



EUROPEAN MONETARY INSTITUTE

SUP/97/30

BANKING SUPERVISORY SUB-COMMITTEE

**INTERNAL CONTROL SYSTEMS OF CREDIT INSTITUTIONS**

JULY 1997

## TABLE OF CONTENTS

	Page
<b>EXECUTIVE SUMMARY</b> .....	1
<b>INTRODUCTION</b> .....	3
<b>1 DEFINITION OF AN INTERNAL CONTROL SYSTEM</b> .....	4
<b>2 BASIC PRINCIPLES FOR A SOUND INTERNAL CONTROL SYSTEM</b> .....	6
2.1 Principles relating to an internal control system as a whole .....	7
2.2 Principles relating to administrative organisation .....	8
2.3 Principles relating to risk control .....	9
2.4 Principles relating to information systems .....	10
2.5 Principles relating to electronic information systems .....	10
<b>3 ROLE OF THE BOARD OF DIRECTORS AND THE SENIOR MANAGEMENT (HIGH-LEVEL CONTROL)</b> .....	12
3.1 Board of directors .....	14
3.2 Senior management .....	15
3.3 Audit Committee .....	16
<b>4 ROLE OF THE INTERNAL AUDITORS</b> .....	17
<b>5 ROLE OF THE EXTERNAL AUDITORS</b> .....	18
<b>6 ROLE OF THE SUPERVISORY AUTHORITIES</b> .....	19

### ANNEXES:

- 1: International definitions of an internal control system.
- 2: Summary of national legislative and regulatory frameworks.
- 3: Participants in the Sub-Group on Credit Institutions' Internal Controls.
- 4: Participants in the Banking Supervisory Sub-Committee.

## **EXECUTIVE SUMMARY**

The present report, prepared by the Banking Supervisory Sub-Committee with the assistance of a specific Sub-Group, contains general considerations on internal control systems of credit institutions from a supervisory perspective. Its main purpose is to assist banking supervisors and other interested parties in assessing the features and the adequacy of the credit institutions' systems of internal control. The report takes account of the work already undertaken on the matter in other international supervisory forums (such as the Basle Committee on Banking Supervision and the Groupe de Contact) and mainly draws upon the practical experience of the banking supervisors of the EU countries. In addition, it benefited from the comments made by a number of international auditing firms.

The report is based on the following main elements. First, the principal output of the report takes the form of a list of basic principles relating to all the relevant aspects which are regarded by banking supervisors as appropriate to promote the establishment and the maintenance of effective internal control systems at credit institutions. In selecting these principles, due consideration was given, owing to the constraints on resources faced by credit institutions, to the balance between the need to ensure the effectiveness of an internal control system and the need to avoid an excessive burden on the institutions. Moreover, due regard was paid to the differences existing in the EU countries in terms of legal and regulatory frameworks and supervisory practices.

Second, the report primarily provides a general and comprehensive overview of internal control systems, given that, at least in the supervisory field, work on the subject is normally confined to specific and particular aspects. Therefore, the emphasis is placed more on the extension of the analysis by attempting to offer a consistent systematisation of all the significant concepts, rather than on an in-depth examination of specific topics. The latter would clearly be needed in the event of further work in this area and/or actual implementation at the national level of the principles set out in the report.

Third, the report does not contain a conceptual analysis of an internal control system, i.e. its components or its relationship with the management process, etc., since this is a very difficult topic on which a variety of different views exist, but rather follows a pragmatic approach in this respect.

As regards its content, the report is divided into three main areas: definition of an internal control system, basic principles for a sound internal control system and the role of the various bodies involved in this area (board of directors, senior management, internal and external auditors, supervisory authorities).

The proposed definition of a system of internal controls - which is based on those definitions put forward by international organisations of professionals and adapted to the specific features of credit institutions - is intended to promote a common understanding of the concept among the EU banking supervisors.

The suggested principles for sound internal control systems refer, for the purpose of an orderly presentation, to the system as a whole and to four main aspects, namely administrative organisation, risk control, information systems and electronic information systems. These principles are intended to serve as basic guidelines to be followed by credit institutions so as to ensure the adoption and maintenance of adequate systems of internal control.

Most of the principles mirror internal control standards which are widely accepted at the international level for companies of all types. Many principles relating to the system as a whole, the administrative organisation and information systems fall within this category (e.g. the segregation of duties, personnel capabilities, written procedures, the completeness and accuracy of records, monitoring procedures, contingency planning, etc.). Other principles are also extensively adopted, but they refer specifically to credit institutions in order to take account of the peculiar characteristics of the banking activity. This applies, *inter alia*, to the principles concerning risk control (as the envisaged establishment of an independent risk management function) and those principles intended to cover credit institutions belonging to a group. Given the importance assumed by information technology in the banking business over the past few years, particular attention is devoted to the selection of internal control principles for the holding and use of data in an electronic form.

With regard to the role of the board of directors and the senior management of a credit institution in the field of internal control systems (so-called high-level control), the report takes account of the significant differences in terms of legislative and regulatory frameworks governing the functions of the two bodies in the different EU countries. Therefore, the two bodies, in the context of this report, are not regarded as identifying legal entities in the EU countries but rather as labelling specific decision-making functions within a credit institution.

The main idea to be put forward in this respect is that the board of directors bears ultimate responsibility for ensuring the establishment and maintenance of an adequate system of internal control, while the senior management is in charge of implementing the strategy set by the board by managing all the practical aspects relating to the effectiveness and efficiency of the system. Therefore, all those practices which are meant either to remind the board of its responsibilities in this area or to assist it in fulfilling its task are fully endorsed. Particular reference is made to the positive role which, in some EU countries and depending on certain conditions, could be played by an Audit Committee as an advisory body to the board.

The important role of the internal audit function, as described in this report, in promoting and ensuring the effectiveness of a system of internal control is fully recognised. Therefore, it is proposed that a system to review the effectiveness of an internal control system should be implemented at each credit institution and that, depending on its size, structure and risks inherent in its activities, the

establishment of an independent internal audit department should be pursued. Some basic principles governing the operation of the internal audit function are also proposed.

For the external audit function, the relevant role that it can play in favouring the adoption and maintenance of effective systems of internal controls has been acknowledged. Without intending to formulate detailed guidelines on the matter, it is suggested that the external auditors, depending on the legal and regulatory framework existing in each EU country, could be an appropriate body to undertake a periodical and thorough assessment of the internal control system of credit institutions. This approach has been endorsed by a number of relevant international auditing firms.

Finally, the report provides a brief description of the main tools used by banking supervisors when dealing with the internal control systems of credit institutions.

## **INTRODUCTION**

Internal control systems have always represented an important element of the operational and management structure of credit institutions. Over the few past years, the scope and the features of the control function have, however, been subject to a process of evolution within credit institutions in relation to the development of banking activity. The globalisation of markets, the internationalisation of credit institutions, the increase in competitive pressures and the wave of financial innovation with particular regard to the spread of derivatives instruments, as well as the development of information technology, have made the banking business more complex. Therefore, the internal control function, which in the past was mainly intended as a tool to reduce the likelihood of events such as fraud, misappropriation and mistakes, has since become more pervasive so as to encompass all the various risks incurred by credit institutions.

Banking supervisors attach great importance to the existence and maintenance of sound internal control systems at credit institutions. The promotion of adequate internal control constitutes, together with other regulatory tools (such as solvency ratio, risk limits, qualitative regulatory provisions, etc.), a crucial element by means of which supervisors aim at ensuring the integrity of credit institutions. From a supervisory perspective, the role of internal control is underlined in the Second Banking Coordination Directive (2BCD) which stipulates that national competent authorities will require credit institutions to have sound administrative and accounting procedures and adequate internal control mechanisms (Article 13 (2)).

The emphasis placed by banking supervisors on the adequacy of internal control systems has increased considerably over the past few years. This is due both to general concerns about the increasing complexity of banking activity and to the features of some specific banking failures. In particular, most of the recent banking crises have shown that serious losses have occurred mainly because of a breach of the main principles of internal control and because of a breakdown in internal control

procedures. Therefore, banking supervisors have made an effort, at the national and international level, to identify ways in which the effectiveness of credit institutions' internal control systems could be improved.

Against this background, the Banking Supervisory Sub-Committee decided to analyse the subject of credit institutions' internal control in depth with a view to identifying some guidelines which could assist banking supervisors in their activity. In particular, the main focus of this work is:

- to set out the scope and principles determining and guiding sound administrative and accounting procedures and internal controls, in accordance with Article 13 (2) of the 2BCD;
- to propose "best practices" for prudent internal controls in selected areas, including the so-called high-level control.

The present report, which relied heavily on the work carried by a Sub-Group set up by the Sub-Committee and benefited from comments made by a number of international auditing firms, is composed of six sections.

The first provides a general definition of an internal control system of a credit institution. The second includes a set of basic principles which supervisors expect credit institutions to follow when devising and implementing their internal control systems. These principles refer to a system of internal controls as a whole and to four main aspects, namely administrative organisation, risk control, information systems and electronic information systems.

The remaining sections contain general supervisory considerations on the role played by all the main bodies involved in the field of credit institutions' internal controls. In particular, the third focuses on the responsibilities of the decision-making bodies of a credit institution in setting up and maintaining an effective internal control system (high-level control). In this context, reference is also made to the possible role of the Audit Committee.

The fourth and fifth focus on the tasks performed by the internal and external audit functions, respectively, in promoting the existence of an adequate system of internal control at credit institutions. The last touches on the role played by banking supervisors in this field.

## **1. DEFINITION OF AN INTERNAL CONTROL SYSTEM**

There is no common definition of an internal control system (ICS) of a credit institution among the banking supervisors of the EU countries. A number of supervisors explicitly refer to the various definitions accepted at the international level and which are generally proposed for companies of all types by some organisations of professionals - such as the US Institute of Internal Auditors (IIA) and

the US Committee of Sponsoring Organisations of the Treadway Commission (COSO) (see Annex 1). Others adopt their own definition for the purpose of national regulations.

So as to achieve a common understanding among the EU banking supervisors of the concept of an ICS, the report adopts a definition which draws upon the two definitions set out in Annex 1 with some adaptations to take into account the specific features of credit institutions' activity. This definition is as follows:

*an ICS can be regarded as the process, including all the controls, financial or otherwise, effected by a credit institution's board of directors, senior management and other personnel to provide reasonable assurance that the following objectives are achieved:*

- a) accomplishment of established goals and objectives;*
- b) economical and efficient use of resources;*
- c) adequate control of the various risks incurred and the safeguarding of assets;*
- d) reliability and integrity of financial and management information;*
- e) compliance with laws and regulations as well as policies, plans, internal rules and procedures.*

It is important to underline that an ICS, regardless of how well designed it may be and how well it may function, can only provide reasonable assurance that the above-mentioned objectives are attained. The likelihood that these objectives will be achieved is affected by constraints inherent in all internal control mechanisms. Human error can always occur and changes in the market and/or technological conditions can invalidate the system, at least until the deficiencies have been detected and removed.

When devising an ICS, a credit institution faces constraints on resources and, therefore, the benefits of controls must be weighed against their cost. This entails a situation in which both quantitative and qualitative estimates and judgements must be made by the credit institution in order to strike the right balance between the cost of installing an ICS and the benefits derived from it.

Point a) involves an ICS aiming at ensuring that the goals and objectives, as set by the board of directors and the senior management in the context of the management process, are achieved by the credit institution. Therefore, this element of an ICS emphasises the effectiveness of the process intended to pursue the corporate objectives.

As regards point b), it should be noted that some of the internationally accepted definitions of an ICS include the economical and efficient use of resources in the list of objectives. This can be regarded as an objective of an ICS insofar as it is set as an objective by the board of directors and the senior management. However, its content goes beyond the scope of this report.

Point c) deals with risk control. This is a key factor of an ICS for credit institutions. The reference made in most definitions of an ICS to the safeguarding of assets seems to be rather limited in the

context of banking activity and more appropriate for industrial and commercial sectors. In the case of credit institutions, risk is not confined to the asset side of the balance sheet. Risk control must capture the risk incurred by a credit institution in all its activities (on and off-balance-sheet items and fiduciary activities). Such comprehensive risk control is essential for a credit institution's financial integrity.

The objective under point d) implies that an ICS should secure the existence at credit institutions of proper accounting records and reliable and complete financial and management information for the internal decision-making process and to ensure compliance with external requirements.

Under point e), an ICS must ensure that all the legal and regulatory provisions affecting a credit institution as well as all the internal rules set by the board of directors and the senior management, which are important internal control tools, are fully met. In this context, rules of conduct also have to be included.

## **2. BASIC PRINCIPLES FOR A SOUND INTERNAL CONTROL SYSTEM**

In this section, a set of basic principles is identified which banking supervisors would expect to be followed by credit institutions in devising and implementing an appropriate ICS. These principles are intended to promote the setting-up and maintenance of effective systems of control aimed at providing reasonable assurance that the objectives set out in Section 1 are achieved. The selection of these principles draws not only on the legislative and regulatory frameworks existing on the matter in the EU countries,<sup>1</sup> but also on the exchange of views and experiences among EU banking supervisors.

The principles have been grouped under five headings: an ICS as a whole and four main aspects usually relating to a credit institution's system of controls, namely administrative organisation, risk control, information systems and electronic information systems. This approach only constitutes a practical way in which to provide an orderly presentation of the principles and, therefore, does not entail the adoption of a particular conceptual framework for the components of an ICS. It is not easy - an ICS being a process - to associate each principle with a specific set of objectives as set out in the definition. However, the principles identified hereafter are aimed at attempting to attain these goals.

The fact that internal control procedures are not dealt with in this context requires some clarification. These procedures are the techniques by which a credit institution controls its business on a day-to-day basis. Credit institutions have a wide range of control techniques at their disposal, i.e. cross-checking, double signature, reconciliation of accounts, limited access to assets and information, limits to positions and risks, follow-up procedures for breaches, staff turnover, etc. Whatever the case, credit institutions should select the most appropriate control techniques, individually or in combination with others, in order to attain their control objectives.

---

<sup>1</sup> In all EU countries, in the context of implementing Article 13 (2) of the Second Banking Co-ordination Directive, the supervisory authorities have issued regulatory provisions covering credit institutions' ICSs (see Annex 2).



The adequacy of internal control procedures depends on a number of factors: the credit institution's organisation, its size and business, the particular area to which the technique is applied, etc. Therefore, an evaluation of the effectiveness of a wide range of control techniques without taking into consideration the framework in which they are set up is not possible. Consequently, the Sub-Committee does not see a need for identifying principles concerning these control techniques. However, it is of the opinion that any set of control techniques should comply with the general and specific principles of an ICS set out below.

## **2.1 Principles relating to an internal control system as a whole**

It is possible to identify a number of general principles which should be common to all credit institutions' internal control systems with a view to promoting their effectiveness. The following principles should at least be considered:

- a) an internal environment which gives adequate consideration to the control function within the credit institution should be promoted; the administrative organisation should be consistent with the pursuit of this objective;*
- b) the objectives of the corporate business and its policies should be clearly defined in accordance with the risk-taking attitude of the credit institution, supported by strategic plans and budgets and clearly communicated throughout the whole organisation;*
- c) an ICS should be comprehensive and cover all the relevant activities of a credit institution and be commensurate with the nature and size of these activities; particular attention should be paid to financial innovation and cross-border relationships with branches and subsidiaries;*
- d) every credit institution which has a credit or financial institution as a subsidiary should be responsible for ensuring that an adequate ICS is in place in the subsidiary. This should apply not only to subsidiaries whose inclusion in the scope of supervision on a consolidated basis is mandatory according to Community legislation,<sup>2</sup> but, where appropriate, to all the relevant entities of a group. However, this would not remove the responsibility of the management of the subsidiaries for their own ICS;*
- e) an ICS should be governed by a risk assessment concept to facilitate the identification, analysis and management of all the risks inherent in the banking activity;*
- f) an ICS should include appropriate measures to prevent fraud and other irregularities;*

---

<sup>2</sup> Directive 92/30/EEC on the supervision of credit institutions on a consolidated basis (Official Journal L 110 28 April 1992).

- g) an ICS should be supported by adequate information and communication systems to safeguard the flow of information necessary for control purposes; moreover, all the various aspects of an ICS should be adequately documented;*
- h) an ICS should be appropriate to the relevant legal framework ensuring compliance with laws and regulations;*
- i) an ICS should clearly identify the follow-up mechanisms in case of internal control failures;*
- j) an ICS should be reviewed on a regular basis and assessed from time to time.*

## **2.2 Principles relating to administrative organisation**

This section refers to the organisational structure (roles and responsibilities) and the operational procedures adopted by a credit institution. Each credit institution should have an administrative organisation adapted to the nature, scope and complexity of both the activities undertaken and the inherent risks. The establishment and maintenance of a sound administrative organisation is an essential aspect of an ICS which should be based on the following elements:

- a) credit institutions should have a clearly defined organisational structure allocating duties and responsibilities and identifying reporting lines; this allocation should ensure that there are no gaps in the reporting lines and that a proper level of management control is exerted over every activity; within matrix management structures special attention should be paid to ensure that this principle is applied;*
- b) an effective segregation of duties should be established in order to avoid the risk of manipulation and errors; in this context, it is essential that internal control mechanisms should be independent of the activities to be controlled;*
- c) personnel should have capabilities commensurate with their responsibilities and should be aware of these;*
- d) operational procedures should be laid down in writing for all relevant transactions and personnel should be familiar with these;*
- e) each process should incorporate its own control procedures to ensure that all transactions are authorised, recorded and processed correctly;*
- f) access to assets and information should be restricted to authorised personnel;*
- g) contingency planning, well communicated to the staff and tested on a regular basis, should be in place to ensure continuity of service and the rapid re-establishment of control over business;*

*h) the administrative organisation should be monitored and updated regularly to ensure its effectiveness.*

### **2.3 Principles relating to risk control**

In undertaking their activity, credit institutions bear different types of risk. These can be classified into two main categories: quantifiable (credit, market, liquidity, etc.) and non-quantifiable (fraud, misappropriation, operational risk, legal risk, reputational risk, etc.). The control of all these risks is another important aspect of an ICS. Credit institutions, depending on the size and complexity of their activities, should develop risk management systems - namely the process of identifying, measuring (in the case of quantifiable risk) and controlling risk exposures - with regard to all the main categories of risk incurred.

In the field of risk management, extensive work has already been undertaken in other international forums with regard to the varying categories of risk borne by credit institutions.<sup>3</sup> Therefore, the report does not undertake an in-depth analysis of this subject and it is necessary to take account of the fact that the main principles of risk management need to be adapted to the specific areas in which risks arise. In this context, it is deemed sufficient to recall the main principles - which refer to both categories of risks (quantifiable and non-quantifiable), unless specified otherwise - as follows:

- a) credit institutions should consider the need to establish an independent risk management function overseeing all activities and covering all aspects of risk;*
- b) for each type of risk, adequate risk-taking policies should be established; this entails the setting of appropriate operational limits for quantifiable risks and the definition of adequate procedures to mitigate non-quantifiable risks;*
- c) risk policies should include the authorisation procedure required for engaging in new activities. All individuals involved should be fully aware of the risks associated with the new activity and the ways in which it is integrated into the overall risk management system;*
- d) compliance with policies and limits should be monitored on a continuous basis and excesses beyond operational limits, as well as breaches of risk alleviation procedures, should be promptly assessed and reported. Clear follow-up procedures for breaches should be set up;*
- e) policies and limits should be reviewed periodically in relation to market developments.*

The principle under point a) deserves particular clarification. In recent years, credit institutions in some EU countries have reacted to the increasing complexity of their activity arising from intensified competition in the financial markets and the development of information technology, by setting up a

---

<sup>3</sup> Reference can be made, inter alia, to the work conducted by the Basle Committee on Banking Supervision in this area which was reflected in the Compendium issued in April 1997.

network of committees - in different forms according to the size and structure of the credit institutions - which are mainly intended to ensure that all risks incurred are identified and adequately controlled. Regardless of the different denominations, these committees are normally classified in relation to the types of risk managed. Examples of these committees, to be added to the more traditional credit risk committees, are those which focus on market risks and the so-called Asset and Liability Committees, the main purpose of which is to optimise the credit institution's earnings through management of the interest rate risk inherent in the balance sheet.

Against this background, and where justified by the size and structure of a credit institution, the decision by credit institutions to establish an independent risk control unit and a network of risk management committees in order to improve their performance is to be seen in a positive light, provided that the respective duties and competences are clearly defined.

#### **2.4 Principles relating to information systems**

The information system deals with the recording of operations and the flow of information for internal decision-making and for external purposes and constitutes another important aspect of an ICS. As for the administrative organisation, the information system should also be commensurate with the features, size and complexity of the business undertaken by a credit institution. Basically, it should be ensured that the credit institution's transactions are not recorded outside the general accounting system in order to avoid cases of fraud and misappropriation in the banking business. In order to ensure the existence of an effective information system, the following basic principles should be considered:

- a) each valid transaction should be recorded accurately in the proper period with an adequate degree of detail and on a timely basis;*
- b) there should be an audit trail making it possible to reconstruct the transactions in their chronological order, to support all information with original documents and to account for movements in balances from one statement to the next;*
- c) the board of directors, senior management and other personnel should be able to receive, on a timely basis, adequate information to enable them to fulfil their obligations;*
- d) information should be made available to the supervisory authorities in due time;*
- e) information for external purposes (annual accounts, supervisory reporting, etc.) should comply with the relevant laws and regulations.*

#### **2.5 Principles relating to electronic information systems**

The use of information technology (IT) entails additional risks for credit institutions. Examples include the loss of data and programs due to inadequate security arrangements, equipment or systems failure and inadequate backup and recovery procedures; inaccurate management information as a result of poor systems development procedures; and the unavailability of alternative, compatible

facilities in the event of prolonged equipment interruptions. Such losses and interruptions can cause serious difficulties for an institution and, in extreme circumstances, could jeopardise its ability to continue conducting its business. Perhaps of greater importance is the danger that decisions may be based on unreliable or misleading information produced by badly designed or poorly controlled information systems.

For all these reasons, credit institutions should have the necessary know-how, organisational and internal controls to hold and process information in an electronic form, both in the case of this being carried out through a mainframe set-up and in the case of credit institutions relying on a personal computer system. The principles identified below apply to both situations, although they should be seen in each specific context. In particular, it should be noted that in a mainframe situation, electronic information systems are normally managed through an IT department, whereas in personal-computer-based systems this occurs through IT sections. A set of general principles aimed at safeguarding IT systems should include at least:

- a) setting procedures for formulating, approving, implementing and reviewing the strategic and short-term IT planning as part of credit institution's business plan. IT strategy and budget should be approved by the board of directors and/or senior management in order to ensure the existence and maintenance of an appropriate technical platform, according to the current and future needs of the institution;*
- b) defining policies, standards, procedures and controls for all aspects related to IT activities. They should facilitate co-ordination with organisational functions and between the parts that either maintain or use electronic information, and should also serve as a basis for the management planning, control and evaluation of those activities. This co-ordination function could be carried out, where appropriate, by a Steering Committee;*
- c) establishing the appropriate independence of the IT function from the user function. The IT function should be responsible for the operation and development of an electronic information system, while the user function should ensure the correctness of each piece of information processed;*
- d) maintaining an adequate segregation between the systems development and computer operation environments so that each can only access directly the information of the other through controlled standard procedures. Duties of the personnel in charge of operating system implementation and maintenance, the administration of logical security and database administration should also be segregated;*
- e) guaranteeing that the internal audit function is capable of ensuring the adequacy and effectiveness of the IT internal controls. Internal auditors should be consulted during the systems development process to ensure that adequate controls and audit trails are incorporated into the systems.*

- f) *establishing and maintaining systems development and quality control methodology that could reasonably ensure that systems comply with the functions for which they were designed, and produce standardised documentation that facilitates their use (by users and operators) and future maintenance;*
- g) *setting up procedures for the approval and acquisition of programs and equipment, and for contracting external services (outsourcing) to ensure that they cover the needs for which they were acquired or commissioned, guarantee the continuity of service and adapt to the standards of the institution;*
- h) *providing systems with controls and audit trails (including backups) to ensure the veracity and integrity of input data and results, the authorisation to use them, the resetting of processes in the event of interruption and the auditability of transactions;*
- i) *establishing logical security procedures and controls to restrict access to data and programs to authorised individuals (passwords, encryption, etc.) and to report and investigate security violations;*
- j) *setting up physical security procedures and policies to minimise operations interruption risks (fire, flood, electricity supply, etc.) and to restrict access to sensitive material to authorised individuals (IT equipment, tapes, documentation, etc.);*
- k) *defining and maintaining a contingency plan to ensure the continuity of vital operations and to allow, within a reasonable time, the recovery of normal operation following any unexpected interruptions for different contingency levels. The contingency plan should be subject to periodical testing.*

In this context, it should be further emphasised that the scope and nature of an effective control system should take account of the level of reliance on information technology and the size and complexity of the institution.

### **3. ROLE OF THE BOARD OF DIRECTORS AND THE SENIOR MANAGEMENT (HIGH-LEVEL CONTROL)**

This section deals with the role which banking supervisors would expect the board of directors and the senior management of a credit institution to play in the field of internal control systems. In particular, it focuses on so-called high-level control, notably the set of controls instituted and exercised by these bodies.

In general, the board of directors can be regarded as the body elected by the general meeting which defines the strategy and general policies and which supervises the management of a credit institution, whereas the senior management consists of senior executives responsible for the business management

of the institution. Hence, the board of directors invests the senior management with decision-making powers and powers of representation.

There are, however, significant differences in legislative and regulatory frameworks as well as varying practices across countries and institutions as regards the functions actually performed by the boards of directors and the senior management within a credit institution. In some EU countries, the board has the main, if not exclusive, function of supervising the senior management so as to ensure that the latter fulfils its tasks (for this reason, in some cases, it is known as a supervisory board). This means that the board has no executive functions. In other EU countries, by contrast, the board has a broader competence in that it lays down the general framework for the management of a credit institution.

Owing to these differences, the notions of the board of directors and the senior management are used in this context not to identify legal entities in the EU countries, but rather to label two decision-making functions within a credit institution. The first is the supreme decision-making activity concerned with ultimate responsibility for the sound administration of an institution, and the second is the more operational decision-making activity concerned with responsibility for the day-to-day management of an institution.

Both bodies play a crucial role in the field of a credit institution's internal controls. The board of directors is ultimately responsible for ensuring the establishment and maintenance of a sound system of internal controls, whereas the senior management is in charge of implementing the strategy set by the board by managing all the practical aspects relating to the effectiveness and efficiency of the ICS.

It should be underlined that the positive attitude of the board of directors and the senior management in respect of the control function is deemed to be essential for the setting-up and maintenance of an environment within the credit institution which promotes an appropriate level of control awareness among the entire personnel.

In this context, the attention paid to the control function should be evidenced in the minutes of the meetings of the board of directors and its committees, as well as in the management reports and the possible inclusion in the annual report of a paragraph dealing with the status of the credit institution's ICSs. Without favouring any particular arrangement, the Sub-Committee generally endorses all initiatives which contribute to reminding the board of directors and the senior management of their respective responsibilities in the field of internal control.

In the following three sections, the specific role of the board of directors and the senior management in the area of an ICS is analysed in detail, together with a description of the function of the Audit Committee. It should be noted that the distribution of competences between the board of directors and the senior management envisaged below should be considered in a flexible manner, in relation to the specific legislative and regulatory features of each EU country.





### **3.1 Board of directors**

The board of directors is, in this context, the body which defines the general framework for the management of a credit institution and shoulders ultimate responsibility for its sound administration. So as to comply with its obligations, the board has to ensure the effective supervision of the activities undertaken by the credit institution. This supervision involves an appropriate level of competence and sufficient time in which to be adequately informed about the institution's condition and management. As regards the specific field of ICSs, the board has ultimate responsibility for ensuring that an adequate system of internal controls is established and maintained. In more detail, this duty is:

- a) to define the main responsibilities at board level and the reporting lines between the board and the senior management;*
- b) to select and define the responsibility of senior managers and assess their performance;*
- c) to approve the general organisational structure of the institution, to ensure that duties and responsibilities are delegated in an appropriate fashion; and to review the delegation system, where appropriate;*
- d) to be fully aware of and understand the risks incurred by the institution, and to know how and to approve the way in which they are evaluated and controlled;*
- e) to approve both risk policies - including risk measurement, control mechanisms and authorisation procedures for existing activities and for engaging in new business - and general limits vis-à-vis the major types of quantifiable risk, and regularly to review exposure to these risks; the board should be informed promptly of major excesses beyond limits;*
- f) to ensure that policies and procedures are set up to mitigate the vulnerability to non-quantifiable risks, such as operational risk, reputational risk, litigation risk, the risk of business interruption and risks arising from frauds, errors and unauthorised access, and to ensure that legislative, regulatory and statutory provisions are met;*
- g) to ensure that a correct, complete and timely information system is set up that allows for an understanding and evaluation of the institution's economic and financial situation, an effective decision-making process based on an adequate evaluation of the impact of any decision and the prompt identification of any breaches of procedures or controls;*
- h) to ensure that the internal audit function is properly defined, has an appropriate standing within the institution, is adequately resourced and functions properly;*

- i) to ensure that the ICS is periodically assessed also in relation to specific changes within the business environment;*
- j) to ensure that adequate mechanisms are in place so that senior managers report back to the board on their findings regarding the ICS on a timely basis;*
- k) to be informed of the conclusions reached by internal and external auditors and, where applicable, by supervisory authorities in the course of their on-site examinations of the institutions and/or group of companies. In the event that deficiencies are noted as a result of this examination, the board should define mechanisms for assigning responsibilities for their correction and thereafter ensure that the proper measures are taken.*

### **3.2 Senior management**

In this context, the senior management is the body responsible for the actual management of a credit institution on a day-to-day basis with a view to achieving the general objectives set by the board. In the specific field of ICSs, the senior management has the duty of implementing the strategy defined by the board by managing all the practical aspects relating to the effectiveness and efficiency of the system of internal controls. In particular, this duty is:

- a) to set qualitative and quantitative objectives for each banking activity in line with the credit institution's strategy, as set by the board;*
- b) to set up an organisation plan allowing for the clear definition of delegations and the effective segregation of duties between operational, administrative, accounting and control tasks;*
- c) to take the necessary measures to enable activities to be conducted by qualified staff with a sound technical ability and adequate experience;*
- d) to set up measures to safeguard property and protect assets;*
- e) to establish and maintain adequate risk identification and measurement systems; to ensure the adequate control of risks, particularly when such risks arise from complex and specialised activities, without engaging in business which cannot be adequately controlled;*
- f) to set up methods to safeguard processing reliability and to secure the maintenance of complete and accurate information for transactions;*

- g) *to establish and maintain management information systems covering the whole range of activities of the institution and financial group, where appropriate; to set up assets, liabilities and off-balance-sheet evaluation standards and profit and loss recording standards;*
- h) *to establish the administrative, operational and control mechanisms required to comply with laws, regulations, policies, plans, internal rules and procedures and to ensure that these are duly communicated to and applied throughout the entire organisation by all the staff members;*
- i) *to ensure the implementation of remedial actions related to internal control weaknesses outlined in the reports drawn up by internal auditors, external auditors and supervisory authorities, or stemming from information originating from any other source; to ensure the continuity of service by establishing adequate contingency plans;*
- j) *to report to the board of directors at least once a year on the scope and performance of the internal control systems.*

### **3.3 Audit Committee**

An Audit Committee (AC), although its features and denomination may vary across countries and institutions, is normally regarded as an advisory body to the board of directors or a sub-committee of the board which consists of non-executive directors. Internal and external auditors may take part in its meetings. In undertaking its tasks, the AC does not bear specific responsibilities as do the board and the senior management, since it is simply intended to favour lines of communication among the various parties involved and to assist the board in carrying out its duties.

It is generally recognised that the main tasks of an AC are as follows:

- to maintain open lines of communication among the board of directors, the senior management and the internal and external auditors to exchange information and views;
- to oversee and appraise the independence, quality, cost-effectiveness and scope of the internal audit function;
- to carry out an independent review of the annual financial statements and other relevant external information;
- to provide advice on the appointment of the external auditor which falls under the competence of the general meeting;
- to assure the board that the institution is operating in compliance with laws and regulations;
- to review the adequacy and effectiveness of the credit institution's overall ICS.

Depending on the size and the ownership structure of a credit institution, as well as on the possible existence of bodies with similar functions, according to national legislation and regulations, the

establishment of ACs could be recommended, where appropriate, to assist the board in fulfilling its task to ensure the existence and maintenance of an adequate system of controls. In the event that ACs are set up, it is necessary for written terms of reference to be formulated by the board which deal clearly with the membership, authority and duties of the Committee.

In some EU countries the internal audit function at credit institutions is directly responsible to the board of directors, or special bodies are able to undertake functions similar to those of the AC. In such cases, the setting-up of ACs could represent an additional layer to the structure of internal control.

#### **4. ROLE OF THE INTERNAL AUDITORS**

Internal audit (IA) is a key element of a system of internal controls which is distinct from the primary control function of exercising day-to-day control over transactions and operations. It is an independent appraisal function established by the board of directors and the senior management to examine and evaluate the credit institution's activities as a service to the organisation. Although the precise features of the IA function may differ across countries and institutions, it is generally recognised that the internal auditors carry out the following five tasks:

- regular review of the scope, effectiveness and efficiency of internal control systems, including the implementation of policies and procedures, as set by the board of directors and the senior management;
- review of the application and effectiveness of risk management procedures;
- review of information systems, including electronic information systems, accounting and other records;
- testing of both transactions and the operation of specific internal control procedures;
- special investigations.

The specific features of IA normally depend on the control environment created by the board of directors and the senior management, the size and the structure of the credit institution and the risks inherent in its activities. According to the legal and regulatory framework existing in particular EU countries, the IA function is responsible either to the board of directors or to the senior management of a credit institution. In some cases, the possibility of outsourcing the internal audit activity is also provided for.

Given the importance of the five tasks listed above for the effectiveness of an ICS, each credit institution should ensure that the tasks are carried out adequately and, depending on its size, structure and the risks inherent in its activities, should pursue the establishment of an independent IA department, where appropriate. The latter is of particular importance when the credit institution belongs to a financial group operating internationally. The activity of the internal auditors should comply with the following general principles:

- a) it should be independent of the operational management which is responsible for the day-to-day control activity;*
- b) it should have access to all the activities of a credit institution (head office and domestic and foreign branches) and of its subsidiaries;*
- c) it should be adequately structured and resourced with individuals qualified to perform their function;*
- d) it should have adequate reporting lines which safeguard its independence.*

## **5. ROLE OF THE EXTERNAL AUDITORS**

In all EU countries the main task of the external audit function is to give an opinion on or to certify the annual accounts of credit institutions. This entails an assessment of whether the financial impact of the credit institution's business has been correctly reflected in the financial statements. In this context, the external auditors are interested in the credit institution's system of internal control only insofar as it is important to the financial statements. In particular, the external auditors assess the operation of an ICS only to the extent that they intend to rely upon the controls to form their opinion of the financial statements. As a consequence, according to their own professional standards, the external auditors are not obliged to give a specific opinion on the adequacy of a credit institution's ICS when auditing the annual accounts.

However, the work undertaken in this field is nevertheless important as emphasised in the report on "The audit of international commercial banks" issued in 1990 by the International Auditing Practices Committee of the International Federation of Accountants, after consultations with the Basle Committee on Banking Supervision. In particular, the report stresses that in most situations - especially in the case of internationally active banks - the external auditors need to rely heavily on the credit institution's ICS. To this end, the external auditors have to undertake a careful evaluation of the internal control system in order to assess the extent to which they can rely on the system in determining the nature, timing and scope of their other audit procedures.

It is general practice within the auditing profession to provide management with a letter describing the main weaknesses found in the internal controls during the annual audit and making the necessary recommendations.

In some EU countries external auditors are required by the supervisory authorities to provide a specific assessment of the scope, adequacy and effectiveness of a credit institution's ICS, including the internal audit system. In this case, the evaluation of the system of controls is not part of the analysis of the annual accounts but constitutes a specific task in itself. In performing this duty, the external auditors,

who must comply with the requirements of independence and competence, can make use, in some cases, of the reports of the internal auditors.

The role of external auditors in the area of internal controls has been examined over the past few years in a number of industry studies referring to companies of all types. The main finding of these analyses is that the effectiveness of an ICS is likely to improve if external auditors are involved in the process of assessing the system of controls.

From a supervisory perspective, the positive role that the external auditors can play in this field has also been recognised at the international level. A further step in this direction has been the “post-BCCI” Directive,<sup>4</sup> by which external auditors of a credit institution have a duty to report to the supervisory authorities any fact or decision which:

- constitutes a material breach of the laws, regulations and administrative provisions;
- affects the continuous functioning of the credit institution;
- leads to a refusal to certify the accounts or to express a reservation.

Moreover, in the Amendment to the Capital Accord to incorporate market risk adopted by the Basle Committee on Banking Supervision in January 1996, external auditors are included among those who are entrusted (the others being the supervisory authorities) with the task of ensuring the validation of internal models used by credit institutions to measure market risk.

Against this background, the Sub-Committee is of the opinion that the external auditor, depending on the legal and regulatory framework existing in each EU country, could be an appropriate specialist to undertake a periodic and thorough assessment of a credit institution’s ICS (see principle j in Section 2.1 above). In this context, specific aspects which deserve particular attention are the scope of the assessment (whether or not it cover the objectives of the “*accomplishment of established goals and objectives*” and the “*economical and efficient use of resources*” of an ICS) and its timing (whether it should be carried out within the context of the external audit of the annual accounts or whether it should be independent of this procedure).

## **6. ROLE OF THE SUPERVISORY AUTHORITIES**

It is in the interest of supervisory authorities to promote the existence and maintenance of sound systems of internal control at credit institutions. The existence of strong ICSs is in fact regarded by supervisors as one of the conditions necessary to secure the integrity of credit institutions. Moreover, the 2BCD stipulates that supervisory authorities will require credit institutions to have adequate

---

<sup>4</sup> Directive 95/26/EC amending various directives in the field of financial services with a view to reinforcing prudential supervision (Official Journal 168 18 July 1995).

internal controls. In this context, supervisory authorities have three instruments at their disposal: regulation, off-site monitoring and on-site inspections.

In all EU countries, in the context of implementing Article 13 (2) of the 2BCD, the supervisory authorities have issued regulatory provisions covering the credit institutions' ICSs. Although the extent of this regulation varies across countries, general provisions are normally laid down in respect of some areas of an ICS, even though there does not seem to be any comprehensive or precise regulation of this subject (see Annex 2). In many cases, the regulation includes a definition of the ICS, some basic principles aimed at promoting an adequate system of controls (both in the context of the licensing procedure and on an ongoing basis) and the main duties of the various bodies involved in the field of internal control.

Off-site monitoring is the surveillance carried out by supervisors on a continuous basis which relies on the credit institution's reporting, discussions with the management in addition to other relevant information. This activity is mainly intended to assess the situation of credit institutions in key financial areas (capital adequacy, asset quality, earning, liquidity, etc.). Supervisors, however, also attempt to evaluate organisational aspects of a credit institution, including its system of internal controls, on the basis of all the information available.

In particular, in some EU countries, the board of directors of a credit institution is required to provide the supervisory authorities with an annual statement concerning the status of the internal control system based on the information stemming from all the relevant sources (reports of audit committees, internal and external auditors, etc.).

In other EU countries credit institutions are required to forward copies of the internal auditors' reports to the supervisory authorities upon request. In general, this request is confined to particular cases, for instance when there is some doubt about the appropriateness or effectiveness of the credit institution's ICS or where the report is expected to contain information on operations of special interest. Furthermore, in some EU countries, supervisory authorities are informed on a regular basis that follow-up actions have been agreed and implemented to remedy any shortcomings outlined by the internal auditors.

Finally, in some EU countries supervisory, authorities also rely on the information provided by the external auditors. In particular, they can obtain access to the management letters or to the special reports, mentioned in Section 5 above.

In most EU countries on-site inspections represent a relevant tool for the purpose of banking supervision. Inspections enable supervisors to form a direct judgement of the management of credit institutions, to gain a better understanding of the institutions' organisation and operations, and to verify the consistency of information provided to the supervisory authorities. Therefore, on-site inspections constitute an important opportunity to assess the effectiveness of credit institutions' ICSs.





## INTERNATIONAL DEFINITIONS OF AN INTERNAL CONTROL SYSTEM\*

<b>Institute of Internal Auditors (IIA)</b>	<b>Committee of Sponsoring Organisations of the Treadway Commission (COSO)</b>
<p>Internal control is actions taken by management to plan, organise and direct the performance of sufficient actions so as to provide reasonable assurance that the following objectives will be achieved:</p> <ul style="list-style-type: none"> <li>• the accomplishment of established objectives and goals for operations and programmes;</li> <li>• the economical and efficient use of resources;</li> <li>• the safeguarding of <b>assets</b>;</li> <li>• reliability and <b>integrity of information</b>;</li> <li>• compliance with <b>policies, plans, procedures, laws and regulations</b>.</li> </ul>	<p>Internal control is a process effected by the board, management and other personnel designed to provide reasonable assurance regarding the achievement of the following objectives:</p> <ul style="list-style-type: none"> <li>• effectiveness and efficiency of operations, i.e. basic business objectives: performance and profitability goals, safeguarding of <b>resources</b>;</li> <li>• reliability of <b>financial reporting</b>;</li> <li>• compliance with applicable laws and regulations.</li> </ul>

\* The main differences between the two definitions appear in bold.



**CREDIT INSTITUTIONS' INTERNAL CONTROL SYSTEMS**  
**Summary of national legislative and regulatory frameworks**

**BELGIUM**

Article 20 of the Law 22/3/93 implements Article 13 (2) of the Second Banking Co-ordination Directive (2BCD). It makes the existence of adequate administrative and accounting procedures and internal control procedures an explicit condition for engaging in banking activities.

The Circular of 6 April 1987, issued by the Banking and Finance Commission (BFC), sets out the basic principles governing the internal audit, its status, the nature and scope of its function, its organisation and execution. It contains the recommendations that the BFC feels are necessary in this field.

The Circular of 17 April 1990, issued by the BFC, regulates the internal organisation and monitoring of credit institutions' operations on the money and foreign exchange markets. The regulation intends to cover all operations which are carried out by credit institutions' dealing rooms. It lays down basic principles relating to the organisation, control and monitoring of these activities in order to ensure that assets are adequately safeguarded, the information system is reliable and the business is conducted in an orderly manner. The Circular of 1 September 1994, issued by the BFC, requires credit institutions to follow the risk management guidelines issued by the Basle Committee on Banking Supervision in July 1994.

The Circular of 21 October 1993, issued by the BFC, deals with independent agents operating for the account of credit institutions. Professionally speaking they carry out transactions in the name of and for the account of a credit institution which belong to the institution's activity through their direct contact with customers. The regulation stipulates, inter alia, that credit institutions must subject the activities of the independent agents to adequate administrative and accounting procedures.

The role and the functioning of the credit institution's board of directors and that of the executive body (Management Committee) are set out in the protocol on the autonomy of the banking function.

**DENMARK**

Article 54 of the Act on Public Limited Companies lays down the rules for internal control procedures. These rules also apply to credit institutions as set out in Articles 1, 12, 15e, 15f and 15j of the Bank Act and implement Article 13 (2) of the 2BCD. The provision defines the respective roles of the board of directors and the senior management in respect of the administration of institutions' assets and bookkeeping.

Article 18 of the Bank Act deals with the administrative organisation of credit institutions. It states that the board of directors must draw up written instructions for the main business areas and clarifies the division of work between the board of directors and the senior management. In January 1996 the Danish Government proposed a new Article 18a of the Bank Act which lays down basic principles in this field (sound administrative and accounting procedures, written procedures for the main business

areas and adequate internal control mechanisms) and gives the power to the Financial Supervisory Authority (FSA) to issue guidelines on this matter. The Executive Order of 29 November 1995, issued by the FSA, regulates the specific issue of transactions among institutions belonging to the same group.

Accounting and information systems are also covered by the general provisions mentioned above. Emphasis is placed on the written procedures in accounting departments, the operation and separation of accounting/reporting functions and the internal reporting to the senior management and the board. As to electronic information systems, the FSA issued an Executive Order which stipulates the mandatory establishment on an IT internal audit department and identifies its specific tasks.

The Executive Order of 5 December 1989, issued by the FSA, deals with internal audit. It imposes the establishment of this function for credit institutions of a certain size (total assets exceeding DKK 750 million). It also defines the main obligation of the internal auditors as being the assessment in their annual report of the effectiveness of the internal control system.

## **GERMANY**

Section 32 of the Banking Act lays down the requirements for the granting of a licence to conduct banking business. These requirements include, inter alia, a business plan showing the nature of the planned business, the organisational structure and the planned internal monitoring procedures. Section 13 of the Regulation of 6 July 1993, issued by the Federal Banking Supervisory Authority (FBSO), on reports and the submission of records under the Banking Act, specifies the requirements for granting a licence in greater detail.

The Regulation of 23 October 1995, issued by the FBSO, lays down minimum requirements for the trading activity of credit institutions. The requirements are based on the risk management guidelines for derivatives activities issued by the Basle Committee in July 1994.

The Regulation of 28 May 1976, issued by the FBSO, lays down requirements for internal audits at credit institutions. These requirements cover the status, staff, scope, functioning and reporting lines of an internal audit function (carried out by a department or, depending on the size of the institution, another body).

Section 5 of the Regulation of 21 July 1994, issued by the FBSO, on the content of the external auditor's reports on a credit institution's annual and interim accounts, states that the report of the external auditor shall include a discussion of the credit institution's legal, financial and organisational basis. Inter alia, these include: the responsibilities of managers, organisational structure, organisational structure of the accounting system, and organisation of the internal audit system. The annual report of the external auditor is also sent to the supervisory authorities. Section 9 of the same Regulation provides more detail on the auditor's assessment of the institution's accounting organisation.

On 16 October 1992 the FBSO issued a Pronouncement on the utilisation of electronic data processing facilities located outside Germany by domestic credit institutions and German branches of foreign credit institutions for accounting purposes.

## **GREECE**

Article 18 (2) of the Banking Law (2076/92) implements Article 13 (2) of the 2BCD. Apart from this provision, there is no specific regulation of credit institutions' internal control. The introduction of a detailed regulation on the matter is currently under consideration.

## **SPAIN**

Article 43 of the Banking Law 26/88 implements Article 13 (2) of the 2BCD. This law is supplemented by Royal Decree 1245/95 which stipulates that the board of directors must establish adequate operating rules and procedures to enable all members to comply at any given time with their obligations and to carry out their responsibilities in accordance with the regulations governing credit institutions, the Company Law or other applicable provisions (Article 2.1.G).

Article 32 of Royal Decree 1243/92 states that credit institutions must continuously monitor interest rate and liquidity risks through adequate internal control procedures which may be subject to requirements or standards laid down by the Banco de España. This gave rise to Rule 4.4 of Circular 5/93, issued by the Banco de España, which introduces some guidelines for the risk policies defined by the credit institutions in this field and the related role of the boards of directors. In this context, specific provisions cover the internal audit function.

Credit institutions which are authorised to access the interbank telephone market settled at the Banco de España are subject to Rule 5 of Circular 14/1992, issued by the Banco de España. This imposes on market members the obligation to establish effective management and information systems to ensure adequate knowledge and control of all risks (credit, market, liquidity and others) incurred in the trading, clearing and settlement of interbank deposit transactions. Internal control systems must be reviewed regularly by internal auditors and by the board of directors.

Among the accounting regulations issued by the Banco de España, Rule 6 of the Circular 4/91 specifies that assets, liabilities, commitments, income and expenses must be clearly identified in the accounting base from which the published and prudential statements are derived. Credit institutions are requested to set up analytic accounting procedures that allow them to calculate the expenses and income of their different products, services, centres, departments, lines of business and any other source which may be useful for management purposes. Additional records needed to produce management information must be established with particular regard to the different risks arising from the credit institution's financial activities.

In February 1997 a Working Group consisting of experts from the Banco de España, the main banking associations (AEB and CECA) and auditing firms issued a report entitled the "Internal Control Systems of Treasury Activities" in order to provide guidance on sound risk management practices for Treasury activities. The report identifies the main risks in this area, outlines the role of the board of directors and senior management and highlights the key elements of a sound management process; it also contains a detailed set of applicable operational procedures. The report was intended for general application, as it is based on practices currently used or recommended by the main Spanish banks, even though their specific implementation will depend on the complexity and range of the activities undertaken by individual banks or banking groups.

## **FRANCE**

Regulation 97/02 of 21 February 1997 (which will come into force in October 1997) was issued by the Banking Regulatory Committee (BRC) and contains the basic provisions covering the risk management and internal control systems of credit institutions (it repeals Regulations 90/08, 90/09, 88/04 and 91/04). The Regulation consists of six sections, the first of which sets out principles and definitions. The second focuses on the organisation of internal controls and requires credit institutions to comply with all the administrative procedures, particularly daily controls and respective efficiency checks; it also addresses the requirements for an efficient internal control system (independence, effective competence, completeness and periodic review). The third specifies detailed requirements regarding the control of valuations and effective book-keeping. It imposes an audit trail for accounting and financial information and requires EDP security controls. The fourth is intended to identify the appropriate measurement procedures for credit institutions' main risk exposures (counterparty risk, market risk, overall interest rate risk and settlement risk). The fifth requires credit institutions to set up risk monitoring and control systems with regard to all risks. The sixth clarifies the way in which the decision-making body (board of directors) should be involved in the follow-up to internal controls. It also requires the annual drawing-up of two reports to be sent to the statutory auditors and to the Banking Commission: the first report contains an assessment of the way in which the internal control function is carried out, the second focuses on risk measurement and the monitoring of all credit institutions' risk exposures on the basis of the information transmitted to the decision-making body.

Regulation 90/07 of 20 June 1990 as amended by regulation 94/03 of 8 December 1994, issued by the BRC, deals with supervision of interbank risks. Credit institutions operating in the interbank market are required to set up a system of internal monitoring of their exposures for each of their banking counterparties and a system of internal monitoring of the distribution of their sources of interbank financing.

## **IRELAND**

Article 16.1 of the Second Banking Directive Regulations, 1992, implements Article 13 (2) of the 2BCD. Section 3 of the Licensing and Supervision Requirements and Standards for Credit Institutions, issued in November 1995 by the Central Bank of Ireland, includes some principles relating to internal control which are regarded as being appropriate for a sound management of credit institutions. These principles relate to the existence of an appropriate organisational structure, effective operating policies and procedures for the ongoing business, adequate risk management systems, the effective review and assessment of significant operations, and the avoidance of conflicts of interest.

## **ITALY**

Article 53.1 (d) of the Banking Law of 1 September 1993 implements Article 13 (2) of the 2BCD. Specific provisions covering internal control can be found in Chapter XXXIX of the instructions for credit institutions, issued by the Banca d'Italia. These provisions:

- lay down guidelines for the activity of the board of auditors whose main duty is to ensure that banking activity is performed in accordance with relevant laws, regulations and technical standards for banking business;
- set the principles governing the organisation and activities of the internal inspectorate department of credit institutions (internal audit) with a view to ensuring its effectiveness and efficiency;

- define the guidelines for the control of the activities carried out by foreign branches of Italian credit institutions. In particular, these guidelines cover the organisational arrangements to be adopted by the relevant corporate bodies and the conditions to which internal controls at foreign branches should adhere.

Other provisions concerning internal control are disseminated within the above-mentioned instructions of the Banca d'Italia and are mainly related to the management process of the various risks incurred by credit institutions. In addition, inspectors of the Banca d'Italia have their own internal guidelines to assess the adequacy of internal control systems in the course of on-site inspections.

## **LUXEMBOURG**

Article 5 (2) of the Banking Law of 5 April 1993 implements Article 13 (2) of the 2BCD. The Circular of 11th January 1977, issued by the Institut Monétaire Luxembourgeois, already contained the essential features of an adequate internal control system and of a specific internal control department at credit institutions. In particular, it regulates the functioning and activity of the department in charge of internal control which must be commensurate with the size of the credit institution and the volume of its operations. The Circular 96/126 of 11 April 1996 completed the regulatory framework in this area. It supplies, inter alia, guidelines for efficient organisation concerning the responsibilities of management, staff, operational and accounting systems, documentation and, more specifically, security measures for the EDP function. Credit institutions must ensure that they exercise effective control over the EDP system and that sufficient protective measures are in place.

The Circular of 15 October 1993 defines the rules for the organisation and internal control in the specific field of the dealing activities of credit institutions. It requires the management of the credit institution to set out in writing the objectives of the bank's dealing activities, the nature of the transactions it intends to undertake, and a set of rules in respect of the organisation and internal control. This circular was supplemented by a Circular dated 21 June 1995 which points out how the general standards of risk management set up for dealing activities are to be applied in the field of derivatives activities.

A Circular from 1989, regarding the audit of the annual accounts of credit institutions by external auditors, stipulates that the general organisation and internal control procedures must be controlled annually by the external auditor who provides his assessment in an analytical report to be forwarded to the Institut Monétaire Luxembourgeois. A copy of the letter of recommendations addressed to the management, by means of which the external auditor points out significant weaknesses in the system of internal controls, must also be forwarded to the Institut Monétaire Luxembourgeois.

## **THE NETHERLANDS**

The Circular of 27 May 1993, issued by De Nederlandsche Bank, contains recommendations and guidelines for credit institutions' administrative organisation. The regulation deals with four main items:

- administrative organisation: some general principles (segregation of duties, attitude of the management, appropriate supervision, quality of the staff) are put forward with a view to ensuring a well-functioning organisation;

- administrative systems: this item relates to the framework for the day-to-day management and therefore includes the correct recording of transactions, as well as complete and timely information on the overall risk position of the institution and on-balance-sheet positions and the development of results;
- management information: this refers to the information available to the management to assess whether targets are being met and the ways in which the staff is performing its tasks;
- internal control: guidelines are being supplied on the procedures intended to ensure compliance with the law, regulations and internal rules, the safeguarding of assets, effective administrative systems, the assessment of the financial position of the institution, and compliance with reporting requirements.

The Regulation of 3 August 1995, issued by De Nederlandsche Bank, lays down guidelines and recommendations for the risk management of credit institutions' derivatives activities. It is intended to structure the administrative organisation of derivatives activities in such a way as to allow credit institutions to deal with the risks concerned in an appropriate manner. The regulation, which supplements the general guidelines mentioned above, includes basic principles for risk management, operational aspects and internal control procedures.

The Memorandum of 20 September 1988, issued by De Nederlandsche Bank, includes measures aimed at assuring adequate security of the electronic data processing (EDP) systems of credit institutions. To this end, some minimum requirements are laid down with regard to the reliability and continuity of EDP systems. A specific role is assigned to the external auditor who is to assess the measures and procedures of the EDP organisation.

Considerations of De Nederlandsche Bank dated 27 May 1994 reflect the position of De Nederlandsche Bank on the development of the outsourcing of credit institutions' EDP operations in the light of the above-mentioned memorandum. Outsourcing is regarded as a situation in which the EDP operations of a credit institution are performed outside the organisation. The basic principle is that the Supervisory Department of De Nederlandsche Bank should be allowed to consult the audit of the EDP centres and, if necessary, conduct direct examinations.

## **AUSTRIA**

The Austrian Banking Law lays down the requirements for the granting of a banking licence. In this context, the applicant must enclose, inter alia, the business plan from which the type of envisaged business, the organisational structure and the internal control procedures must be derived. Section 42 of the Banking Act contains the basic rule concerning the internal control of credit institutions and implements Article 13 (2) of the 2BCD. This provision refers to the internal audit function. Credit institutions are obliged to set up such a function, which is the responsibility of the senior management. The obligation to establish a separate audit department does not apply to institutions of a smaller size (balance sheet not exceeding ATS 1.5 billion and not more than thirty employees); the persons involved in the audit function must comply with specific requirements; in the case of groups of credit institutions, the internal audit of the group is carried out by the parent company.

External auditors are obliged - under a regulation issued on the basis of the Banking Act - to assess whether an internal control system has been set up in accordance with regulations and whether it fulfils its duties in a prudent and adequate manner. Any deficiency must be set out in the annual report



that the external auditors have to submit to the Oesterreichische Nationalbank and to the Federal Ministry of Finance (FMF). An in-depth definition of the tasks and features of the external auditors can be found in Sections 60-63 of the Banking Act. Furthermore, there are specific guidelines issued by the Institute of External Auditors and agreed with the Oesterreichische Nationalbank and the FMF. These guidelines have been updated in the context of recent amendments to the Banking Act, which take account of developments in the field of prudential supervision as well.

## **PORTUGAL**

With the instructions attached to Circular No. 261, series A, of 12 April 1994, and in the light of the provision under Article 13 (2) of the 2BCD, the Banco de Portugal defined some general minimum requirements with which internal control systems of credit institutions must comply. This regulation defines the main objectives of an internal control system (security of assets, control of all risks involved, compliance with laws and regulations, reliable accounting and financial information and reporting to supervisory authorities, and the prevention of involvement in money laundering operations) and the set of procedures intended to achieve these objectives. Specific provisions are addressed to data processing systems. The board of directors is to prepare an annual summary report on the internal control system to be submitted to the Banco de Portugal, accompanied by the advice of the board of auditors. With Circular-Letter No. 50 of 19 June 1995, the Banco de Portugal spelt out in detail the minimum content of this annual report (features of the internal control systems, data processing systems, internal audit and internal control dysfunctions).

## **FINLAND**

The Guideline of 14 January 1994, issued by the Financial Supervision Authority (FSA), regulates the duty of credit institutions' supervisory boards in the field of internal controls. In particular, it states that at least once a year the supervisory board, in order to form a view on the credit institution and its group, must consider the assessment of the bank made by the external auditors and, where that made internal audit exists, that made by the internal auditors.

Chapter 8, Section 68 of the Act on Credit Institutions contains some general provisions covering the risk management of credit institutions. In this context, credit institutions and undertakings belonging to the same consolidation group are required to have adequate risk monitoring systems with regard to their activities.

The Guideline of 15 May June 1995, issued by the FSA, is intended to promote the efficiency of the risk management of derivatives activities of credit institutions and undertakings belonging to the same consolidation group. The regulation draws on the guidelines issued by the Basle Committee in July 1994 and experience gained in the risk monitoring activity of the FSA and credit institutions. The guidelines are classified by type of risk incurred by the credit institution (credit, market, liquidity, operational, legal and strategic risks).

The definition of guidelines covering the management of credit risk by credit institutions is currently under way. The purpose of this regulation is to enhance the efficiency of the risk management of all activities entailing a credit risk of credit institutions and undertakings belonging to the same consolidation group. The regulation sets out the general principles of an efficient risk management process, risk classification and the monitoring of customers, credit analysis and credit decisions.

Chapter 3, Section 9 of the Commercial Bank Act stipulates that auditors, appointed by the board of directors, should carry out a special audit of the credit institution's management and administration at least once a year.

## **SWEDEN**

There is no law requiring credit institutions to establish adequate internal controls or an internal audit function. According to the Banking Business Act, a credit institution shall have no less than two auditors. These auditors are required to examine the annual report and the accounting records as well as the administration by the board of directors and the senior managers. Such examinations are to be performed in accordance with accepted auditing standards. There is no regulation which requires the auditor to assess the effectiveness of an internal control system as a whole.

The Guidelines of 24 November 1994, issued by the Financial Supervisory Authority (FSA), contain basic and general rules for the sound and prudent conduct of a credit institution's business activity. The main responsibility lies with the board of directors. The regulation covers four main items as follows:

- management: credit institutions are required to set up internal guidelines concerning the management of all risks (investment and operational risks) incurred in their activity;
- internal information: adequate systems should be in place to ensure relevant information on business activities on a continuous basis;
- internal control: some principles are laid down to assure an effective internal control system. These are regarded not only as being the procedures aimed at ensuring adequate control and compliance with law, regulation and internal rules, but also as including the organisation and the accounting procedures of a credit institution;
- internal audit: it is stated that the internal audit function should report directly to the board of directors or the managing director. An independent IT audit function is also recommended.

## **THE UNITED KINGDOM**

The Bank of England monitors the adequacy of institutions' systems and controls through the use of reporting accountants' reviews. These reviews are performed under Section 39 of the Act which gives the Bank of England the power to request information for the performance of its functions under the Act. To facilitate this procedure, the Bank of England has issued two notices. S&S/1996/5, the Bank of England's relationship with Auditors and Reporting Accountants, and S&S/1996/6, Guidance Note on Reporting Accountants' Reports on Accounting and Other Records and Internal Control Systems.

S&S/1996/5 details the means of communication between the reporting accountants and the Bank of England. This includes reports (including those on accounting and other records and internal controls), trilateral discussions (to discuss the reports among other matters), and any exercise of the right or duty to report issues of concern to the Bank of England. It also details the normal timetable for reviews of accounting and other records and internal controls.<sup>5</sup>

---

<sup>5</sup> As to the impact of the Barings case on the UK regulation, the Report of the Board of Banking Supervision Inquiry recommends that the Bank of England should commission reporting accountants' reports more flexibly than in the past

S&S/1996/6 provides guidance on the Bank of England's interpretation of the Act's requirements in relation to records and systems, to assist the authorised institution in assessing whether these records and systems meet the requirements and to assist reporting accountants in reporting on the records and systems. The guidance is broad and basic so that it will encompass a variety of institutions, both large and small, incorporated in the United Kingdom or overseas. The notice concentrates on the scope and nature of the records and systems rather than on prescribing their detail.

In respect of accounting records, general requirements are set out in respect of timely recording, sufficiently detailed recording, the authorisation of limits, and the recording of credit decisions. The notice also sets out the basic requirements of management information and indicates who should be aware of such information. In respect of internal controls, the notice sets out the general requirements for planning and conducting the business in a prudent manner. It then considers the minimum control objectives that an institution should address in greater detail. In addition to this, the guidance note looks specifically at controls in an information technology environment and the desirable characteristics of internal audit. Beyond the level of internal controls, the notice also addresses the desirability of having an Audit Committee. Finally, the notice sets out the format which reporting accountants' reports should follow.

---

and should cover, where appropriate, activities carried out by the institution in different jurisdictions. The Guidance Note S&S/1996/6 incorporates these recommendations.

EUROPEAN MONETARY INSTITUTE  
Banking Supervisory Sub-Committee

Participants in the Sub-Group on Credit Institutions' Internal Controls

Chairman	Mr. F. Vargas
	Banco de España
Banque Nationale de Belgique	Mr. P. Lefèvre
Commission Bancaire et Financière, Brussels	Mr. F. Beukelaers
Danmarks Nationalbank	Mr. J. Ladekarl
Finanstilsynet, Denmark	Ms. K. Kjargaard
Deutsche Bundesbank	Mr. K.-H. Hillen
Bundesaufsichtsamt für das Kreditwesen	Mr. W. Wendt
Commission Bancaire, Paris	Mr. F. Visnovsky
Bank of Greece	Mr. H. Voyatzis
Banco de España	Mr. L. Rodríguez
Central Bank of Ireland	Mr. J. Fitzgerald
Banca d'Italia	Mr. S. Caringi
Institut Monétaire Luxembourgeois	Ms D. Mander
De Nederlandsche Bank	Mr. H. de Poot
Oesterreichische Nationalbank	Mr. E. Schmidbauer
Federal Ministry of Finance, Austria	Mr. W. Fend
Banco de Portugal	Mrs. C. Ferrinho
Financial Supervisory Authority, Finland	Mr. J. Haajanen
Financial Supervision Authority, Sweden	Mr. J. Hedqvist
Bank of England	Mr. D. Swanney
European Monetary Institute	Mr. M. Grande

EUROPEAN MONETARY INSTITUTE

Participants in the Banking Supervisory Sub-Committee

Chairman	Mr. T. de Swaan
	De Nederlandsche Bank
Banque Nationale de Belgique	Mr. J.- J. Rey
Commission Bancaire et Financière, Brussels	Mr. J.- L. Duplat
Danmarks Nationalbank	Mr. J. Ovi
Finanstilsynet	Mr. H. Bjerre-Nielsen
Deutsche Bundesbank	Mr. E. Meister
Bundesaufsichtsamt für das Kreditwesen	Mr. J. Sanio
Bank of Greece	Mr. I. P. Vahaviolos
Banco de España	Mr. R. Poveda
Commission Bancaire, Paris	Mr. P. Duquesne
Central Bank of Ireland	Mr. G. Murphy
Banca d'Italia	Mr. B. Bianchi
Institut Monétaire Luxembourgeois	Mr. J.-N. Schaus
De Nederlandsche Bank	Mr. J. Brockmeijer
Oesterreichische Nationalbank	Mr. D. Spranz
Federal Ministry of Finance	Mr. A. Stanzel
Banco de Portugal	Mr. A. Marta
Suomen Pankki	Mr. E. Ollila
	Mr. H. Koskenkylä
Financial Supervisory Authority, Finland	Mr. K. Jännäri
Sveriges Riksbank	Mr. S. Ingves
Financial Supervisory Authority, Sweden	Mr. C. Norgren
Bank of England	Mr. M. Foot
	Mr. D. Green
European Monetary Institute	Mr. M. Grande
	Mr. J. Priesemann