluctant to deal if they doubt that the trade will settle. Thus it is important that the risks in securities settlement systems be appropriately managed in order that such are not a source of systemic disturbances to securities markets and other payment and settlement operators.

2.8. FINANCIAL RISK

Financial risk concerns the financial strength of the securities settlement system and if its capital is sufficient to meet the on-going operational and strategic investment needs of the participants and markets it serves.

2.9. HUMAN RESOURCE RISK

The specialist nature of securities settlement systems activities necessitates specialist knowledge in certain areas of its business - management, legal, operations and IT to name a few. In order to ensure an adequate knowledge base at all times staff retention, training, succession plans and formalised procedures (for knowledge exchange) form an essential requirement of the securities settlement system's business. Any sudden or prolonged and significant loss of management or experienced staff gives rise to an increased potential for operational risk.

2.10. REPUTATIONAL RISK

Given their role, the reputation and standing of a securities settlement system is essential to the safeguarding of the Luxembourg and the Eurozone. It is essential that such systems conform to best practice and project an image of integrity and stability. Accordingly a securities settlement system should adhere to international standards, working closely with and supporting industry groups and standards committees.

3 EXPLANATION OF CROSS-BORDER SECURITIES SETTLEMENT PROCESS[13]

Securities settlement is effected via many different channels in the cross-border environment, all of which could have an impact on financial stability. It is important to understand these different channels so that those relating to PSs and more specifically those deemed to be SSSs - Embedded can be determined. In particular, there are a number of different methods for the settlement of a cross-border trade, depending upon the non-resident counterparty (or counterparties) to a trade gains access to the securities settlement system where the security is issued and/or held in safekeeping. Such methods of cross-border settlement are not mutually exclusive since market participants may use one method for certain categories of counterparties or types of security and another channel for other counterparties and securities.

3.1. INTERNATIONAL CENTRAL SECURITIES DEPOSITORIES (ICSD)

The ICSDs, CBL and Euroclear Bank (EB) historically provided settlement and custody services for Eurobonds. The services offered have expanded and today a wide range services are provided, spanning a range of currencies and instruments where settlement can be effected in more than one way; their core business in cross-border processing however remains in bonds. The ICSDs operate efficient links to many national markets, often using local agents, which allows for settlement between their participants and counterparties located in a national market. Trades between the participants of any one ICSD are settled on the books of that ICSD whereas a participant in one ICSD can settle their trade over an electronic link or 'bridge' between the two ICSDs.

3.2. LINKS BETWEEN SECURITIES SETTLEMENT SYSTEMS

Bilateral links provide another method for settling cross-border trades between participants of different securities settlement systems and these can be reciprocal links whereby the participants of either operator can settle their trades in the other operator while other links permit settlement in one direction only. In some links, a system operator becomes a full participant in another operator while in other links free-of-payment transfers only are possible.

3.3. DIRECT MEMBERSHIP

In this method, the non-resident counterparty establishes direct access to the securities settlement system in the country where the security is issued through membership in the relevant securities settlement system. This method may not be available to all non-resident counterparties, however, because some operators prohibit non-resident financial institutions from becoming direct participants. Alternatively, local branches or subsidiaries of non-resident financial institutions may be allowed to participate.

[13] Largely extracted from CPSS - IOSCO paper on Recommendations for securities settlement systems January and October 2001.

3.4. LOCAL AGENT

A common method of settling cross-border trades is to employ a local agent or custodian in the country of issue. This agent is a direct member of the securities settlement system and can perform settlement and settlement-related services. For example, the agent may provide banking services such as funds transfers, overdraft facilities, foreign exchange transactions, and securities borrowing and lending. Custody services that would typically be offered include securities safekeeping, collection of interest and dividends, and processing of corporate actions. The precise mix of services that the non-resident counterparty obtains from the local agent is determined contractually.

3.5. GLOBAL CUSTODIAN

A global custodian provides its customers with access to settlement and custody services in multiple markets, using a network of subcustodians, both the global custodian's own branches and other local agents. The non-resident counterparty is thus able to employ a single communication link for providing settlement instructions and for receiving reports from local markets. The global custodian also typically offers accounting and credit services including multi-currency banking and cash management services. Some global custodians provide their customers with daily conversion of all foreign currency denominated receipts and payments into the investor's home currency.

4 LIST OF CORE PRINCIPLES[14]

The Governing Council of the ECB has adopted the Core Principles as Eurosystem oversight minimum standards.

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

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.

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

IV.[15] 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.

V.[15] 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.

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

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

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

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

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

[14] Extracted from BIS paper on Core Principles for Systemically Important Payment Systems January 2001.

[15] Systems should seek to exceed the minima included in these two Core Principles.

5 GLOSSARY

The following glossary of terms is not intended to provide legally precise definitions but to assist in the understanding of the subject and the policy and procedures. Terms are defined in this glossary with particular reference to PSs, SSSs – Embedded, and SSSs - Other and their operators.

Acceptance for settlement	The stage in the processing of a payment at which it has passed all risk management and other tests and can be settled under the systems rules and procedures.
Access	The right or opportunity for an institution to use the services of a particular payment or securities settlement operator on its own account or for customers. See also *participant, direct participant indirect participant*.
Agent or agent bank	See *depository bank*.
Authentication	The methods used to verify the identity of an institution, individual or hardware device involved in payment or securities settlement activities and to confirm that a message or instruction has not been modified or replaced in transit.
Business continuity	A payment or securities settlement operator's business continuity arrangements aim to ensure that it meets agreed service levels even if one or more components of the operator's operational or IT infrastructure fail or if it is affected by an abnormal external event. Arrangements can include both preventative measures and contingencies.
Cash correspondent	A financial institution which acts as a supplier to an operator for the handling of external receipt and payments of funds in one or more currencies.
Collateral	An asset that is delivered by the collateral provider to secure payment or performance of an obligation to the collateral taker. For example, participants in some payment and securities settlement systems
Contract law	Body of law concerned with making and enforcing agreements.
Counterparty	One party to a trade or transaction. A trade and the settlement process, which follows involves two counterparties.

Credit risk	Credit risk is the risk of loss from default by a participant, typically as a consequence of its insolvency where a counterparty will not settle an obligation for full value, either when due or at any time thereafter. In securities processing, two types of credit risk are usefully distinguished: pre-settlement risk and settlement risk. Pre-settlement risk is also called replacement cost risk, that is, the risk of loss of unrealised gains on unsettled contracts with the defaulting participant. Settlement risk is sometimes termed principal risk, the risk of the loss of securities delivered or payments made to the defaulting participant prior to detection of the default. Settlement risk also involves liquidity risk that arises on the settlement date, as discussed below.
Custody risk	Risk may arise from the safekeeping and administration of securities and financial instruments on behalf of others. Users of custodial services face risk from the potential loss of securities in the event that the holder of the securities becomes insolvent, acts negligently or commits fraud. Even if there is no loss of the value of the securities held by the custodian or sub-custodian, the ability of participants to transfer the securities might temporarily be impaired.
Debt securities	Securities created through and evidencing a loan by the issuer, such as, for example, commercial paper, notes, certificates of deposit, medium-term notes and bonds.
Default	Failure to complete a funds transfer according to its terms for reasons that are not technical or temporary, usually as a result of insolvency.
Delivery against payment / delivery versus payment (DvP)	The irrevocable exchange of securities and cash value to settle a transaction, involving the simultaneous exchange of securities and cash.
Delivery free of payment (FoP)	A transaction for the irrevocable delivery of securities without an associated payment of funds.
Depository bank	A bank or SSS - Embedded or SSS - Other which is used for the settlement and safekeeping of securities.
Direct participant	A participant of a payment or securities settlement operator.
(Systemic) Disruption	Events whose impacts have the potential to threaten the stability of the financial system, by transmitting from one financial institution to another, including through payment and securities settlement operators. See also *systemic risk*.
Eurobond	Bond issued by a borrower outside of a domestic market, denominated in a Eurocurrency, underwritten and sold by an international syndicate of financial institutions.

Equity	A share in the ownership of a company.
Exit criteria	Criteria for an exiting participant of a payment or securities processing operator to cease to participate.
Final settlement	Settlement which is irrevocable and unconditional.
Financial risk	The ability of the operator to be financially viable. This risk concerns the financial strength of the operator and if its capital is sufficient to meet the on-going operational and strategic investment needs of the participants, markets and other organisations, e.g. the bank it serves.
Funds transfer	See *payment*.
Gridlock	A situation that can arise in a PS in which the failure of some payments to be accepted for settlement prevents a substantial number of other payments from other participants from being accepted for settlement.
Haircut	The difference between the market value of a security and its collateral value.
Human resource risk	The specialist nature of securities settlement system activities necessitates specialist knowledge in certain areas of its business - management, legal, operations and IT to name a few. In order to ensure an adequate knowledge base at all times staff retention, training, succession plans and formalised procedures (for knowledge exchange) form an essential requirement of the securities settlement system's business. Any sudden or prolonged and significant loss of management or experienced staff gives rise to an increased potential for operational risk.
Indirect participant	A class of participant of a payment or securities settlement operator which settle transactions across the books of a direct participant.
Intraday liquidity	Funds which can be accessed during the business day, usually to enable financial institutions to make payments in real time.
Legal risk	Legal risk is the risk that a party will suffer a loss because laws or regulations do not support the rules of the operator, the performance of related settlement arrangements, or the property rights and other interests held.

Liquidity risk	Liquidity risk includes the risk that the seller of a security who does not receive payment when due may have to borrow or liquidate assets to complete other payments. It also includes the risk that the buyer of the security does not receive delivery when due and may have to borrow the security in order to complete its own delivery obligation.
Loss-sharing	An agreement between participants regarding the allocation of any loss arising when one or more participants fail to fulfill their obligations.
(Pre-settlement) matching	The process that compares settlement (and optional trade) details given by two counterparties to a trade in an instruction.
Non-repudiability	The ability to prevent denial or repudiation by the sender or receiver of a message or instruction.
Operator	An operator is the central organisation, providing products and services to participants, often using technical agents and suppliers and operating in a legal and regulatory environment which can be wider than the home state, e.g. the Eurozone.
Operational risk	Operational risk is the risk of unexpected losses as a result of deficiencies in operators and controls, human error or management failure.
Optimisation routine	Processes in payment and securities settlement capabilities to determine the order which instructions are accepted for settlement. See also *queue/queuing*.
Oversight	A public policy activity principally intended to promote the safety and efficiency of payment and securities settlement capabilities and in particular to reduce systemic risk.
Participant	A party that is recognised in the rules of a payment or securities settlement operator as eligible to exchange and settle instructions with another participant either directly or indirectly.
Payment	The payer's transfer of a monetary claim on a party acceptable to the beneficiary.
Payment system	A PS is an arrangement, which allows the users of the system to transfer funds. Central to payment activities are the arrangements that facilitate the transfer of funds between the participants (those intermediaries which connect directly to the central operator or each other). It is these arrangements which constitute a PS, which therefore include the networks, which link participants, the message routing systems, and infrastructure rules and procedures.

Pledge	A delivery of assets, without an absolute transfer of ownership/title, as security for the performance of an obligation owed by one party to another.
Primary market	The market, in which securities are first issued, subscribed and distributed.
Prudential supervision	The assessment and enforcement of compliance by financial institutions with laws, regulations or other rules intended to ensure that they operate in a safe and sound manner and they hold capital and reserves sufficient to support the risks that arise in the course of their business activities.
Public disclosure	Making information publicly accessible.
Queue/queuing	An arrangement whereby instructions are held pending acceptance for settlement by an operator.
Real-time Gross Settlement System (RTGS)	A payment or securities settlement capability in which transaction processing and settlement take place continuously and in real time (that is without deferral) and gross (i.e. transaction by transaction)
Real-time processing	The processing of transactions on an individual basis at the time they are received rather than at some later time.
Real-time risk management	Process that allows risks associated with participants in payments and securities settlement capabilities to be managed immediately and continuously.
Repurchase agreement (Repo)	Contract to sell and subsequently repurchase securities at a specified time and price.
Reputational risk	Given their role, the reputation and standing of a securities settlement system is essential to the safeguarding of the Luxembourg and the Eurozone. It is essential that such systems conform to best practice and project an image of integrity and stability. Accordingly a securities settlement system should adhere to international standards, working closely with and supporting industry groups and standards committees.
Secondary market	The market for tradable securities that is made by market makers, principles or agents after the completion of the primary market (new issue) distribution and until final redemption.
SSS - Embedded **Securities settlement system embedded with payments**	An SSS - Embedded is defined broadly as the full set of institutional arrangements, procedures and rules for the primary and secondary market and the confirmation, clearance and DvP settlement of securities trades (and derivatives if relevant), the safekeeping of securities and any related services.

SSS - Other	An SSS – Other is defined as the full set of institutional arrangements, procedures and rules for the primary and secondary market and the confirmation, clearance and settlement of securities trades, the safekeeping of securities and any related services. In such systems, securities are processed independently from funds where the cash leg is settled first.
Securities Settlement System	A system which permits the transfer of ownership of and/or title to securities.
Settlement	An act that discharges financial obligations between two or more parties. This term applies equally to payments and to the irrevocable delivery of securities against final payment.
Settlement asset	An asset used for the discharge of settlement obligations as specified by the rules, regulations or customary practice for a payment or securities settlement capability.
(Risk of) Settlement bank failure	In addition to the risks associated with counterparties, participants in a securities settlement system may face the risk of a settlement bank failure. The failure of any bank that provides cash accounts to settle payment obligations for such systems' participants could disrupt settlement and result in significant losses and liquidity pressures for those participants.
Settlement institution	The institution across whose books transfers between participants take place in order to achieve settlement within a settlement system.
Straight-through Processing (STP)	Automation of processing that allows data to be entered only once and then used for all subsequent payment processes.
S.W.I.F.T.	Formal abbreviation of the Society for Worldwide Interbank Financial Telecommunications.
System	A system is a mechanism, which comprises an operator, participants, technical agents and/or suppliers, contracts and rules and a legal and regulatory framework.
Systemic risk	Systemic risk is the risk that the inability of one institution to meet its obligations when due will cause other institutions to fail to meet their obligations when due. The possibility that the liquidity and credit problems precipitated by these failures to perform will disrupt financial markets and impair the functioning of payment and settlement operators is of particular concern.

Technical agent	Technical agents and some suppliers are deemed to be important for reasons of efficiency or stability and as such subject to oversight. A technical agent is a supplier of service where an operator has located a significant portion of its operational or IT infrastructure or where several payment or securities settlement related operational or IT activities are centralised.
Unwind	To undo a process that was presumed to have been completed.

6 BIBLIOGRAPHY

European Union – Selected instruments taken from the Treaties.	1999
BIS – Delivery versus payment in securities settlement systems.	September 1992
BIS – Cross-border securities settlements.	March 1995
European Central Bank press release – Memorandum of Understanding on Co-operation between payment system overseers and banking supervisors in stage three of EMU.	2 April 2001
ECB – Role of the Eurosystem in the field of payment system oversight.	June 2000
EMI (now the ECB) – Standards for use of EU securities settlement systems in ESCB credit operations.	January 1998
ECB – Assessment of EU securities settlement systems against the standards for their use in ESCB credit operations.	September 1998
Speech by Tomasso Padoa-Schioppa, Member of the Executive Board ECB, Brussels.	9 November 2000
CPSS - IOSCO – Recommendations for securities settlement systems.	October 2001
Speech by Yves Mersch, Governor of the BCL, Prague.	28 March 2000
Bank of England - Oversight of payment systems.	November 2000
Luxembourg law – implementation of the EU Settlement Finality Directive.	12 January 2001
ECB – Correspondent Central Banking Model.	November 1999
BCL Circular letter.	23 February 2001
BIS Committee on Payment and Settlement Systems Core Principles for Systemically Important Payment Systems.	January 2001