

## **KREDITILSYNET**

### **The Financial Supervisory Authority of Norway**

Translation as of October 2004

Translated by Government Authorised Translator Peter Thomas.

*This translation is for information purposes only. Legal authenticity remains with the official Norwegian version as published in Norsk Lovtidend.*

---

## **GUIDE TO REGULATIONS NO. 1057 OF 20 JUNE 1997 ON RESPONSIBILITY FOR INTERNAL CONTROL AND ON DOCUMENTATION AND CONFIRMATION OF INTERNAL CONTROL (INTERNAL CONTROL REGULATIONS)**

### **1 About internal control**

An institution's internal control is the action it takes, through its organisation and routines, to secure its own and its customers' assets and, through sound operations, to achieve established targets. This entails more than what is often perceived as internal control. Achieving targets also presupposes a systematic strategy and planning efforts, identification of risk factors, choice of risk profile, along with the establishment and implementation of control measures to ensure that the targets are reached.

Internal control is therefore a continual process – initiated, implemented and monitored by the institution's board of directors, management and other staff. Internal control is designed to give reasonable assurance of goal achievement in the following areas:

- Targeted, efficient and appropriate operations
- Reliable internal and external reporting
- Compliance with laws and rules along with internal guidelines

Satisfactory internal control is of great significance for the business of all institutions, regardless of scale and size. The design and dimensions of internal control will, however, differ depending on business areas, risk profile and scale of activity.

According to the COSO Report (1996) central elements of sound internal control are:

- A good internal control environment with commitment at all levels of the institution
- Continuous attention to risk with regular risk analyses and reporting
- Establishment and implementation of relevant internal control measures
- Good communication and information
- Active monitoring on the part of the board of directors and management

An important prerequisite for achieving sound internal control is the formulation of clear-cut and consistent goals at the various levels of the organisation, along with a clear definition of the institution's risk profile.

In the event of major internal changes in institutions, in business and in markets, it is important that the board of directors and management give increased emphasis to internal control.

Internal audit activity forms part of an institution's internal control system. Kredittilsynet would emphasise that the obligation to establish an internal audit function does not imply that this function should take over any of the line management's internal control responsibilities. See the section on internal audit activity later in this guide.

## **2. About the internal control regulations**

The main purpose of the regulations is to make clear the board of directors' and management's responsibility for internal control.

The regulations set minimum requirements for the institution's processes and documentation in regard to internal control, including risk assessments, internal control measures and monitoring. It does not comprise the institution's choice of specific business goals, strategies or risk profile. However, it is clear from the general requirements as to sound institutional management that a process attending to these important elements of institutional management also needs to be established.

It is emphasised that to the extent that the institution has outsourced parts of its business, these will also be encompassed by the internal control regulations. The institution is responsible for the outsourced activity and should therefore, through the necessary agreements, impose requirements on the entity that has taken over the outsourced activity to ensure that also this entity has established satisfactory internal control.

The Basel Committee on Banking Supervision has established 13 fundamental principles for internal control. While the principles are formulated with banks in mind, they are also relevant to the other institutions coming under the internal control regulations. Kredittilsynet considers the intentions behind these principles to be well in line with the requirements of the regulations (see the Basel Committee's website at [www.bis.org](http://www.bis.org)).

## **3. The board of directors' responsibility for internal control (section 2-1)**

The board of directors' responsibility for the institution's internal control follows inter alia from the principles of the Private Limited Companies Act and the Public Limited Companies Act (sections 6-12 and 6-13).

The board of the directors shall see to it that internal control in the institution is secured on a sufficient scale and in a systematic manner. The board has a free hand in finding a practical and overviewable means of achieving this although, based on chosen objectives and strategies, it will need:

- to establish principles for internal control in the various areas of the institution's business. Together with the regulations themselves, such principles can act as an

overarching guide for risk management in the enterprise. The board should therefore seek to give the principles a form and a content which concisely shows how the institution should give weight to factors of significance for assuring satisfactory operations, including distribution of roles between the board of directors and the administration and other controlling functions, organisational conditions, systems-related factors, and how principles for delegating authority should be established.

- to see to it that the institution establishes an internal control process which meets the requirements of the internal control regulations.

- to see to it that internal control is implemented and monitored. It is of central importance in this connection to review and decide the institution's approach to risk assessment and associated control measures (section 3-2), reporting to top management (section 4-1) and reporting by the internal auditor, in the event the external confirmation required in institutions which have not established an internal audit function (section 4-2). It is important in this connection to see to it that mechanisms are established/implemented to counteract observed flaws, and that internal control is taken into account when decisions are made regarding significant changes in the business.

- to see to it that the institution's internal control and the associated process is documented for the various areas of business in compliance with the internal control regulations.

The board of directors is also required to consider establishing an internal audit function in the institution. This function is likely to be an important aspect of the board's monitoring of internal control. It is especially relevant in large, complex organisations and in institutions with high operational risk. It entails a strengthening of internal control, and will also be relevant in institutions not encompassed by the internal audit requirement set out in section 4-2 of the regulations. Where an institution has not found it necessary to establish an internal control function, Kredittilsynet is entitled in the course of supervision to ask the board to justify its decision not to do so.

Where conglomerates are concerned, the board of directors of each subsidiary is responsible for ensuring that particular subsidiary's compliance with the requirements of the regulations. However, the group board of directors will naturally wish to keep itself informed of the management and control machinery that is established in subsidiaries and of the associated processes. This will enable it to judge whether internal control being is maintained on a group-wide basis in keeping with the aim of the regulations.

#### **4. The chief executive officer's responsibility for internal control**

The chief executive officer is responsible for ensuring that the institution's internal control complies with the principles set out in the Private Limited Companies Act and the Public Limited Companies Act (sections 6-14 and 6-15).

The chief executive officer shall, with a basis in the institution's objectives and actual risks faced at various levels of the organisation, ensure that a satisfactory internal control regime is established in keeping with the principles and guidelines established by the board directors and in accordance with the requirements of the regulations. The CEO shall ensure that internal control is implemented, monitored and documented in an effective manner.

The CEO is key to establishing a sound internal control environment at all levels of the institution. It is essential to lay a basis for good communication within the organisation, as well as an open interaction on these factors with the board and relevant control bodies such as the internal and external auditor and, in the event, the control committee and audit committee.

It is important that the CEO involves himself in the various stages of the internal control process that are envisaged by the regulations. At smaller institutions it will be natural for the CEO to participate in this effort himself, whereas in larger institutions the CEO will above all initiate the process, participate in the overarching risk assessment and proactively assess whether the established management and control machinery is satisfactory. It will be crucial to oversee that the line managers play an active part in their respective areas.

The CEO will need to ensure that the board of directors receives sufficient information on the main features of the institution's internal control system.

## **5. Overview of internal control (section 3-1)**

The documentation requirement encompasses the control measures implemented to prevent risks leading to losses and deficiencies. Such measures may include division of work, establishing limits, guidelines, systems/processes with built-in manual and electronic control mechanisms, reporting etc.

Documentation of control measures is designed:

- to provide managers at all levels with an overview of how satisfactory operations should be assured
- to specify control measures which managers in the various areas are required to implement and monitor over the year
- to provide a basis for external supervision

The regulations require a systematic overview of the institution's control measures in respect of significant risks. However, the institution is free to choose its system, mode of presentation and retention medium in relation to the scale and complexity of its business so long as the aims are met. In institutions with overviewable and uniform operations, documentation may appear to be a simple, systematic enumeration of a central control measures, whilst in institutions whose product areas feature a varying risk profile documentation will need to be segmented to enable the respective areas to be individually

assessed. It is important to systematise the documentation such that it provides an overall picture of the control measures employed.

The overview must at the same time be sufficiently updated and detailed to serve as a practical point of departure for the board's and the supervisory authorities' assessment of whether the measures employed assure satisfactory operations.

In conglomerates an overall picture of the internal control measures will be desirable in many cases. This said, the presentation will nonetheless need to meet the requirements in relation to the individual subsidiaries encompassed by the regulations.

## **6. Review of risk and protective measures (section 3-2)**

This requirement is designed to support the implementation of a satisfactory process as regards risk assessment, establishment of control measures and infusing an awareness of residual risk in the institution. The institution is free to choose its preferred method of working.

The review will be a point of departure for assessing the need for changes in the institution's control measures. Assessing the consequences of changes in organisation is particularly important.

According to the regulations, risks and associated control measures shall be assessed at least once a year. This does not have to be done at specific times. Individual areas can be analysed at different times of the year. However, all significant risk areas must be assessed in the course of a single year regardless of whether or not changes have taken place. Results from different aspects of the internal control reporting can also be presented to the board at different times, although in this case it would be natural to set aside time for a comprehensive annual assessment in connection with the summary required by the regulations.

All managers should be actively involved in the process of risk assessment and choice of control measures. It is not enough just to build, for example, on the conclusions reached by controller departments or the internal audit. Reports based on visits by the internal audit, if any, and statements from the external auditor may well be very useful, but caution must be shown in involving these entities to an excessive degree since the objectivity of the audit function may be impaired.

Here too, the institution is free to choose its method of documentation, bearing in mind that the intention of documentation is to reflect work procedures and significant assessments so as to make it possible to confirm that the institution has assessed risks and necessary control measures in all areas of its business and operations. Similarly it would be natural for the documentation to show the extent to which managers at various levels have participated in the process.

## **7. Confirmation from management (section 4-1)**

The aim of this requirement is to ensure that sufficient information on the ongoing implementation of internal control, including observed failures, reaches the management and board. Achieving this will normally require the establishment of a systematic programme for monitoring and reporting which includes managers at all levels of the organisation. Significant flaws and errors that are immediately rectified should also be reported. This will provide a basis on which to assess relevant countermeasures, at the same time as affording a picture of how well the internal control process functions.

The documentation requirement is designed to ensure that the institution will subsequently be in a position to demonstrate that the process has been implemented and that the information has been communicated.

The reporting regime requires managers at all levels of the organisation to monitor control measures adopted within their particular areas of responsibility. This is with a view to being able to intervene when controls fail or prove inadequate. The regulations impose no particular requirements as to how monitoring should be carried out, although insight is usually obtained by means of personal presence, making enquiries at meetings with colleagues, making spot checks and other special enquiries, scrutinising key figures and ratios and measuring deviations in IT systems, reviewing reports after a visit by the internal auditor and the like. The existence of a systematic monitoring arrangement, and regular reassessment of this arrangement, is regarded as a highly important aspect of internal control. The institution's management must be prepared for the board of directors, control committee, internal audit and the supervisory authorities to request information on monitoring arrangements.

The regulations impose no specific requirements on the monitoring arrangements or on the method, frequency and scope of transmission of reports to the top management. It is left to the institution itself to decide what measures are best suited to ensuring that the management and board are sufficiently informed to be able to discharge their responsibility for satisfactory, goal-oriented operations. As a rule this will entail concentration on increasingly significant factors the higher the level at which the information is to be presented in the organisation. However, it must be kept in mind that even details may be crucial if they arise in large numbers, are spread across the institution or give an indication of shortcomings of a general nature. As in the case of many other provisions in the regulations where institutions are free to choose their preferred system, this section also entails an obligation to make choices that ensure that the intention of the regulations is fulfilled. In the final analysis this is the board's responsibility.

## **8. Internal audit (section 4-2)**

### First paragraph – internal audit

Internal audit activity is a monitoring function which, independently of the administration in general, carries out systematic risk assessments, checks and investigations of the

institution's internal control regime to assess whether it is functioning in an appropriate and satisfactory manner.

Internal auditing is an independent specialist area, with its own standards, methods and ethical rules. The Institute of Internal Auditors Norway prepares recognised standards within this field. Recommendations and standards published by other associations and organisations in this field will also be regarded as recognised standards to the extent that they contribute to fulfilling the objectives of the regulations.

The institution's board of directors shall approve the internal audit unit's resources and annual plans. The resources, both in terms of competence and capacity, are expected to be tailored to the business and scale of the institution. Other aspects of the basis for approval are the goodness-of-fit of the institution's own internal control programme, the need for high-quality risk assessment on the part of the internal audit unit, annual plans and reports, as well as information obtained by the board of directors in its contact with the head of the internal audit unit.

The internal audit function may be outsourced entirely or in part to an external provider of such services. The premise is that the relationship between the institution's board of directors and the internal audit unit is regulated by a separate agreement. The institution's external auditor may not, however, accept this task since it would be counter to section 4-5 second paragraph of the Auditors Act.

The regulations require institutions with total assets for their own and their customers' account in excess of NOK 10 billion to establish an internal control function. It may be decided that this requirement shall come into play at the latest once total assets have exceeded the above threshold for more than twelve months and the institution is unable to provide evidence that total assets will fall below this threshold in the course of the next six months.

All Norwegian institutions as defined in section 1-1, regardless of size, that are part of a financial group whose total assets for their own and their customers' account exceed NOK 10 billion are required to have an internal audit function. In financial groups which have found it appropriate to establish an internal audit unit at group level, this unit will as a rule also be responsible for internal auditing as a coordinated group function. However, the regulations require each individual subsidiary's board of directors to approve the internal audit unit's resources and plans for the company in question on an annual basis, and requires that they receive at least once a year a separate report, or a coordinated report for the entire group, from the internal audit unit giving an account of conditions in the company in question. Similarly, it will be natural for the group board of directors to ensure that it receives at least once a year and overall picture of the audit unit's view of the group's internal control situation.

## Second paragraph – independent confirmation

This provision only applies to institutions that have not established an internal audit unit. It is designed to ensure that the board of directors of institutions that have not established internal audit functions also, as a minimum, make sure that they obtain independent confirmation of the institution's internal control regime once a year. The independent confirmation shall be issued by a body outside the operative organisation. The board of directors or, where appropriate, the group board of directors, must assure itself that this body has the competence and other qualifications required to issue such confirmation. In Kredittilsynet's view it may be appropriate for the institution's external auditor to issue the confirmation, although other entities within or outside the institution which are not part of the operators organisation may also issue such confirmation.

The confirmation must be in a position to specify the investigations on which it is based. Moreover, it must be clearly stated whether the entity in question considers that the processes associated with risk assessment, control choice, implementation and reporting have been carried out in a proper manner in keeping with the requirements of the regulations. Where the investigation has brought to light shortcomings or significant failures, this must also be stated.

### **9. Retention and reporting to Kredittilsynet (section 5-1)**

Apart from the minimum requirement regarding the period of retention, the regulations impose no particular requirements on the retention of documentation. The institution should nonetheless take into account any need to demonstrate that internal control has been properly attended to over a longer period, and choose a period of retention for the various types of documentation on this basis. There are no constraints as regards the medium of retention, since it is not the form but the information itself that is significant. It would be natural to consider both safety and ease of access in this context.

#### Reference:

Solberg, Marte. 1996 [red.]. *Intern kontroll – et integrert rammeverk. Oversettelse av COSO-rapporten*. Oslo: Cappelen Akademisk Forlag. [*Internal control – integrated framework*. Norwegian translation of the COSO-report]