

6 April 2006

Consultation Paper

STANDARDS ON OUTSOURCING

CEBS presents a revised version of its Standards on Outsourcing. The proposed standards are based on current practices and also take into account international, such as the Joint Forum, and European initiatives in the field of outsourcing.

Taking account of the comments received during the first public consultation, and subsequent legislative developments, these Standards are open for three further months of consultation in accordance to CEBS' public statement on consultation practices. CEBS invites comments on this revised consultation paper by **6 July 2006** (CP02rev@c-eps.org). Comments received will be published on the CEBS website unless the respondents request otherwise.

Alignment with securities regulation

Following comments received during the first round of consultation, CEBS and the Committee of European Securities Regulators (CESR) have ensured that the proposed standards are consistent with the Markets in Financial Instruments Directive (MiFID) and its application to credit institutions. CEBS strived to align the Standards to the highest degree possible with regulation under MiFID, taking into account the "Draft Commission Directive implementing Directive 2004/39/EC" as published on the Commission homepage on 6 February 2006.¹ A mapping of the present version of CEBS Standards and the latest draft of MiFID Level 2 measures will be published by the end of April. Examples of alignment worth highlighting are:

- a. consistent use of "senior management" in the sense of Dir 2000/12/EC which is in essence identical to MiFID;
- b. the approach taken towards the outsourcing of senior management responsibilities and functions; and
- c. limitations on outsourcing only of activities at the core of credit institutions, which is comparable to the approach taken by MiFID Level 2.

¹ Draft Commission Directive implementing Directive 2004/39/EC of the European Parliament and of the Council as regards organisational requirements and operating conditions for investment firms, and defined terms for the purposes of that Directive (6.2.2006).

In spite of CEBS' attempts at alignment there remain areas in which CEBS Standards diverge from MiFID Level 2 regulations. The main reason for this is that MiFID Level 2 and CEBS Standards do not have the same scope of application and do not regulate the same area. Whereas CEBS Standards are directed towards credit institutions generally possessing a universal licence to conduct all kinds of banking business, including investment services, MiFID is directed towards investment service providers (which may also be credit institutions). Secondly, CEBS Standards are aimed at prudential supervision, while MiFID has more of a conduct of business focus. This explains why CEBS Standards explicitly refer to risk management which is a core focus for prudential supervision. The areas of divergence were identified in the cross-sectoral talks and they were accepted by the other Level 3 committees.

It is for all these reasons that in several places CEBS Standards diverge from MiFID Level 2 regulation, while taking into account as far as possible industry requests for alignment. The following paragraphs explain why a different approach has been taken in several instances:

- a. Definition: CEBS Standards are using the same definition as the Joint Forum's Outsourcing Standards, which put an emphasis on "continuity". MiFID also asks for continuity but refers to it in different articles.
- b. Materiality: CEBS Standards use the concept of "materiality". This is a term which is not used in MiFID, though MiFID – Level 2 regulation does regard operational functions as "critical or important". Material activities as defined in CEBS Standards embrace not only critical or important activities, but also the risk management of such activities, other licensed activities and activities with a significant impact on risk management. The deviation from MiFID terminology is thus justified.
- c. Risk management: risk management is considered of such importance for prudential reasons and in the context of banking supervision that CEBS Standards mention it explicitly.
- d. Activities which must not be outsourced: CEBS Standards now mention explicitly "services and activities concerning the acceptance of deposit or to lending" as activities which must not be outsourced to an unauthorised entity. MiFID Level 2 contains comparable rules only in relation to "portfolio management provided to retail clients" if the service provider is located in a third country. This difference in approach is explained by the CEBS Standards' focus on prudential supervision.
- e. Adequate information/prior notification: following strong requests from supervisory authorities to refrain from the requirement of prior notification, this criterion has been changed. Now an outsourcing institution is requested to "adequately inform" its supervisory authority in certain cases. MiFID Level 2 requests in one specific case prior notification. CEBS believes that the expression "adequately inform" leaves sufficient room for its interpretation by national authorities in line with MiFID Level 2 requirements.

- f. Outsourcing of non-material activities: CEBS Standards apply to all kinds of outsourcing for prudential reasons. Thus, outsourcing of non-material activities is also within the scope of their application. However, the principle of proportionality is accepted in the application of these Standards.

CEBS Standards: introduction

There is currently no harmonisation at the EU level in the area of outsourcing undertaken by credit institutions and, accordingly, different supervisory approaches have developed across the EU to address the potential risks arising from this practice. A number of European countries have, for some years, had in place formal outsourcing regimes. Given the increasing use of outsourcing by institutions, including on a cross-border basis, and its implications for effective prudential supervision, CEBS has deemed it appropriate to develop these Standards in order to promote greater consistency of approach where possible within the national legal frameworks. The Standards are based on a range of current practices and the common elements of policy that have been elaborated to date in various Member States but also take into account various recent international and European initiatives in the field of outsourcing.

There is an obvious overlap between the proposed standards, on the one hand, and relevant MiFID rules, and the ensuing Level 2 measures proposed by the Commission that will apply to all authorized entities offering investment services under the MiFID, on the other hand. CEBS and CESR have duly consulted to ensure that the proposed standards:

- are in full compliance with the MiFID Level 2 provisions and that their application to credit institutions subject to MiFID is fully consistent; and
- are consistently applied to all credit institutions, thus contributing towards establishing a level playing field for them.

These Standards are designed to promote an appropriate level of convergence in supervisory practices throughout the EU. At the same time, the Standards are principles-based and provide national supervisors with an adequate degree of flexibility to take into account domestic rules and specific features of their local markets and to accommodate developments in market practices.

Part 1: Definitions

Standard 1

For the purposes of these standards, the following is meant by:

- a. outsourcing: an authorised entity's use of a third party (the "outsourcing service provider") to perform activities on a continuing basis that would normally be undertaken by the authorised entity, now or in the future. The supplier may itself be an authorised or unauthorised entity;**
- b. purchasing: *inter alia*, the supply (i) of services, goods or facilities without information about, or belonging to, the purchasing institution coming within the control of the supplier; or (ii) of standardized products, such as market information or office inventory (authorised entities should ensure that what they are buying is fit for purpose);**
- c. outsourcing service provider: the supplier of goods, services or facilities, which may or may not be an authorised entity, and which may be an affiliated entity within a corporate group or an entity that is external to the group;**
- d. outsourcing institution: the authorised entity which is the buyer of such goods, services or facilities;**
- e. authorised entity: a licensed credit institution;**
- f. material activities: (i) activities of such importance that any weakness or failure in the provision of these activities could have a significant effect on the authorised entity's ability to meet its regulatory responsibilities and/or to continue in business; (ii) the management of risks related to these activities (iii) any other activities requiring a licence from the supervisory authority; and (iv) any activities having a significant impact on its risk management;**
- g. senior management: persons who effectively direct the business of the authorised entity;**
- h. "chain" outsourcing: outsourcing where the outsourcing service provider subcontracts elements of the service to other providers.**

Part 2:
Standards on outsourcing addressed to authorised entities

Standard 2

The ultimate responsibility for the proper management of the risks associated with outsourcing or the outsourced activities lies with an outsourcing institution's senior management.

1. All outsourcing regimes should ensure that the outsourcing of functions to an outsourcing service provider does not impair the supervision of the outsourcing institution.
2. Responsibility for outsourced functions must always be retained by the outsourcing institution. The outsourcing of functions does not relieve an outsourcing institution of its regulatory responsibilities for its authorized activities or the function concerned.
3. Outsourcing institutions should be required to retain adequate core competence at a senior operational level in house to enable them to have the capability to resume direct control over an outsourced activity, in extremis.
4. Outsourcing shall not affect managers' full and unrestricted responsibilities under applicable legislation (e.g. under banking law).

Standard 3

Outsourcing arrangements can never result in the delegation of senior management's responsibility.

1. The outsourcing of core management functions is considered generally to be incompatible with the senior management's obligation to run the enterprise under their own responsibility. Core management functions include, inter alia, setting the risk strategy, the risk policy, and, accordingly, the risk-bearing capacity of the institution. Hence, management functions such as the setting of strategies and policies in respect of the authorised entity's risk profile and control, the oversight of the operation of the entity's processes, and the final responsibility towards customers and supervisors should not be outsourced.

Standard 4

4.1 An authorised entity may not outsource services and activities concerning the acceptance of deposits or to lending requiring a licence from the supervisory authority according to the applicable national banking law unless the outsourcing service provider either (i) has an authorisation that is equivalent to the authorisation of the outsourcing institution; or (ii) otherwise allowed to carry out those activities in accordance with the relevant national legal framework.

4.2 Any area of activity of an outsourcing institution other than those identified in Standards 2 and 3 may be outsourced provided that such outsourcing does not impair:

- a. the orderliness of the conduct of the outsourcing institution's business or of the financial services provided;**
- b. the senior management's ability to manage and monitor the authorised entity's business and its authorised activities;**
- c. the ability of other internal governance bodies, such as the board of directors or the audit committee, to fulfil their oversight tasks in relation to the senior management; and**
- d. the supervisory authority's ability to fulfil its supervisory tasks.**

4.3 An outsourcing institution should take particular care when outsourcing material activities. The outsourcing institution should adequately inform its supervisory authority about this type of outsourcing.

1. These requirements do not affect the principle of managers' sole responsibility (Standard 2) for all authorised activities. The managers of the outsourcing institution shall be fully responsible to the supervisory authority for any outsourced activity. The managers should therefore take suitable measures to ensure that the outsourced activities continue to meet the performance and quality standards that would apply if their own institution were to perform the relevant activities in-house.
2. An outsourcing institution should adequately inform its supervisory authority on any material activity to be outsourced. Such information should be made available in a timely manner in order for the supervisor to evaluate the proposal or to allow him to consider whether the proposal raises prudential concerns and to take appropriate action if required. Outsourcing institutions should be aware that for the outsourcing of material activities the supervisory authority may impose specific conditions. In doing so, the supervisory authority will consider factors such as the size of the institution, the nature of the outsourced activity, the characteristics and market position of the service provider, the duration of the contract and the potential of the outsourcing to generate conflicts of interest (e.g. the supervisory authority may wish to prohibit the outsourcing of the financial accounting and the preparation of the

annual accounts to the outsourcing institution's external auditor, or to the office with which the external auditor is connected).

3. An outsourcing institution should inform its supervisory authority of any material development affecting the service provider and its ability to fulfil its obligations to customers.
4. Subject to the principles that apply to cross-border outsourcing expressed under Standard 4.1(i), no special rules are needed in relation to the geographical location of an outsourcing service provider. However, due to possible data protection risks and risks to effective supervision by the supervisory authority, institutions should take special care when entering into and managing outsourcing agreements that are undertaken outside the EEA.
5. Intra-group outsourcing and outsourcing according to Standard 4.1(i) can be material. Outsourcing institutions should be aware that supervisory authorities may take specific circumstances into consideration, such as the extent to which the outsourcing institution controls the service provider or has the ability to influence its actions, and the extent to which the service provider is included in the consolidated supervision of the group, when assessing the risks associated with an intra-group outsourcing arrangement and the treatment to apply to such arrangements.

Standard 5

There should be no restrictions on the outsourcing of non-material activities of an outsourcing institution.

1. In such cases the outsourcing institution does not need to adequately inform its supervisory authority. Nevertheless, outsourcing institutions should adequately manage the risks relating to such outsourcing arrangements at all times. In line with Standard 2, the senior management of the outsourcing institution should be fully responsible for any outsourced activity.
2. Areas which could be regarded as non-material are those not falling within the definition of "material activities" according to Standard 1(f), and may include:
 - a. areas which do not potentially constitute relevant risks and which, if outsourced, would not compromise the provisions set forth in Standard 4.2 above; and
 - b. purely advisory services used by the institution. For example, this applies to legal and tax consulting, even where this is not limited to individual aspects or projects.

Standard 6

6.1 The outsourcing institution should have a policy on its approach to outsourcing, including contingency plans and exit strategies.

6.2 An outsourcing institution should conduct its business in a controlled and sound manner at all times.

1. The outsourcing institution should have a general policy that covers all aspects of outsourcing, including non-material outsourcing, whether the outsourcing takes place within a corporate group or not.
2. When drawing up the policy the outsourcing institution should recognise that no form of outsourcing is risk free. The policy should recognise that the management of non-material and intra-group outsourcing should be proportionate to the risks presented by these arrangements.
3. The policy should explicitly consider the potential effects of outsourcing on certain significant functions (e.g. the internal audit function and the compliance function) when conducting the risk analysis prior to outsourcing.
4. The policy should ensure that the outsourcing service provider's financial performance and essential changes in the service provider's organisation structure and ownership structure are appropriately monitored and assessed by the outsourcing institution's management so that any necessary corrective measures can be taken promptly.
5. The outsourcing institution should specify an internal unit or individual that is responsible for monitoring and managing each outsourcing arrangement.
6. The policy should consider the main phases that make up the life cycle of an institution's outsourcing arrangements:
 - a. the decision to outsource or change an existing outsourcing arrangement (the decision making phase);
 - b. due diligence checks on the outsourcing service provider;
 - c. drafting a written outsourcing contract and service level agreement (the pre-contractual drafting phase);
 - d. the implementation, monitoring, and management of an outsourcing arrangement (the contractual phase). This may include also the following-up of changes affecting the outsourcing service provider (e.g. major change in ownership, strategies, profitability of operations);
 - e. dealing with the expected or unexpected termination of a contract and other service interruptions (the post-contractual phase). In particular, outsourcing institutions should plan and implement

arrangements to maintain the continuity of their business in the event that the provision of services by an outsourcing service provider fails or deteriorates to an unacceptable degree, or the firm experiences other changes. This policy should include contingency planning and a clearly defined exit strategy.

Standard 7

An outsourcing institution should manage the risks associated with its outsourcing arrangements.

1. Compliance with this article should include an on-going assessment by the outsourcing institution of the operational risks associated with all its outsourcing arrangements. An outsourcing institution should inform its supervisory authority of any material development.

Standard 8

All outsourcing arrangements should be subject to a formal and comprehensive contract. The outsourcing contract should oblige the outsourcing service provider to protect confidential information.

1. Any outsourcing arrangement should be based on a clear written contract.
2. An outsourcing institution should make sure that the written contract takes account of the following (bearing in mind other specific national rules and legislation):
 - a. The operational activity that is to be outsourced should be clearly defined.
 - b. The precise requirements concerning the performance of the service should be specified and documented, taking account of the objective of the outsourcing solution. The outsourcing service provider's ability to meet performance requirements in both quantitative and qualitative terms should be assessable in advance, including compliance with these Standards.
 - c. The respective rights and obligations of the outsourcing institution and the outsourcing service provider should be precisely defined and specified. This should also serve to ensure compliance with laws and supervisory regulations and guidelines for the duration of the outsourcing arrangement.
 - d. In order to underpin an effective policy for managing and monitoring the outsourced activities, the contract should include a termination and exit management clause, where proportionate and if deemed

necessary, which allows the activities being provided by the outsourcing service provider to be transferred to another outsourcing service provider or to be reincorporated into the outsourcing institution.

- e. The contract should cover the protection of confidential information, banking secrecy and any other specific provisions relating to handling confidential information. Whenever information is subject to confidentiality rules at the level of the outsourcing institution at least the same level of confidentiality should be ensured by the service provider.
 - f. The contract should ensure that the outsourcing service provider's performance is continuously monitored and assessed so that any necessary corrective measures can be taken promptly.
 - g. The contract should include an obligation on the outsourcing service provider to allow the outsourcing institution's compliance and internal audit departments complete access to its data and its external auditors full and unrestricted rights of inspection and auditing of that data.
 - h. The contract should include an obligation on the outsourcing service provider to allow direct access by the outsourcing institution's supervisory authority to relevant data and its premises as required.
 - i. The contract should include an obligation on the outsourcing service provider to immediately inform the outsourcing institution, or the supervisory authority directly, of any material changes in circumstances which could have a material impact on the continuing provision of services. This may require obtaining consents from affected parties such as the parent company and relevant home supervisory authority.
 - j. The outsourcing contract shall contain provisions allowing the outsourcing institution to cancel the contract by contractual notice of dismissal or extraordinary notice of cancellation if so required by the supervisory authority.
3. When drafting the contract the outsourcing institution should bear in mind that the level of monitoring, assessment, inspection and auditing required by the contract should be proportionate to the risks involved and the size and complexity of the outsourced activity.

Standard 9

In managing its relationship with an outsourcing service provider an outsourcing institution should ensure that a service level agreement (SLA) is put in place.

1. A service level agreement should normally contain a mixture of quantitative and qualitative performance targets, to enable an outsourcing institution to assess the adequacy of service provision.
2. An outsourcing institution should also consider the need to evaluate the performance of its outsourcing service provider using mechanisms such as service delivery reports, self-certification or independent review by the outsourcing institution's, or the outsourcing service provider's, internal and/or external auditors.
3. An outsourcing institution should be prepared to take remedial action if the outsourcing service provider's performance is inadequate.

Standard 10

10.1 The outsourcing institution should take account of the risks associated with "chain" outsourcing.

10.2 The outsourcing institution should agree to chain outsourcing only if the sub-contractor will also fully comply with the obligations existing between the outsourcing institution and the outsourcing service provider, including obligations incurred in favour of the supervisory authority.

10.3 The outsourcing institution should take appropriate steps to address the risk of any weakness or failure in the provision of the sub-contracted activities having a significant effect on the outsourcing service provider's ability to meet its responsibilities under the outsourcing agreement and SLA.

1. The sub-outsourcing of outsourced activities and functions to third parties (sub-contractors) should be treated by the outsourcing institution like a primary outsourcing measure. Compliance with these conditions should be ensured contractually, for example by a clause in the outsourcing contract requiring the prior consent of the outsourcing institution to the possibility and the modalities of sub-outsourcing.
2. The outsourcing institution should ensure that the outsourcing service provider agrees that the contractual terms agreed with the sub-contractor will always conform, or at least not be contradictory, to the provisions of the agreement with the outsourcing institution.

Part 3: Standards on outsourcing addressed to supervisory authorities

Standard 11

Supervisory authorities should require that the outsourcing institution has established supervisory authority access to relevant data held by the outsourcing service provider and, where provided for by the national law, the right for the supervisory authority to conduct on-site inspections at an outsourcing service provider's premises.

1. Supervisory authorities should aim to be satisfied that outsourcing institutions ensure that their outsourcing contracts with outsourcing service providers grant the supervisory authority the rights to information and, where provided for by the national law, to inspection, admittance and access (including access to databases), as well as the right to give directions or instructions, which the supervisory authority needs to exercise its supervisory functions.
2. Supervisory authorities should encourage outsourcing institutions to ensure that information may also be made available to the supervisory authority by the outsourcing service provider's external auditor.
3. Supervisory authorities should aim to ensure that their powers to issue orders or instructions to the outsourcing institution can be reliably enforced, without being compromised by instructions issued to the outsourcing service provider' by other bodies, so as to ensure the orderly performance of the outsourced activities.
4. The supervisory authorities should aim to ensure that they can obtain detailed information about any outsourcing processes which might undermine the stability of the consolidated group whose overall supervision is, ultimately, their responsibility.
5. In the case of outsourcing to service providers abroad, the outsourcing institution should be responsible for ensuring that the supervisory authority can exercise its information gathering rights, including its right to demand documents and audits, and, compatibly with the overall legal framework its inspection rights.
6. The requirement to cancel the outsourcing contract (under Standard 8.2(j)) should be properly justified by the supervisor on the basis of non-compliance with the provisions of these standards, in particular of those with regard to the safeguarding of rights of supervision and enforcement.
7. The outsourcing institution may – prior to outsourcing – consider in consultation with the supervisory authority what alternative measures could adequately mitigate the risks involved.

Standard 12

Supervisory authorities should take account of concentration risk.

1. Supervisory authorities should seek to identify any concentration risks at the level of the individual institution and on a sectoral level and seek to monitor these risks at a systemic level.