



Internal Control over Financial Reporting in Listed Companies



Internal Control over Financial Reporting in Listed Companies

The opinion in this document are the responsibility of the working group and therefore, do not necessarily coincide with those of the Comisión Nacional del Mercado de Valores

Comisión Nacional del Mercado de Valores distributes its reports and publications via the internet at www.cnmv.es

© CNMV. The contents of this publications may be reproduced with attribution.

Design and Printing: Artegraf, S.A.

ISBN: 978-84-87870-96-5

Depósito Legal: M-29273-2010

Contents

Section I. Internal control over financial reporting	9
Introduction	9
Purpose and scope	10
Legal framework	11
EU directives	11
Current regulations in Spain	11
The annual corporate governance report	12
Audit committee	12
Auditors	13
New regulatory features in Spain	14
Regulatory framework in other countries	14
Working group proposals	15
Regulatory developments	15
Framework	16
Guidance	16
The role of external auditors	16
Entities seeking listing	18
Section II. Framework	19
General issues	19
Content and scope	19
Responsability	19
Voluntary nature	20
Binding definitions	20
Financial information	21
Reliability of financial reporting	21
ICFR as an integrated process	22

Principles and good practice	22
The entity's control environment	22
Risk assessment in financial reporting	24
Control activities	25
Information and communication	26
Monitoring	27
Section III. Guidance for disclosures on internal control over financial reporting	29
General principles	29
Purpose and content of guidance	29
Alternative ICFR disclosure	29
Binding definitions	30
Characteristics of the information to be disclosed	30
Basic indicators	31
The entity's control environment	31
Risk assessment in financial reporting	32
Control activities	33
Information and communication	34
Monitoring	35
Section IV. Audit committee monitoring of internal controls over financial reporting	37
The monitoring process	37
Concept and objectives of monitoring	37
Support functions for monitoring	37
A monitoring checklist	38
Audit committee competencies	38
The evaluation process	39
Documenting ICFR and the evaluation process	39
Evaluating the design of ICFR	39
Evaluating the effective functioning of ICFR	41
Evaluation control weaknesses	43
Monitoring and evaluation schedule	43

1	Glossary of terms and acronyms	47
2	Procedures for external auditor review	53
3	Members of the working group and CNMV support	55

Section I. Internal control over financial reporting

Introduction

Disclosure requirements constitute an area of securities market practice that has come on rapidly in recent years. In particular, the rules governing financial reporting by listed companies have been successively refined, while their technical complexity has grown exponentially. For companies to keep up, it is essential that their internal control systems evolve in tandem, so markets can have reasonable confidence in the reliability of the financial information they are being supplied with.

Spain's regulatory framework for internal control has seen few changes in recent years beyond those outlined below:

- Listed companies are obliged to give a general account in their Annual Corporate Governance Report (ACGR) of their risk identification and management policy and to state their degree of compliance with the recommendations of the Unified Code for the Good Corporate Governance of Listed Companies published by the Comisión Nacional del Mercado de Valores (CNMV) (Spanish National Securities Market Commission) in May 2006 (Unified Code).
- Audit committees must be apprised of financial reporting processes and the internal control systems in place, as well as overseeing the internal audit function.
- External auditors must review internal control systems to determine the scope, nature and timing of the audit tests that will enable them to issue an opinion on the company's financial statements. On concluding their review, they should report any material weaknesses in internal control to senior management and the audit committee.

Internal control regulations in Spain stand in contrast to the more stringent requirements of other markets, which impose varied obligations regarding the maintenance and monitoring of internal control systems, disclosure to the market of their characteristics and operation, and, in some cases, external reviews and certifications. These obligations vary in their scope, obligated parties and the incremental cost entailed.

In Europe, control matters are addressed in a number of legislative initiatives. In particular:

- In May 2006, the European Parliament and the Council approved Directive 2006/43 on statutory audits of annual accounts and consolidated accounts. This Directive establishes that the audit committees of listed companies should monitor the financial reporting process, and the effectiveness of internal control, internal audit and risk management systems.
- In June 2006, the European Parliament and the Council approved Directive 2006/46, which requires financial institutions to provide the market with a description of the main features of any existing risk management systems and internal controls in relation to the financial reporting process.

It is accordingly worth examining Spanish regulations on internal control over financial reporting, in order to identify opportunities for improvement, and to draw up recommendations and good practices that listed companies can use as a benchmark to develop or strengthen their internal control systems and enhance the reliability of their financial statements.

Purpose and scope

The Internal Control Working Group (ICWG) was set up at the instance of the CNMV in order to draft a set of recommendations on internal control over financial reporting (ICFR). The work of the ICWG has focused on three basic goals:

- (a) Review the Spanish regulatory framework with regard to internal control over financial reporting, comparing it with that of other countries (United States, United Kingdom, France and Germany) with a view to putting forward improvement measures.
- (b) Establish a framework of ICFR principles and good practice, including the monitoring of system operation.
- (c) Contribute to enhancing the transparency of the information companies provide to the market regarding their ICFR.

In pursuing these objectives, the ICWG started from the following premises: (i) to bear in mind the requirements imposed by European Union legislation; (ii) to align the internal control disclosure requirements of Spanish markets with those of neighbouring markets; and (iii) to provide more incentives for companies to strengthen their internal control mechanisms, ensuring that compliance with recommendations does not exact too great an extra cost or act as a barrier to the admission to trading of new companies.

The work of the ICWG has given rise to the following documents:

- (a) A proposed regulatory development in respect of ICFR.
- (b) A framework consisting of a set of general principles and good practices for internal control over financial reporting, to aid listed companies in the design, implementation, operation and monitoring of an ICFR system which makes for more reliable financial information.

- (c) A guidance document for companies to describe their ICFR.
- (d) A checklist for audit committee monitoring of ICFR.
- (e) A glossary of terms.
- (f) A procedural model for external auditor review.

The document prepared by the ICWG is intended for all kinds of listed companies, whatever their size, market capitalisation and business sector or the nature of the securities they issue.

Legal framework

EU directives

Directive 2006/43 sets out to harmonise the requirements for statutory audits across the European Union. Its main implications for the ICWG's remit are as stated below:

- The adoption of International Auditing Standards (IASs), which makes little difference regarding the scope and purpose of the statutory audit of internal control systems with respect to the Technical Auditing Standards (TASs) in force in Spain. However, the definition of an internal control system as set out in the IASs coincides with that put forward by the Committee of Sponsoring Organisations of the Treadway Commission (COSO), and its five key components.
- The new functions assigned to the audit committees of listed companies, including the monitoring of the financial reporting process and the effectiveness of internal control, the internal audit function, as and when applicable, and risk management systems.

Directive 2006/46 on annual accounts obliges companies to disclose an annual corporate governance statement as a separate part of their annual reports, and to include a description of the main features of any existing risk management systems and internal controls in relation to the financial reporting process. Article 46a of the text specifies that this description should be subject to review by the external auditor, to check that it matches the annual accounts.

Current regulations in Spain

The general framework governing internal control systems, which mixes legal requirements with voluntary Unified Code recommendations, establishes that audit committees should be cognisant with the company's financial reporting process and internal control systems. However transparency requirements place no particular emphasis on internal control systems, and nor do they envisage third-party verification of disclosures to the market on ICFR. Finally, Spanish regulations do not specify an internal control framework or guidelines on the content, terms and definitions of the information to be disclosed.

The annual corporate governance report

Article 116 of the Spanish Securities Market Law requires listed companies to publish an annual corporate governance report (ACGR) providing a detailed explanation of the structure and operation of their governing bodies, and describing their risk management systems and degree of compliance with corporate governance recommendations, subject to the comply or explain rules.

Regarding risk management systems, the current ACGR form requires companies to specify as follows:

- Describe the company's risk policy, detailing and assessing the risks covered by the risk management system and explaining why it is adequate for dealing with each type of exposure.
- Report whether any kind of risk affecting the company (operational, technological, financial, legal, etc.) has materialised in the year, indicating the circumstances triggering the event and the effectiveness of the systems in place for its mitigation.
- State whether the company has a committee or equivalent body charged with establishing and monitoring control mechanisms and, if so, provide a list of its functions.
- Identify and describe compliance processes in respect of the regulations the company is required to follow.

The ACGR is an integral part of the annual report (management report) and failure to produce it, or the existence of omissions or false or misleading data are serious breaches of market regulations. However, neither Article 116 of the Securities Market Law nor the current ACGR form are explicit on the details to be given on ICFR pursuant to Directive 2006/46.

Audit committee

The Additional Provision Eighteen of the Securities Market Law requires listed companies to establish an audit committee with a majority of non-executive members, whose remit will be to monitor the internal audit function, as appropriate, and be cognisant with the company's financial reporting process and internal control systems. Directive 2006/43 goes further in this respect and requires the committee to actually monitor these functions as well as being aware of how they work.

The Unified Code urges the audit committee to exercise the following responsibilities with regard to internal control and reporting systems:

- Monitor the preparation and the integrity of the financial information prepared on the company and, where appropriate, the group, checking for compliance with legal provisions, the accurate demarcation of the scope of consolidation and the correct application of accounting principles.

- Review internal control and risk management systems on a regular basis, so the main risks are properly identified, managed and disclosed.
- Monitor the independence and efficacy of the internal audit function; propose the selection, appointment, reappointment and removal of the head of internal audit; propose the department's budget; receive regular report-backs on its activities; and verify that senior management are acting on the findings and recommendations of its reports.
- Establish and supervise a mechanism whereby staff can report, confidentially and, if necessary, anonymously, any irregularities they detect in the course of their duties, in particular financial or accounting irregularities, with potentially serious implications for the firm.

The Unified Code also recommends that listed companies should have an internal audit function, under the supervision of the audit committee, to ensure the proper operation of internal reporting and control systems.

Auditors

The Technical Auditing Standards (TASs) issued by the Spanish Accounting and Audit Institute (ICAC) distinguish between “reviews whose purpose is to evaluate and improve an entity's internal control system, carried out by an auditor in its expert capacity in response to a specific mandate” and “the review and evaluation of internal control systems carried out during an audit of accounts”.

In the case of an audit of accounts, the external auditor should review and assess the internal control system to determine the scope, nature and timing of tests. The auditor may take the professional decision to limit the scope of this internal control review, but is duty bound to notify the company's senior management, audit committee or board of directors of any material system weaknesses uncovered during the audit process.

The TASs confine the auditor's review of the management report, of which the ACGR forms part, to the following actions:

- Check that the accounting information in the management report matches the data used to draw up the audited annual accounts. There is no obligation to use audit procedures to verify information other than that drawn from the audited accounting records.
- Read through the entire management report to identify any serious contradictions between the information gleaned during the audit or any significant errors in the economic and financial information presented.
- The auditor's report should contain a paragraph stating that the management report does not form an integral part of the annual financial statements but that the accounting information contained in its pages is consistent with the same. If there are significant discrepancies and the auditor concludes that the

management report is incorrect, it should detail the discrepancies or errors found.

New regulatory features in Spain

Two legislative initiatives still in the pipeline at the time of publishing this paper will affect the obligations and/or recommendations envisaged in the current regulatory framework with regard to the contents of ACGRs, the terms of reference of audit committees and the conditions governing the work of external auditors:

- In October 2009, the Government sent a draft Audit Law to the Lower House of Parliament. Its approval would entail the writing into Spanish law of new competencies for listed companies' audit committees via an amendment to the Additional Provision Eighteen of the Securities Market Law.

Among these new competencies are monitoring the effectiveness of internal control and risk management systems along with the preparation and presentation of financial statements.

- In November 2009, the Government approved a preliminary draft of its Sustainable Economy Law, which introduces a number of new provisions to the Securities Market Law; including the provision that ACGRs should henceforth include "A description of the main features of internal control and risk management systems with regard to statutory financial reporting".

Regulatory framework in other countries

The regulatory frameworks of our principal neighbouring markets establish obligations and recommendations for the internal control systems of listed companies that tend to be more developed than Spanish rules. Requisites vary significantly from one country to another and place differing demands on companies in terms of organisational structures, cost implications and the degree of built in reliability.

Some regulators have opted for highly structured requirements with increased accountability for directors and senior officers, of a breadth and depth involving considerable investment by the obligated parties. A prime example here would be the U.S. system enshrined in the 2002 Sarbanes-Oxley Act (SOX), which was later imitated by Japan (J-SOX) and Canada (C-SOX). Other countries like the United Kingdom, France or Germany have preferred to impose less strict and costly systems.

The following table describes the main features of these regulatory frameworks with regard to a series of core attributes:

Attributes	United States	United Kingdom	France	Germany
Nature of the obligation	Annual review of ICFR. The degree of disclosure to the market is less in quantitative terms, but qualitatively more demanding in that it extends to system effectiveness and weaknesses detected.	Companies must maintain, monitor and describe their internal control system, with annual review recommended. They must disclose whether they conduct this review, and whether incidents detected (which need not be specified) have been or will be dealt with.	Companies must disclose the characteristics of their internal control, but are not expressly obliged to report the findings of system reviews. However, if the company's report fails to specify material weaknesses encountered during financial auditing, the external auditor must refer to them in its report.	Companies must report on their ICFR, with audit committees charged with monitoring the system, and implementing and maintaining an early risk identification system.
Model characteristics	Geared to ICFR.	Refers to risk management, with an emphasis on ICFR.	Refers to risk management, with an emphasis on ICFR.	Covers all aspects of internal control, but tending to prioritise business continuity risks over ICFR.
External verification	ICFR to be evaluated by the external auditor, which issues an opinion on its effectiveness based on a specific auditing standard.	External auditors must have procedures in place to review all information supplied to the market, and publish a report identifying any exceptions encountered during their application. A specific auditing standard exists to this effect.	Similar to the United Kingdom. In addition, the external auditor must determine whether material weaknesses found during financial auditing have been adequately described in the report. Otherwise, it must disclose them in its own report.	External auditors must issue a reasoned opinion on the early risk identification system deployed by management, based on a specific auditing standard, but without public disclosure. There is no requirement to review ICFR information and monitoring.
Reference framework	COSO is suggested but no particular framework is imposed.	A specific national framework has been developed, but is not obligatory.	A specific national framework has been developed, but is not obligatory.	No reference to any internal control framework, though early risk identification systems are usually explicit about measures to be taken.
Guidance for companies to facilitate compliance with ICFR disclosure and monitoring obligations	Guidance available.	Guidance available	Guidance available	No guidance available.

Working group proposals

Regulatory developments

The ICWG believes that for the above legislative initiatives to be effectively and consistently enforced with reasonable cost/efficiency, ICFR must be more closely regulated with models provided for its adequate monitoring, and has borne this in mind when drawing up the following framework of principles and good practice.

For reasons of transparency, the ICWG is calling for tighter disclosure requirements for ICFR, such that:

- Basic disclosures are included in the ACGR, to which end the ICWG has prepared a guidance document based on the framework, as set out in Section III.
- Consideration goes to the alternative ICFR disclosure regime envisaged in Section I – *Guidance* below.
- The definitions in Appendix 1 become binding in nature, provided the reference framework is that proposed.
- Disclosures refer to internal controls in operation during the year covered by the ACGR.

Framework

The ICWG has established a voluntary framework for internal control over financial reporting, as set out in Section II, in order to give companies a set of benchmark recommendations for comparing and assessing their ICFR, and to harmonise reporting standards in their respect.

This framework, based on the COSO Report, includes a catalogue of good practices and principles for ICFR components, including the oversight role to be exercised by the audit committee.

Guidance

A guidance document has been prepared to assist companies with their ICFR disclosures and facilitate their interpretation. Its contents are set out in Section III, specifying the reference indicators for use in each case.

The ICWG assumes that companies fulfilling the requisites specified in a) and b) of Section III – *Alternative ICFR disclosure*, comply in full with ICFR disclosure requirements, particularly principle 30 of Section II – *Framework – Principles and good practice*, concerning the work of the external auditor.

The Group has also produced a checklist for audit committees in fulfilling their ICFR monitoring role, as set out in Section IV.

The role of external auditors

The ICWG has looked closely at the possibility of bringing external auditors in on the process by requiring them to issue a report, which would serve to enhance the transparency and quality of ICFR disclosures. On the plus side, the ICWG considered that an ICFR evaluation report from the external auditor could help secure the following objectives:

- (a) Strengthen trust in public disclosures to the market concerning ICFR.
- (b) Aid compliance with the rules and principles specified in framework recommendations.

- (c) Facilitate comparability of the information published by listed companies.
- (d) Favour convergence with neighbouring countries, which tend to specify external auditor involvement in the review of ICFR information.

However, this study also revealed a series of drawbacks, which the Group felt should be borne in mind. In particular:

- (a) A degree of contradiction between the fact that one ACGR chapter is subject to outside review while the rest is not. In any event, it should be mentioned that from the moment the ACGR is formally inserted into the annual report it also comes under the scrutiny of the external auditor, who checks that the accounting information it contains matches that presented in the annual financial statements.
- (b) Possible duplication of functions, since TASs require external auditors to examine companies' internal control systems in sufficient depth to determine which audit tests are needed, and they are also obliged to report any ICFR weaknesses detected to the appropriate governing bodies.
- (c) Existence of an incremental cost deriving from the need to increment the services provided by the external auditors and, as a result, their fees.

After weighing up the pros and cons in what was necessarily a prolonged debate, the members of the ICWG arrived at a common position as formulated in the following terms:

- (a) An ICFR report is felt to be warranted and companies are urged to commission one from their external auditor for subsequent public disclosure.
- (b) Given the nature of the information to be reviewed, the report sought should be of limited scope. In particular, reviews need not extend to assessing the design and effectiveness of ICFR, so auditors can confine themselves to the following tasks, as per the models prevailing elsewhere in Europe:
 - Attain a sufficient understanding of the ICFR established by the company.
 - Review ICFR explanatory and supporting documentation to ascertain whether claims made in the ACGR in its respect are founded in reality.
 - Confirm that the information given on ICFR is consistent with the auditor's findings during its account auditing work and in the course of this limited review.
 - For the sake of uniformity, it might be useful to develop a guidance document setting out the precise scope of the review and the format to be used for the external auditor's report as detailed in Appendix 2.
- (c) It is presumed that some companies, in view of their particular circumstances (degree of development and organisation of internal audit services, complexity

of operations, comparative cost/benefit analysis as a function of business size, etc.), may have reasonable grounds for deciding not to follow this recommendation, in which case they are invited to explain the reasons for their decision.

- (d) External auditors, it is considered, should keep the cost of this review within reason, given its limited scope and the synergies available with the rest of their audit work.
- (e) Companies asking external auditors to review their ICFR – whether voluntarily (pursuant to the recommendation in this framework) or when required (under the laws of foreign markets where their shares are traded, for instance the SOX Act in the United States) – should publicly disclose the auditors’ report, along the lines specified in Section III – *Alternative ICFR disclosure*.

Entities seeking listing

Entities should supply information on their ICFR systems when they apply for stock market admission, complying with the same requirements as companies already listed.

Section II. Framework

General issues

Content and scope

This framework sets out a body of general principles and good practices for internal control, with the aim of helping listed companies to design, implement, run and monitor their systems of internal control over financial reporting (ICFR).

In recent years, the concepts of enterprise risk management and internal control have been developed and standardised. These may be worth clarifying as ICFR is a key element in both processes:

- Enterprise risk management is a process designed to identify potential events that may affect the entity and manage any risks so that they remain within acceptable bounds, providing reasonable assurance regarding the achievement of objectives.
- Internal control is a process effected by an entity's board of directors, management and other personnel and designed to provide reasonable assurance regarding the achievement of objectives in effectiveness and efficiency of operations, reliability of financial reporting, and compliance with applicable laws and regulations while safeguarding the entity's assets.

Internal control is an integral part of enterprise risk management and its five basic components, as proposed by this framework, which need to be combined in an integrated process, are as follows: (i) control environment; (ii) risk assessment; (iii) control activities; (iv) information and communication; and (v) monitoring.

- ICFR is one aspect of internal control and comprises a set of processes that the board, audit committee, senior management and other personnel implement to provide reasonable assurance as to the reliability of the financial information disclosed to the markets. This framework is limited in scope to ICFR only.

Responsibility

The board of directors is responsible for having an adequate and effective ICFR system in place, while senior management, generally via its financial area, is responsible for its design, implementation and functioning. The audit committee is the body

charged with overseeing the ICFR and it is recommended that it should be supported in this task by an internal audit function. The internal audit function, following an annual audit plan, helps the committee assess the effectiveness of ICFR and reports to it periodically on weaknesses detected and on the progress of scheduled corrective measures.

The Unified Code also makes the audit committee responsible for supervising the process of preparation and the integrity of financial information including responsibility for reviewing compliance with regulations in force, the appropriate demarcation of the scope of consolidation and the correct application of accounting policies.

Also, the draft Spanish Audit Law designed to bring audit practice into compliance with EU regulations requires the audit committee to monitor the effectiveness of internal control, including ICFR, and monitor the process used to prepare and present financial information.

Voluntary nature

This framework, while respecting the principle of voluntary adoption, recommends a number of principles and good practices whose application will help improve the quality of ICFR systems. However, their adoption and application does not in itself guarantee effective ICFR. Companies must assess the adequacy of the design and functioning of controls and correct any weaknesses they find within a reasonable timeframe.

To enhance transparency on the markets, it would be helpful if the internal control framework and practice applied by each entity were disclosed through the annual corporate governance report. To help in preparing this information, a guidance document been drawn up (see Section III) including a checklist of indicators for each component of ICFR. Entities are asked to report on the implementation of each indicator, its characteristics and alternative systems used and make other relevant disclosures.

The recommendations in this framework are targeted at all listed companies in Spain, irrespective of their size, nature of the securities listed or business sector.

Binding definitions

Application of this framework requires companies to adhere to a number of principles and generally accepted elements of good practice. Although the framework is voluntary, the definitions given in this document to concepts and terms in its various sections are binding and, to help with their definition, a glossary of terms has been included as Appendix 1, which must be applied by entities that use these terms in their market disclosures on ICFR.

The purpose of using binding definitions is to enhance the usefulness and standardisation of the information that listed companies provide to investors and analysts.

If the entity follows another generally accepted framework for internal control it should expressly state which, and the definitions in this other framework would then be binding.

If the entity employs terms and concepts that are not formally defined in the framework selected – or alternatively is not following any generally accepted framework – it should satisfy itself that the terminology used is adequately defined in the report itself, to ensure a clear understanding of the specific control tools in use.

Financial information

The statutory financial information for Spanish companies is laid down by Royal Decree 1362/2007 of 19 October, and includes consolidated and individual annual and interim financial reports, and intermediate statements.

For the purposes of this framework and the other contents of this document, financial information includes the statement of financial position, income statement, statement of changes in equity, statement of cash flows, notes to the financial statements and the accounting information contained in the management report and quarterly interim reports.

Financial information must be adapted to take account of amendments to its reporting standards – Spanish General Chart of Accounts (Spanish GAAP) or International Financial Reporting Standards (IFRSs)– as well as other pertinent requirements.

Information to disclose to securities markets on the ICFR must be annual and refer to the same year as the annual financial report, notwithstanding the requirement for listed companies to keep the system permanently functional so that there is reasonable assurance that the information provided at interim reporting dates is reliable.

Reliability of financial reporting

Financial reporting is considered to be reliable if it presents the transactions, facts and other events affecting the reporting entity and consolidated group, in accordance with applicable standards. To achieve this, the entity's ICFR must establish that:

- (a) Transactions, facts and other events presented in the financial information exist in reality and were recorded at the right time (existence and occurrence).
- (b) The information includes all transactions, facts and other events in which the entity is the affected party (completeness).
- (c) Transactions, facts and other events are recorded and valued in accordance with applicable standards (valuation).
- (d) Transactions, facts and other events are classified, presented and disclosed in the financial information in accordance with applicable standards (presentation, disclosure and comparability).
- (e) Financial information shows, at the corresponding date, the entity's rights and obligations through the corresponding assets and liabilities, in accordance with applicable standards (rights and obligations).

ICFR as an integrated process

The ICFR system should provide reasonable assurance as to the reliability of the financial information that listed entities report to the securities markets.

To achieve this, the various components of an internal control system – control environment, risk assessment, control activities, information and communication and monitoring – must be coordinated and work in harmony to prevent, detect, offset, mitigate or correct instances of fraud or errors with a material impact on financial statements. When the system is reasonably designed and its components work properly, it can be said that it is effective and provides reasonable assurance that financial information has been reliably prepared.

Nonetheless, a weakness in one component does not necessarily mean that the internal control system as a whole is inadequate, provided that it is offset or mitigated by other components. As a result, assessing the effectiveness of ICFR means analysing a wide variety of issues and patterns of behaviour within the entity's organisation, and this in turn requires a fair dose of professional judgement.

Principles and good practice

The principles and good practices recommended by this framework draw on the internationally recognised reports by COSO (the Committee of Sponsoring Organizations of the Treadway Commission) but are limited to ICFR issues only.

COSO was used because of its wide international dissemination and because the extent to which this framework has been developed, taking into account areas going beyond financial reporting alone, means that the principles and good practices it recommends will be compatible with an integrated approach to risk management.

Also taken into account were the recommendations of the Unified Code where these relate to ICFR and its monitoring.

These principles and good practices are shown in the greyed-out panels below, listed in the same order as the five components of the COSO framework.

The entity's control environment

The control environment includes factors such as integrity, ethical values, professional competence, management philosophy and style as well as organisational structure. It sets the tone for behaviour in an organisation and directly influences staff awareness of internal control. It is the foundation for all other components of internal control, providing discipline and structure.

A significant percentage of human resources in any organisation are involved, either directly or indirectly, in preparing financial information. The work performed by the unit responsible for preparing the financial statements relies heavily on information provided by the organisation's other departments. As a result, the number of people involved in preparing financial information is much greater than the number actually responsible for drawing it up.

As a result, it is recommended that companies foster an environment of internal control within their organisation. Among the principles and good practices tending to achieve this aim are the following:

1. Compile and regularly update a statement of ethical values —either as part of the general code of conduct or in a separate document— regarding the reliability of financial information and compliance with applicable regulations, which is approved by the board of directors and communicated to all levels of the organisation.

This statement should be supported by specific explanations so that its importance and content are understood by everyone within the organisation.

2. Establish monitoring procedures to ensure respect for the principles of integrity and professional ethics, as well as measures to identify and correct violations of these values within the organisation.
3. The board of directors encourages open discussion of any relevant issue, for the entity and its group, regarding financial information.
4. Audit committee members, particularly the chairman, are appointed in light of their knowledge and experience of accounting, audit or risk management. There are also procedures in place to keep audit committees informed of regulatory changes in these areas.
5. Develop appropriate lines of authority and responsibility for the various processes involved in preparation of financial information, for each relevant functional area, location and business unit in the organisation.
6. The internal control model chosen is applied uniformly across the whole organisation and includes at least the following components: (i) a set of standards and duly documented procedures; (ii) a structure that supports the model and assures its correct functioning and compliance with regulatory requirements; and (iii) information tools that guarantee its integrity.
7. Ensure the organisation has adequate human and other resources and provides the personnel involved in preparing and reviewing financial information, or evaluating ICFR, with the necessary training to carry out their functions.

Such personnel should have sufficient up-to-date knowledge of accounting rules, auditing, internal control and risk management for their function and level of authority.
8. Employee performance reviews and the organisation's remuneration practices, including those of senior management, take account of and contribute to the reliability of financial information and are integrated within risk management policy.
9. The organisation must employ and retain people that have the necessary competencies to prepare financial information through a process of regular review and updating.

Risk assessment in financial reporting

Risk assessment allows the entity to analyse the impact of potential events on the achievement of objectives related to the reliability of financial information. Several types of risk can affect reliability, including: errors of calculation or application of standards, faulty systems, accounting fraud, ignorance of key information, incorrect estimates or projections and other risks of various kinds.

These general risks will translate into specific issues for each of the organisation's components and for each heading and item of financial information. These may vary from one entity to another. For instance, the risk of errors in recording income will be handled very differently by a entity that relies on estimates of the stage of completion of projects in progress, where control will focus on human error and fraud prevention procedures, than by another company which records thousands of transactions a day, where the emphasis will be on the robustness of IT systems.

Ignorance of, or a failure to update, the process for identifying risks of misstatement could have a material impact on financial information and undermine any control activity. This process is a cornerstone of any adequate control system and relies in turn on a thorough knowledge of the entity's businesses and procedures for financial reporting.

As a result, companies are expected to have a system – approved and monitored at appropriate hierarchical levels – to analyse these risks and to act as the basis for other ICFR components. Among the principles and good practices tending to achieve this aim are the following:

- 10. Specify financial reporting objectives with sufficient logic and clarity to enable the identification of risks that may result in material misstatement.**

These objectives should be aligned with the general objectives of the entity to ensure the reliability of financial information (existence and occurrence, completeness, valuation, presentation, disclosure and comparability, rights and obligations).

- 11. Identify and analyse risks to the achievement of financial reporting objectives as a basis for determining which controls should be put in place. In assessing the importance and likelihood of the risk of material misstatement, the entity considers circumstances such as: (i) complexity of the transactions and applicable regulations; (ii) volume of transactions and size of the accounting items affected; (iii) complexity of the calculations; (iv) need to use estimates or projections; (v) need to use judgment; and (vi) importance of the information.**
- 12. The potential for an error with material impact due to fraud is explicitly considered in assessing risks to the reliability of financial information.**

13. Risks to the achievement of financial reporting objectives are an integral part of the entity's risk mapping and, therefore, take account of the effects of other types of risks (operational, technology, financial, legal, reputational, environmental, etc.).

Control activities

Control activities have to take place at various levels of the organisation to reduce the risks of errors, omissions or fraud that might affect the reliability of the financial information. These activities must cover any risks identified in the process of initiating and authorising transactions and in registering, processing and disseminating financial information.

The board of directors and senior management will tend to use the following management control tools: comparative analysis of actual and forecast performance, indicators of changes in business and the financial position, budget projections and multiyear plans. It should also review the judgements and assumptions made in areas where transactions are most complex and have the greatest impact on the financial statements. As a result, besides the authorisation of significant transactions, the typical control activities carried out by the board and senior management will revolve around analytical reviews of estimates and projections used, and of the major assumptions made in preparing financial information.

Elsewhere in the organisation, control activities will usually consist of systematic procedures that require less overall knowledge of the entity's business. However, these control activities must be communicated by the senior management in a way that ensures they are well understood by all employees and correctly applied. Rolling out the control system through the organisation allows the board of directors and senior management to limit their functions to the abovementioned activities.

A clear distinction should be made between controls whose objective is to ensure effective and efficient operations and those whose aim is to ensure the reliability of financial information.

- Companies will normally have a set of procedures, controls and monitoring mechanisms designed to guarantee that operations are carried out correctly and the organisation's objectives are achieved. These arrangements are usually called operational controls.
- Control activities for ICFR cover all activities that address risks to financial information, including some that while principally serving an operational purpose also have a direct impact on such risks.

Among the principles and good practices tending to achieve this aim are the following:

14. Introduce controls that adequately address risks to achieving the objectives of reliable financial information and that prevent, detect, mitigate, offset or correct the potential impact of such risks long enough in advance.
15. Develop control activities – appropriate policies and procedures – taking account of their cost and potential effectiveness in mitigating risks at all stages of the financial reporting process, including critical judgments, estimates, evaluations, projections and closing of accounts.
16. Ensure that control systems include an appropriate mix of preventive measures (mitigating risks of errors or fraud in financial information) and detective measures (identifying misstatements and cases of fraud when they arise). Similarly, some controls must be carried out by people (manual) and others by the entity's IT systems (automated).
17. Design and implement controls for IT and communication systems that have an impact on financial reporting and the closing of accounts. These systems should guarantee at least secure access to data and programs, control of changes, correct functioning, business continuity and appropriate segregation of duties.

IT processes for the final user – including spreadsheets and other bespoke programs – must be documented, preserved, protected and regularly reviewed to maintain their integrity.

18. Define internal control policies, which should be formally approved and documented, to oversee the authorisation, contracting, monitoring and recording of activities outsourced to third parties.
19. Ensure that financial information records the impact, if any, of the entity's risk management policy. This policy will be detailed in the section of the annual corporate governance report relating to risk management systems.
20. Financial information and ICFR descriptions sent to the board for authorisation for issue must have been adequately revised by the persons responsible for their preparation.

Information and communication

IT and communications systems should identify, capture, process and distribute information on transactions, facts and other events affecting the entity, in a time-frame that allows those involved to carry out their assigned functions.

Internal communication systems are used to disseminate throughout the organisation the criteria, guidelines, instructions and, in general, all the information its

members need to carry out their functions in the time available. IT systems must be designed to provide all necessary internal and external data that might have a significant impact on financial statements.

The quality of internal and external IT and communication systems is critical to achieving the objective of reliability in financial information. Among the principles and good practices conducive to better reliability are the following:

- 21. Identify, capture and use relevant information at all levels of the organisation so that it can be disseminated in a form and timeframe that secures the objective of reliability in financial information.**
- 22. The source data for financial reporting are collected in a complete, accurate and appropriate manner for all transactions, facts and other events affecting the entity.**
- 23. Relevant information is identified, collected and communicated in a timeframe and form that allows those responsible for carrying out controls to fulfil their functions.**
- 24. Communication between the board of directors and senior management in matters relating to the reliability of financial information must be fluid enough for them to carry out their functions and responsibilities.**
- 25. Establish and formally communicate policies, processes and controls related to financial reporting to the employees involved, in such a way that they cover the activities of the whole organisation (accounting manuals, procedures for activities, etc.).**

Monitoring

Monitoring the system is fundamental to obtaining reasonable assurance that the risks of error, omissions or fraud in financial reporting are being effectively controlled, either by prevention, detection, mitigation, offsetting or correction. An internal control system, even when appropriately designed, may be failing partly or completely or may not be working in time or in the correct way, without this becoming apparent and being corrected.

Entities operate in a changing environment and risks may change for many reasons, including: (i) economic circumstances; (ii) changes in the business sector in which the entity operates; (iii) advances in IT; (iv) the emergence of new types of transaction; or (v) changes in financial reporting standards.

Among the principles and good practices tending to achieve this aim are the following:

26. The audit committee, so as to obtain reasonable assurance that the financial information is reliable, is responsible for overseeing:

- (i) The establishment of appropriate policies and procedures.
- (ii) The preparation and integrity of financial information, reviewing the design of the ICFR system and compliance with regulatory requirements.
- (iii) Adequate definition of the scope of consolidation, allowing for the possible existence of complex corporate structures, special purpose vehicles, holding companies, etc.
- (iv) The correct application of accounting principles.

It also oversees the organisation's continuous monitoring of control activities, so as to obtain reasonable assurance that ICFR is in place and effective.

27. In carrying out its oversight functions, the audit committee has an adequately resourced internal audit function, ensures its independence and effectiveness and also checks that senior management takes account of the conclusions and recommendations contained in its reports.

28. Oversight is carried out through a general understanding of the organisation's internal control system, of the risks it faces and the controls that mitigate them, of any deficiencies identified – which must be reported to the board and relevant management for correction – and through monitoring the corrective action taken to resolve them in an appropriate timeframe, taking into account the importance of the various different parts of the financial statements.

29. Information disclosed to the market about ICFR is given in sufficient, accurate and appropriate detail to be correctly interpreted and understood and is published in a form that allows it to be monitored.

30. To strengthen the transparency and quality of ICFR disclosures to the market, it is advisable that the external auditor should be involved in its review and issue a report setting out its conclusions. However it is understood that the entity, in the light of its particular circumstances, may decide not to call on the external auditor to review its ICFR disclosures, in which case it should explain its reasons.

Section III. Guidance for disclosures on internal control over financial reporting

General principles

Purpose and content of the guidance

This guidance document has been issued for a dual purpose: (i) to aid companies in drawing up their basic market disclosure on ICFR according to the framework provided in Section II of this paper; and (ii) to help users interpret and compare the information given.

The guidance document includes a series of references to internal control practices whose implementation must be described in narrative form. A considered response from companies regarding all the points covered is of prime importance to establish the development status of ICFR.

Companies should also offer any other information not specified in the guidance which helps towards a better understanding of their ICFR, bearing in mind their particular circumstances.

The references to internal control practices are grouped into five sub-sections corresponding to the five components of internal control systems described in Section II – *Reference framework*. Each sub-section includes a brief explanation of the information sought, the reasons why the practices stated are considered important and other pointers, so companies are clear as to what is expected of them. This is followed by a greyed-out panel specifying the data to be reported.

Alternative ICFR disclosure

The ICWG proposes that entities whose annual financial statements include:

- (a) A certificate signed by the company's chief executive and chief financial officer (or alternatively by the board of directors or audit committee) in which: (i) they expressly recognise their responsibility for establishing and maintaining an ICFR suited to the company's circumstances; (ii) they indicate the internal control framework to serve as a reference in assessing the effectiveness of the company's ICFR (provided this framework is generally accepted) and (iii) expressly

assert to the effectiveness of otherwise of the company's ICFR at the closing of accounts for the year, and

- (b) A report from the external auditors stating whether they view the company's ICFR as effective or otherwise at the closing of accounts, based on generally accepted auditing standards and using as reference a generally accepted internal control framework (along the lines of the SOX compliance report in the United States).

Should not be required to present the information proposed by the ICWG for general reporting purposes, though they are of course free to present it voluntarily.

Regarding the inclusion of the external auditors' report referred to in paragraph (b) above, in jurisdictions where such inclusion is mandatory, the time limit for publication shall be as they establish, unless the same report has previously been published on other securities markets.

Binding definitions

In preparing its information, the company should respect the binding nature of terms and concepts, or define them appropriately, as instructed in Section II Framework – *General issues – Binding definitions*. The purpose of using binding definitions is to enhance the usefulness and standardisation of the information listed companies provide to investors and analysts.

Characteristics of the information to be disclosed

The information to be supplied to investors pursuant to the following sections of this guidance document must have certain shared characteristics conducive to the greatest possible precision, clarity and comparability. It should accordingly:

- Keep blanket declarations and statements of principle to an absolute minimum. The purpose of this information is not to provide a theoretical explanation of the goals pursued, but rather a specific description of the control tools available to ensure the reliability of financial reporting.
- Avoid going into excessive detail about the mechanics of the organisation's control systems which would be of scant use to the users of the information.
- Be written in a way that would permit any user of financial information to form conclusions about the nature of the ICFR system, avoiding any technical jargon, internal or otherwise, that might impair understanding.
- Allow the market to evaluate and compare the information supplied by the company over the course of time and with respect to other companies.
- Respect the minimum contents specified, though companies are free to detail any other aspects they feel may give a clearer picture of the mechanisms making up their ICFR.

- Be provided annually referring to the same year as the financial statements, though companies must maintain their systems in constant operation so users can be reasonably sure of the reliability of the information contained in interim statements.

Basic indicators

The entity's control environment

The purpose here is to ensure that the market is informed about the specific mechanisms the company has deployed in order to maintain an internal control environment conducive to comprehensive, reliable and timely financial reporting (including the inputs used in drawing up financial statements), and which acknowledges the possible existence of failures or irregularities which must be detected and corrected.

The control environment starts with the tone set by senior management, which should strive to lead by example, establishing a code of conduct and adhering to its precepts, and ensuring that policies and procedures are properly designed and communicated.

Information on the company's control environment reveals the extent to which senior management take responsibility for maintaining a well ordered organisational structure and behavioural culture guided by the same principles that shape the other internal policies. Though experience shows that high-level rules and policies are not enough on their own to guarantee the honesty and rigour of organisational processes, their existence is nonetheless a valuable pointer. And the absence of such rules or flaws in the same can effectively sabotage the implementation of even the best internal control system.

For this reason, a basic principle is that the board of directors is ultimately accountable for the existence and regular updating of suitable, effective ICFR, with the audit committee assigned responsibility for its oversight and senior management for its design and implementation.

Also, a properly functioning ICFR requires a well documented organisational structure that draws clear lines of responsibility and authority, facilitating its effective communication through the organisation. Tasks and responsibilities should be allocated in such a way that senior management control extends to all organisational levels and activities.

Among the mechanisms for creating the right kind of culture in an organisation are those that acquire and retain the capacities needed to generate complete and reliable financial information.

Finally, a cornerstone of any well functioning ICFR system is that employees undertake to perform their work effectively and to report any operational failures or conduct contrary to ethics, internal policies and applicable regulations to the appropriate management level.

Accordingly, companies should specify at least the following components with a description of their main characteristics:

1. The bodies and/or functions responsible for: (i) the existence and regular updating of a suitable, effective ICFR; (ii) its implementation; and (iii) its monitoring.
2. The departments and/or mechanisms are in charge of: (i) the design and review of the organisational structure; (ii) defining clear lines of responsibility and authority, with an appropriate distribution of tasks and functions; and (iii) deploying procedures so this structure is communicated effectively throughout the company, with particular regard to the financial reporting process.
3. The existence or otherwise of the following components, especially in connection with the financial reporting process:
 - Code of conduct, approving body, dissemination and instruction, principles and values covered (stating whether it makes specific reference to record keeping and financial reporting), body in charge of investigating breaches and proposing corrective or disciplinary action.
 - ‘Whistle-blowing’ channel, for the reporting to the audit committee of any irregularities of a financial or accounting nature, as well as breaches of the code of conduct and malpractice within the organisation, stating whether reports made through this channel are confidential.
 - Training and refresher courses for personnel involved in preparing and reviewing financial information or evaluating ICFR, which address, at least, accounting rules, auditing, internal control and risk management.

Risk assessment in financial reporting

The purpose of these indicators is to inform the market about the degree of development and systematisation in the entity’s process for identifying the sources and risks of errors or irregularities in its financial reporting. The reliability of financial reporting depends on the correct application of current standards to routine or typical transactions, but also to less frequent transactions demanding the use of more complex rules which may have a material impact on financial statements.

Hence reference should be made to cases where the company’s operations are of greater complexity, involve a particularly large volume of transactions, present difficulties of calculation, estimation, evaluation or judgement, or have quantitative or qualitative materiality.

Failure to identify key financial reporting risks or to submit the risk identification and assessment process to periodic review can undermine any control activity, so the information that entities provide under this heading is of utmost importance.

The company should accordingly report the following at least:

4. The main characteristics of the risk identification process, including risks of error or fraud, stating whether:

- The process exists and is documented.
- The process covers all financial reporting objectives, (existence and occurrence; completeness; valuation; presentation, disclosure and comparability; and rights and obligations), is updated and with what frequency.
- A specific process is in place to define the scope of consolidation, with reference to the possible existence of complex corporate structures, special purpose vehicles, holding companies. etc.
- The process addresses other types of risk (operational, technological, financial, legal, reputational, environmental, etc.) insofar as they may affect the financial statements.
- Finally, which of the company's governing bodies is responsible for overseeing the process.

Control activities

Investors should be reliably informed of the scope of the specific control activities the entity has implemented to mitigate the risk of errors or irregularities in financial reporting. This is perhaps the broadest area of the control framework and the one which lends itself least to generalisations.

However hands-on experience directs us to certain critical areas that are common to many firms, such as: (i) procedures for confirming estimates and critical judgements; (ii) outsourced functions; and (iii) the systematisation and documentation of closing procedures. Also on the list are procedures whose scale or importance makes them a likely source of errors or omissions with a material impact on financial statements.

Current legislation lays responsibility for drafting financial statements on the board of directors. However, any organisation must necessarily have its financial information prepared and reviewed in a series of prior functions before it is certified by the board and disclosed to the markets. And we can assume that information users will want the assurance that critical accounting judgements, and the estimates underlying the main headings in the entity's financial statements or its budgetary projections are reviewed by senior management and the board of directors.

This review is considered a control activity in the lead-up to the disclosure of financial information and does much to ensure that the judgements and projections used concur with those of the entity's ultimate decision-makers and have been revised by them.

Accordingly, the entity should indicate the existence of at least the following components, and specify their main characteristics:

5. Documentation and flow charts of activities and controls (including those addressing the risk of fraud) for each type of transaction that may materially affect the financial statements, including procedures for the closing of accounts and for the separate review of critical judgements, estimates, evaluations and projections.
6. Internal control policies and procedures for IT systems (including secure access, control of changes, system operation, continuity and segregation of duties) giving support to key company processes regarding the preparation and publication of financial information.
7. Internal control policies and procedures for overseeing the management of outsourced activities, and of the appraisal, calculation or valuation services commissioned from independent experts, when these may materially affect the financial statements.
8. Procedures for reviewing and authorising the financial information and description of ICFR to be disclosed to the markets, stating who is responsible in each case.

Information and communication

The information sought is so investors know whether the entity has deployed procedures and mechanisms to convey the applicable control directives to the staff engaged in drawing up financial information, and are cognisant with the information systems giving support to such processes. Entities should accordingly state:

- (a) Whether they have a specific area in charge of establishing and maintaining updated the company-level policies, options, criteria and standards to be used in processing and recording transactions so they can be presented in due form in the financial statements.
- (b) The scope, development status, standardisation and automation of the information systems and tools used to generate the entity's published financial information.

The financial information supplied to the markets should be drawn up consolidating the information provided by different business units and components. Except for simple organisations or those completely integrated, this process will involve

procuring information from each unit in a format compliant with the standards applicable at entity level, especially when they use differing accounting standards, valuation rules and presentation formats. This requirement applies not only to statements of financial position, income statements, etc., but also the other information needed to draw up the notes to the financial statements.

Accordingly, the entity should state whether it has at least the following components in place, specifying their main characteristics:

- 9. A specific function in charge of defining and maintaining accounting policies (accounting policies area or department) and settling doubts or disputes over their interpretation, which is in regular communication with the team in charge of operations.**
- 10. A manual of accounting policies regularly updated and communicated to all the company's operating units.**
- 11. Mechanisms in standard format for the capture and preparation of financial information, which are applied and used in all units within the entity or group, and support its main financial statements and accompanying notes as well as disclosures concerning ICFR.**

Monitoring

Any internal control system can develop flaws if its operation is not regularly reviewed and monitored. Hence the need to provide itemised information on how the entity monitors its internal control system, particularly its ICFR, in order to prevent or remedy deficiencies in its design or operation. The points to be covered concern ICFR monitoring by the audit committee and should reflect actions taken to this end during the financial year.

In order to assess the development status of this ICFR component, it is vital that companies indicate the extent of internal communication of any incidents detected and whether the opportune measures have been taken or plans drawn up for their correction. Entities must also confirm whether the effects such shortcomings might have on financial information have been borne in mind during its preparation and specify if they have affected already published information, requiring its correction as per the applicable standards.

The monitoring process also empowers senior management to certify the overall effectiveness of ICFR design and operation. This may take place at the company's own volition or to comply, for instance, with corporate governance standards in other jurisdictions where it does business. In such cases, provided the entity has the corresponding external auditor's report, it can attach the documentation stated in Section III – *General principles – Alternative ICFR disclosure* in compliance with this guidance document.

If the entity has not conducted an annual review of the totality of its ICFR, it should indicate the scope of its review, the extent of results distribution, whether improvement actions have been taken, and whether possible weaknesses have been borne in mind when preparing financial information.

Accordingly, the entity should indicate the existence of at least the following components, describing their main characteristics:

12. An internal audit function whose competencies include supporting the audit committee in its role of monitoring the internal control system, including ICFR.
13. A discussion procedure whereby the auditor (pursuant to TAS), the internal audit function and other experts can report any significant internal control weaknesses encountered during their review of the financial statements or other assignments, to the company's senior management and its audit committee or board of directors. State also whether the entity has an action plan to correct or mitigate the weaknesses found.
14. Describe the scope of the ICFR assessment conducted in the year and the procedure for the person in charge to communicate its findings. State also whether the company has an action plan specifying corrective measures for any flaws detected, and whether it has taken stock of their potential impact on its financial information.
15. Describe the ICFR monitoring activities undertaken by the audit committee.
16. State whether the ICFR information supplied to the market has been reviewed by the external auditor, in which case the corresponding report should be attached. Otherwise, explain the reasons for the absence of this review.

Section IV. Audit committee monitoring of internal controls over financial reporting

The monitoring process

Concept and objectives of monitoring

The audit committee is the body responsible for monitoring financial reporting. This means seeing that financial information is correctly prepared and presented, legal requirements duly complied with, the scope of consolidation appropriately delimited and accounting principles rigorously applied.

The purpose of ICFR is to provide reasonable assurance that a company's financial information is reliable. The audit committee's monitoring activity seeks to ensure its continued effectiveness by gathering sufficient evidence of its correct design and operation. This means evaluating the process of identifying risks which could impair the fair presentation of financial statements, and checking that controls are in place for their mitigation and that these controls are working properly. Monitoring also involves reviewing, analysing and discussing financial information with management and internal and external auditors, to ensure that the accounting principles applied are the correct ones and the information supplied is complete and consistent with the company's operations.

System monitoring must be an ongoing process if it is to be effective over time. That said, assessments can also be conducted on a "snapshot" basis to see how control mechanisms or the control system as a whole are working on a specific date.

Support functions for monitoring

The job of drawing up financial information falls to the company's managers. Although the audit committee should be proactive in analysing key ICFR control and monitoring areas, it will normally commend the actual evaluation to support functions: (i) internal auditors; (ii) external auditors (except when legal incompatibilities arise); and (iii) other experts, with whom it will maintain a fluid dialogue in the furtherance of its supervisory responsibilities.

The audit committee will analyse any observations on ICFR received from support functions, whether made in the course of their normal duties or as a result of some special assignment.

In any case, audit committees will do all they reasonably can to ensure that personnel engaged in control activity monitoring tasks:

- Show integrity and independence in the pursuit of their duties, so the conclusions they reach are objective and impartial. This objectivity will depend, among other factors, on their relationship with and degree of distance from the control procedure under assessment and their level of authority and responsibility within the organisation.
- Have the right professional skills to perform their work diligently. In the case of more complex controls and risks, it is important that the staff charged with monitoring them have the necessary technical training.

A well-run internal audit function will give invaluable support to the audit committee in discharging its oversight responsibilities and monitoring the organisation's internal control system. In the course of the audit plan, as pre-approved by the committee, the internal auditor will send it regular reports with assessments of ICFR, summarising all the most important findings.

The external auditor, meanwhile, will assess internal control as part of its financial audit at sufficient length to establish the nature, timing and scope of the audit procedures necessary to express an opinion on the totality of the financial statements, informing the audit committee of any major weaknesses detected.

Once the information is in from internal and external auditors or other experts, the audit committee will make sure the weaknesses detected in the system have been notified and duly corrected.

A monitoring checklist

Senior management should identify critical processes and associated risks that might materially affect financial information, evaluate their potential severity and deploy mitigating measures. The audit committee, in its oversight role, should have a sound understanding of what constitutes an effective risk management and internal control system and sufficient information to review its assessment and verify that risks are being managed in accordance with the established procedures. Following is a checklist of components conducive to a well functioning monitoring system:

(a) Monitoring fundamentals:

- The board of directors and senior management take on board the importance of monitoring.
- The organisational structure accommodates the audit committee and senior management in the monitoring process.
- The personnel involved understand the goals of ICFR monitoring.

(b) Definition, design and execution of monitoring processes:

- Monitoring tasks are defined and included in the work plans of support functions, with a description of their essential features.

- Monitoring procedures allow controls to be evaluated in areas with meaningful risks.
- The controls selected are appropriate for assessing the effectiveness of ICFR.
- There is persuasive evidence to support conclusions about the effectiveness of control.
- Such evidence is assessed on a continuous or ad hoc basis.

(c) Evaluation and communication of results:

- Prioritise findings in evaluation reports.
- Provide the necessary support so conclusions about the effectiveness of ICFR are communicated and understood.
- Propose corrective actions and follow up their implementation as and when necessary.

Audit committee competencies

The Securities Market Law and Unified Code specify the following audit committee competencies in respect of ICFR:

- Monitor the preparation and the integrity of the financial information prepared on the company and, where appropriate, the group, checking for compliance with legal provisions, the accurate demarcation of the scope of consolidation, and the correct application of accounting principles.
- Understand the processes used to draw up the financial statements and provide reasonable assurance that the supporting IT systems are reliable.
- Review internal control and risk management systems on a regular basis, so major risks are properly identified, managed and disclosed.
- Monitor the independence and efficacy of the internal audit function; propose the selection, appointment, reappointment and removal of the head of internal audit; propose the department's budget; receive regular report-backs on its activities; and verify that senior management are acting on the findings and recommendations of its reports.
- Establish and supervise a mechanism whereby staff can confidentially report any irregularities they detect in the course of their duties, in particular those of a financial or accounting nature. Review all information received through this or other channels.

In addition, the entry into force of the regulatory changes referred to in Section I and the good practices described herein will give rise to new audit committee competencies as listed below:

- Review, analyse and discuss the financial statements and other key financial information with senior management and internal and external auditors, to check that information is reliable, understandable and relevant and that accounting policies are consistent with those applied at the preceding annual close.
- Approve the internal audit plan for assessing ICFR and receive periodic reports on its findings, as well as the actions scheduled to correct flaws or failures.
- Monitor the procedures developed by senior management to make meaningful estimates, evaluations and judgements, considering their impact on the financial statements.
- Monitor senior management decisions on adjustments proposed by the external auditor, and take note of any discrepancies, stepping in to mediate if necessary.

Audit committees will exercise these competencies with the appropriate degree of scepticism, asking searching questions and holding open meetings with managers and auditors.

The evaluation process

The following section details a number of basic issues related to the process of evaluating ICFR, which are meant to provide guidance and support for audit committees, and those to whom they commend the execution of these tasks, to achieve effective and efficient monitoring.

The audit committee should confirm that the process used to evaluate the system is robust enough to achieve its objectives and to validate the conclusions of the reports submitted to it by those carrying out the work of evaluation.

Documenting ICFR and the evaluation process

Adequate documentation of ICFR is an integral part of the control system. Not only does it help to clarify the organisation's control processes and activities, inform those involved of their responsibilities and describe the environment in which the controls operate, it also makes it easier to monitor and evaluate the system's design.

An appropriate evaluation of the design and operation of ICFR will require preliminary documentation prepared by management identifying objectives, risks and the associated controls along with records of their implementation.

Evaluating the design of ICFR

To obtain reasonable assurance that an ICFR system is well designed, the committee must adequately understand the risks to the financial reporting process and the control procedures put in place to mitigate them.

The criteria of effectiveness and efficiency require that efforts to identify and understand controls over financial reporting must extend beyond process controls to the entity's general controls.

Evaluating the risk identification process

When designing the ICFR system, the entity's senior management must establish, as a starting point, the objectives for achieving reliable financial reporting of each component and heading (existence and occurrence, completeness, valuation, presentation, disclosure and comparability, rights and obligations). Having defined these objectives, it must then identify the risks to each and the source and probability of errors arising, and assess the scale of their likely impact on financial reporting.

The work of evaluation should centre on reviewing the risk identification process carried out by management and concentrate on risks which, individually or jointly, may involve material misstatement or fraud in financial reporting.

Identification of controls to mitigate risks to financial reporting

Having evaluated the risk identification process, the focus shifts towards checking that the mechanisms put in place by management effectively mitigate the risks of errors with a material impact on financial reporting.

The mechanisms in place will include a range of control procedures and activities, including controls on processes, systems, accounting and transactions as well as the entity's general controls. General controls are "umbrella" procedures that cover the whole organisation and address the control environment and information and communication systems. They also include control activities carried out by the board and senior management which affect the entity as a whole.

Deficiencies may arise in the design of ICFR because there are insufficient controls to mitigate the risks identified or, where controls are in place, they are not effective enough or adequately targeted.

To decide if the design of a control or set of controls mitigates the risk of errors arising, the committee must come to a judgement as to whether the existing controls, functioning appropriately, can prevent or detect in time an error that would lead to a material misstatement in financial reporting.

To allow subsequent monitoring of ICFR operation, it is important to identify, during the process of evaluating its design, which points represent "key controls", i.e. controls that would adequately mitigate, long enough in advance, any material misstatement or fraud arising in its financial reporting.

Key controls include the entity's general controls and controls over processes. The impact that the entity's general controls have on ICFR components makes them critical to the effectiveness of monitoring and the efficiency of the process.

Each "key control" will be selected on the basis of its effectiveness in mitigating risks of error and its contribution to the efficiency of the monitoring process.

Evaluating the effective functioning of ICFR

Monitoring the ICFR components being evaluated will require the committee to check not only that they are well designed but also that they are functioning pro-

perly. Evaluation of the effective functioning of controls must concentrate on the areas of greatest risk and the key controls.

The key controls selected for evaluation can be either manual or run automatically by the IT systems in place. In the latter case, evaluation will extend to reviewing general controls over these systems.

Standard of evidence

The standard of evidence required to conclude that a control is working adequately will be directly proportional to two factors: (i) the inherent risk of the ICFR control concerned; and (ii) the risk of it causing a material misstatement in financial reporting:

- Evaluating the inherent risk of a control failing involves analysing the following points: the type, frequency and complexity of the control, the risk of evading the controls in place, the estimates and judgments that need to be made for it to function, the competence of the personnel involved, the nature and scale of the errors it is meant to prevent or detect, the degree of its reliance on other controls being effective, and accumulated experience of how the control has functioned during previous processes.
- Evaluating the risk of a material misstatement in financial reporting involves considering both the materiality of the accounting item being reported, and whether the supporting documentation or transactions may contain errors that would have a material impact on the financial statements.

Factors to be considered when judging the scale of the risk of material misstatement include whether: (i) the item being reported on is based on estimates or is valued using internal models; (ii) it is susceptible to the risk of fraud; (iii) it is the subject of complex accounting standards; (iv) there have been changes in the nature or volume of transactions that comprise it; and (v) it is sensitive to changes in the technological, economic, financial environment, etc.

Methods for gathering evidence

Evidence can be gathered through direct validation tests on the controls, through monitoring procedures or through a combination of the two. Tests provide evidence up to the time they are carried out.

When drawing up plans to evaluate the functioning of a control the following points must be decided: (i) the nature of the tests to be run; (ii) the timeframe to be evaluated; (iii) the scope of the tests on the control; and (iv) the objectivity and competence of those carrying out the tests.

The nature, timeframe and scope of the resulting validation will depend on the standard of evidence required to conclude that the control concerned is functioning effectively.

Considerations with multiple locations

While there are cases where certain risks of errors in financial reporting can be mitigated by central controls, complete monitoring of ICFR demands that the entity examine all its significant locations and business units.

Control activities that have been designed and implemented in a standardised and centralised manner to prevent a single risk in several locations can be assessed globally. However, those that have not and which are specific to the location where the entity operates will need to be evaluated individually, in accordance with the review scope established.

Evaluating control weaknesses

The process of financial reporting requires the entity to consider and evaluate any weaknesses identified. These will be notified to the managers of the system so that they can correct them. Corrective action becomes more urgent and important when the weaknesses detected are thought to have a material impact on the reliability of financial reporting.

In evaluating the impact of a control weakness, or a set of ICFR weaknesses, thought should be given to how it would affect the level of assurance required to record transactions in compliance with applicable standards. In a complete evaluation, the entity must determine the impact of each significant control deficiency to verify whether, on its own or in combination with other shortcomings, it could become a material weakness.

Evaluating the impact of one or several ICFR weaknesses means looking at both quantitative and qualitative considerations, in order to: (i) determine whether there is a reasonable possibility that the internal control would fail to prevent or detect in time an error in an item or note in the financial statements (probability of occurrence); and (ii) what would be the severity of the potential error arising from such weakness(es).

Monitoring and evaluation schedule

The internal control system must be continuously monitored.

The scope of ICFR evaluation in each period is at the audit committee's discretion and must be based on the objectives and risks of financial reporting. Evaluations can cover the whole of ICFR every year or else be strung out over several years, in which case the following options can be considered:

- Establish a rotation policy for the different parts of the financial statements or locations, so that they are all covered in periods no longer than every two or three years, bearing in mind such factors as: (i) the results of previous evaluations; (ii) whether or not the control processes have changed; (iii) the risk of errors by reference to their probability, nature and impact; and (iv) the carrying out of unscheduled tests.

- Focus on the processes most critical to financial reporting (the entity's general controls, closing of accounts, general IT controls, etc.).

If the evaluation is being done to determine its effectiveness on a specific date, tests will focus on the risks and controls existing at that time.

Appendices

Appendix 1

Glossary of terms and acronyms

Glossary of terms (Binding definitions)

To enhance the usefulness and standardisation of the information that listed companies provide to investors and analysts, we present below the binding definitions used in the different sections of this document:

Accounting policies area or department: an internal group within the entity responsible for defining accounting policies for subsequent application throughout the organisation, so as to ensure compliance with applicable financial reporting standards, and for settling doubts or conflicts over their interpretation.

Closing of accounts procedure: final process of grouping and consolidating information from an entity's various business units and recording adjustments calculated at corporate level.

Code of conduct: a document setting out the core principles and values that must govern the actions of the organisation's staff and their responsibilities in the event of fraud, malpractice or unlawful conduct, with the aim of establishing a generally accepted corporate ethical code.

Compensating controls: controls which are used to meet the objective of another control that failed to work properly, and which help reduce risk to an acceptable level.

Control activities/control: policies and procedures that help ensure management policy decisions are put into effect. Control activities, whether automated as part of the IT system or carried out through manual process, can serve a range of control objectives and be applied at different functional and organisational levels.

Control environment: controls originated by management and cascaded through all levels of the organisation. The concept extends to the internal control functions, attitudes, awareness and activities of governing bodies and management, and the importance attached to ICFR.

Detective controls: controls designed to detect errors or irregularities that might affect financial reporting.

Disciplinary regime: set of formal rules that lay down the consequences for members of an organisation of a confirmed breach of the code of conduct.

Enterprise risk management: process designed to identify potential risks that may affect the organisation, manage risks to keep them within the bounds acceptable to the management and thereby provide reasonable assurance as to the achievement of the entity's objectives.

Error: for the purposes of this document, any accidental or intentional action that results in the omission or misstating of information, with the result that financial reporting fails to comply with the reporting standards applying to the entity.

Financial information: this is understood to mean the content of the annual or interim financial statements, including the statement of financial position, income statement, statement of changes in equity, statement of cash flows, notes to the financial statements and the accounting information contained in the management report and quarterly interim reports.

Fraud: an intentional act committed by one or more people among the company's managers, employees or third parties, which involves the use of deception to obtain an illegal or unfair advantage.

General controls of an entity: controls that operate over the whole organisation and generally take effect through controls at process, transaction or application level. An entity's general controls will vary in their precision and nature and may directly or indirectly affect the likelihood of an error being prevented or detected in time.

ICFR monitoring: a set of activities to verify that internal control policies and procedures in place to assure the reliability of financial reporting have been appropriately designed and are operating effectively, so as to provide reasonable assurance that the system is effective in preventing, detecting and correcting any material error or fraud in financial reporting.

ICFR weakness: an internal control weakness originating from:

- A weakness in the system's design, due to the absence of controls necessary to guarantee the reliability of financial reporting or because of design faults in existing controls so that even though the control operates effectively the risk remains uncovered, or
- A weakness in the system's functioning because the controls in place, although adequately designed, fail to operate effectively.

Information and communication: information systems identify, capture, process and disseminate information on transactions and events. Communication systems disseminate through the organisation the criteria, policy directions, instructions and other information that the members of the organisation need to understand their functions and the manner and timeframe within which they must be carried out.

Internal audit: an independent and objective function within the organisation providing assurance and advice, conceived to add value and improve the organisation's operational effectiveness. It helps to organise and achieve its objectives by bringing a systematic and disciplined focus to evaluating and improving the effectiveness of the risk management, control and corporate governance processes.

Internal control over financial reporting (ICFR): the set of processes implemented by an entity's board, audit committee, management and other personnel concerned to provide reasonable assurance as to the reliability of the financial information disclosed to the markets.

Internal control: process effected by the organisation's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:

- Effectiveness and efficiency of operations.
- Reliability of financial reporting.
- Compliance with regulations applicable to the entity.
- Safeguarding of assets.

Key controls: controls that adequately mitigate, long enough in advance, the risk of fraud or errors of material impact in published financial information. They include general controls at entity level and control activities selected for their effect in mitigating any material misstatement in financial reporting.

Listed companies: companies issuing securities that are traded on regulated securities markets.

Management: people with executive responsibility for carrying out the company's activities, reporting to senior management.

Manual of accounting policies: a document specific to each entity and disseminated through all its component units, setting out and explaining the standards for financial reporting and how they must be applied to the entity's specific operations. The recording standards in the accounting manual are based on those applying to the entity (usually IFRSs or the Spanish General Chart of Accounts), have been adapted as required for internal use, indicate specific options taken up by the entity, and cover all types of transactions carried out by the entity.

Material weakness: a weakness or set of weaknesses in ICFR that creates a reasonable possibility of material misstatement in financial reporting and which is neither prevented nor detected in time (see definition of *Materiality*).

Materiality: the size of an error or omission in financial reporting that may change or influence the reasonable judgement of an individual.

Preventive controls: controls designed to prevent errors or irregularities that might affect financial reporting.

Process controls: controls over an organisation's operating processes that are more specific than general controls.

Reasonable assurance: however well designed and effective risk management may be, it cannot provide an absolute guarantee that the entity's objectives will be met, due to its inherent limits.

Risk assessment: process to identify and evaluate risks affecting the reliability of financial reporting and deploy policies to address them.

Risk: the possibility that an event may occur and adversely affect the reliability of financial reporting.

Senior management: managers reporting directly to the board or chief executive of the company as well as in all cases the internal auditor.

Significant risk: a risk whose potential impact could be material and which demands special attention.

Significant weakness: a weakness or set of weaknesses in ICFR that is less severe than a material weakness, but sufficiently serious to demand the attention of those monitoring the process of financial reporting.

Unified Code: the unified code for the good governance of listed companies, published by the CNMV in May 2006.

Whistle-blowing channel: a direct route to the audit committee, whose existence and access points are disseminated to all members of the organisation, outside the usual reporting hierarchy, so they can report irregularities that come to their attention, mainly of a financial or accounting nature.

Glossary of acronyms

ACGR: Annual Corporate Governance Report

CNMV: Spanish National Securities Market Commission

COSO: Committee of Sponsoring Organizations of the Treadway Commission (working group sponsored by five organisations and including professionals from the fields of internal audit, external audit, accounting, finance and the academic world, established in 1985 with the aim of creating a framework for internal control. Its first framework, published in 1992, has undergone subsequent developments focusing on issues such as risk management, monitoring, adaptation to smaller companies, etc.)

IASs: International Auditing Standards

ICAC: Spanish Accounting and Audit Institute

ICWG: Internal Control Working Group on financial reporting (sponsored by the CNMV)

IFRSs: International Financial Reporting Standards

LMV: Securities Market Law

PGC: Spanish National Chart of Accounts

SOX: Sarbanes-Oxley Act of 2002

TAS: Technical Accounting Standards issued by ICAC

Appendix 2

Procedures for external auditor review

External auditors conducting a review of an entity's ICFR disclosures in its annual report should base the principle procedures they follow on:

1. Reading and understanding of the information prepared by the entity regarding ICFR – disclosures included in the management report – and an evaluation of whether this information meets all the minimum reporting requirements as described in Section III Guidance for ICFR disclosures.
2. Questioning of personnel responsible for drawing of the information detailed in point 1 above: (i) to obtain an understanding of the process that goes into drawing up the information; (ii) to obtain information that permits an evaluation of whether the terminology used complies with the framework definitions; and (iii) to obtain information on whether the control procedures described are in place and functioning.
3. Review the explanatory documents supporting the information detailed in point 1 above, including documents directly made available to those responsible for describing ICFR systems. The documentation to be reviewed may include reports prepared for the audit committee by internal audit, senior management and other internal or external specialists.
4. Comparison of the information detailed in point 1 above with their knowledge of the entity's ICFR obtained through the external audit procedures applied during the annual audit.
5. Reading of the minutes taken at meetings of the board of directors, audit committee and other committees of the entity to evaluate the consistency between the ICFR business transacted and the information detailed in point 1 above.
6. Obtaining a management representation letter in connection with the work performed, signed by those responsible for preparing and formulating the information detailed in point 1 above.

The report should list the specific procedures carried out and report as exceptions any discrepancies between the information obtained as a result of the review procedures and the information reported by the entity.

These procedures are not of sufficient scope for the external auditor to give an opinion on the quality of the design of the ICFR system reported, the completeness of the risks identified by the entity, the adequacy and proper functioning of the controls in place to mitigate them or assertions by the entity to the model's effectiveness (design and effective functioning).

Accordingly, entities may voluntarily request an evaluation of the effectiveness of their ICFR, to cover its design, effective functioning or both. Clearly, the scope of such an evaluation as well as the level of assurance and type of opinion provided will differ from those of the above report.

Such activities should in any case be performed in accordance with a future set of professional guidelines.

Appendix 3

Members of the working group and CNMV support

Chairman

José Luis López Combarros

Members

BANCO BILBAO VIZCAYA ARGENTARIA, S.A.	Javier Malagón Navas, Raymundo Mendoza Vázquez
BANCO SANTANDER, S.A.	Juan Guitard Marín, Fernando Revuelta Revuelta
DELOITTE, S.L.	Luis Manuel Carro Martínez
ERNST & YOUNG, S.L.	Ana María Prieto González
GAMESA CORPORACIÓN TECNOLÓGICA, S.A.	Félix Zarza Yabar
GAS NATURAL SDG, S.A.	Carlos Ayuso Salinas, Laura de Miguel Pascual
FERROVIAL, S.A.	Jesús Herranz Lumbreras, Jesús Saavedra Lorenzo
IBERIA LÍNEAS AÉREAS, S.A.	Martín Cuesta Vivar, Antonio Toledo Gonzalo
INDITEX, S.A.	Carlos Crespo González
INDRA SISTEMAS, S.A.	Javier de Andrés González, Carlos Campos Carrizo
INSTITUTO DE AUDITORES INTERNOS DE ESPAÑA	Luis Aranaz Zuza, Javier Faleato Ramos
KPMG ASESORES, S.L.	Tomás López de la Torre Vázquez
MAPFRE, S.A.	José Manuel Muries Navarro, Blanca Sotillo Alonso
PRICEWATERHOUSECOOPERS, S.L.	Rocío Fernández Funcia, Carlos Sobrino Hernández
REPSOL YPF, S.A.	Isidoro Mansilla Barreiro, Miguel Torres López
TELEFÓNICA, S.A.	Jesús García Cuadrado
URÍA MENÉNDEZ ABOGADOS, S.L.P.	Cándido Paz-Ares Rodríguez

CNMV support

Paulino García Suárez

Antonio Cano Muñoz

Marta Ortega Arranz

Gema Gullón Pérez
