

# **A Conceptual Basis of Internal Audit**

# 1 Nature and Content of Audits

## 1.1 General Definition of Audit

### KEY POINTS

- During audits, an independent party compares the existing condition to pre-determined criteria (such as US-GAAP, or the policies and procedures of the organization).
- Audits serve two important control functions. Firstly, they are detective control mechanisms by which auditors identify and investigate variances or deviations from predetermined standards. Secondly, they are used as preventive control mechanisms because the expectation of an audit should deter individuals from engaging in fraudulent financial reporting or making careless errors.
- In the course of their evaluation, auditors identify business risks and evaluate the effectiveness and efficiency of the control systems designed to avoid, reduce or eliminate those risks. Auditors should also be aware of the risk of fraudulent activities.
- The primary goal of auditing is to serve the company by providing an independent and objective evaluation of the organization's adherence to operational, financial and compliance policies, guidelines and regulations.
- Likewise, audits are performed to protect the interests of third parties, such as investors and creditors.

### Auditing in General

In general, auditing is defined as a systematic process of objectively obtaining and evaluating evidence regarding the current condition of an entity, area, process, financial account or control and comparing it to predetermined, accepted criteria and communicating the results to the intended users. The criteria to which the current state is compared may be a legal or regulatory standard (such as the Sarbanes Oxley Act), or internally generated policies and procedures.

### Internal Control

Internal control is defined as,

*“a process affected by an entity's Board of Directors, management or other personnel – designed to provide reasonable assurance regarding the achievement of objectives in the following categories:*

- (1) reliability of financial reporting,*
- (2) effectiveness and efficiency of operations, and*
- (3) compliance with applicable laws and regulations”* (COSO 1992).

Further, the Institute of Internal Auditors (IIA) defines control as, “any action taken by management to enhance the likelihood that established objectives and goals will be achieved” (Sawyer et al. 2003). Controls may be preventive (to deter undesirable events from occurring), detective (to detect and correct undesirable events which have occurred), or directive (to cause a desirable event to occur). A control system is the integrated composition of control components and activities that are used by an organization to achieve its objectives and goals.

Audits are part of the overall control system of an organization and provide several important control functions. Firstly, they can serve as detective control mechanisms – that is, through their audit investigations, auditors may identify and evaluate errors or omissions, or variances between the current condition and predetermined criteria. Secondly, audits can be a preventive control mechanism, such that errors, misstatements and fraudulent activities do not occur in the first place. Finally, the results of audits should be used to identify and propose any potential improvements to the audited entity.

Audits entail comparing the current, existing condition of a process, organization, division or account to predetermined, accepted criteria. A variety of audit procedures may be used. Audit procedures are the activities that the auditor performs to obtain sufficient, competent evidence to ensure a reasonable basis for the audit opinion. Examples of some audit procedures available to auditors include: observation of personnel or procedures, physical examination of assets, inquiries or interviews with personnel, confirmation with outside parties, recomputation or recalculation of data, examination of documents, and analytical procedures.

The final objective of audits is to preserve the interests of various third parties, including investors and creditors. In this regard, audits must comply with the standards of the third parties and any applicable regulations. For example, from an accounting perspective, audits of financial reporting must focus on the accuracy of the organization's financial statements and must be performed in accordance with the standards of the Public Company Accounting Oversight Board (PCAOB). Alternatively, audits of internal controls over financial reporting provide an assessment of the risks and controls relevant to the operations affecting the financial reporting process and financial data and should be based on a formal control framework, such as the COSO Internal Control Integrated Framework (see Section A, Chapter 1.2 and 1.3). Internal control assessments should also be performed in accordance with the guidance of the PCAOB.

## Objectives of Audits

## Audit Procedures

## Preserving the Interests of Third Parties

### LINKS AND REFERENCES



- COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION (COSO). 1992. *Internal Control Integrated Framework*. New York, NY: AICPA.
- INSTITUTE OF INTERNAL AUDITORS. 2004. *Standards for the Professional Practice of Internal Auditing*. Altamonte Springs, FL: The Institute of Internal Auditors.
- KEITH, J. 2005. Killing the Spider. *Internal Auditor* (April 2005): 25–27.
- MESSIER, W. F. 2003. *Auditing and Assurance Services: A systematic approach*. 3<sup>rd</sup> ed. Boston, MA: McGraw-Hill.
- PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD (PCAOB). 2004. *Auditing Standard No. 2: An Audit of Internal Control Over Financial Reporting Performed in Conjunction With an Audit of Financial Statements*. [http://www.pcaobus.org/Standards/Standards\\_and\\_Related\\_Rules/Auditing\\_Standard\\_No.2.aspx](http://www.pcaobus.org/Standards/Standards_and_Related_Rules/Auditing_Standard_No.2.aspx) (accessed May 31, 2007).
- RITTENBERG, L. E. AND B. J. SCHWEIGER. 2005. *Auditing: Concepts for a changing environment*. 5<sup>th</sup> ed. Boston, MA: Thompson.

- ROBERTSON, J. C. AND T. J. LOUWERS. 1999. *Auditing*. 9<sup>th</sup> ed. Boston, MA: Irwin/McGraw-Hill.
- SAWYER, L., M. DITTENHOFER, AND J. SCHEINER. 2003. *Sawyer's Internal Auditing*. 5<sup>th</sup> ed. Altamonte Springs, FL: The Institute of Internal Auditors.
- SEARS, B. 2002. *Internal Auditing Manual*. New York, NY: Warren, Gorham & Lamont.

## 1.2 Definition of Internal Audit

### KEY POINTS

- Internal auditing is an independent, objective assurance and consulting activity designed to assess the effectiveness of the control environment, add value, and improve an organization's operations.
- In the past, Internal Audit was regarded as merely focused on financial and accounting matters, but today its role has developed to include active risk and control evaluations and is considered integral to the corporate governance process.
- The internal audit function is part of the internal monitoring system of the organization and therefore should be positioned within the organization such that the independence of internal auditors can be guaranteed. Ideally, Internal Audit should report functionally to the Audit Committee of the Board of Directors and administratively to the Chief Executive Officer (CEO) of the organization.
- Generally, an internal audit is a multi-step process aimed at determining whether existing processes and procedures (the condition) comply with applicable rules and regulations (the criteria) or deviate in any way from these criteria.
- The Committee of Sponsoring Organizations of the Treadway Commission (COSO) established the concepts and criteria that an internal audit function should follow in practical terms.

#### IIA Definition

The Institute of Internal Auditors (IIA), which is the international professional organization that oversees internal audit guidance, certification, education, and research, defines internal auditing as:

*[...] an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.* (IIA Standards for the Professional Practice of Internal Auditing, Glossary)

#### Transformation of Internal Audit

The IIA's definition demonstrates the transformation that Internal Audit has undergone in recent years with regard to its role and how it is perceived. In the past, Internal Audit was regarded as a management support function that generally focused on financial and accounting matters. Now its role may include active risk management, which – along with traditional auditing – is an integral part of the corporate governance process. Internal Audit no longer focuses only on transac-

tions that occurred in the past to determine whether control systems were effective. Today's internal auditors also look ahead to identify the potential risks that may adversely affect the organization and to evaluate the control mechanisms that will avert or minimize them. Moreover, the activities of internal auditors are no longer limited strictly to audit tasks; management consulting is now considered an important and expanding role for internal auditors. Thus, when internal auditors identify areas for improvement in the course of their regular audit work, they will also suggest recommendations as to how the organization can improve its operations.

Internal audits allow management to delegate its oversight function to the internal audit department. In larger companies management can not perform the oversight function itself for several reasons, including,

- growing complexity of the operating environment due to automated data processing,
- increased decentralization in physical location and decision-making as a result of globalization or internationalization, and
- its lack of expertise required to conduct efficient, high-quality audits.

Internal Audit is part of the internal monitoring system of an organization. This system comprises all monitoring measures and precautions put in place within the company to secure assets and guarantee the accuracy and reliability of the accounting system. This task is managed with objective-based and compliance-focused comparisons between the existing condition and the accepted criteria, as required by all applicable policies, regulations, and laws.

In recent years, internal control has become increasingly important. This is evidenced in the numerous laws, regulations and standards that now require that organizations have an internal audit function or an internal control review. Several of the most influential requirements are described further in Section A, Chapter 1.3.

Generally, an internal audit is a multi-step process aimed at determining whether existing processes and procedures (the condition) comply with predetermined rules and regulations (the criteria) or deviate in any way from this standard. Firstly, to perform an internal audit, the auditors must identify and understand the criteria to which the condition must be compared. Secondly, internal auditors collect evidence regarding the existing condition. Thirdly, Internal Auditors analyze and evaluate the evidence. Analysis and evaluation may include (among other activities):

- observation of processes and procedures,
- inquiry of key participants in the processes,
- comparison of current period information with prior year information,
- comparison of current information with budgets and forecasts,
- comparison of current activities with approved policies and procedures,
- sampling and testing the actual performance to the desired performance,
- utilizing computer assisted audit tools to review, compare and analyze large amounts of data.

**Support for Corporate Management**

**Systematic Positioning of Internal Audit**

**Internal Audit in the Context of Legal Requirements**

**Internal Audit Process in General**

Fourthly, based on this analysis and evaluation, Internal Auditors draw conclusions about the effectiveness of the control systems and the extent to which the current condition meets the required criteria. Finally, the results of the work and the conclusions drawn by the auditor are communicated to the relevant parties (audited units, management etc.) along with any necessary recommendations for improvement in the form of an audit report. It is management's responsibility to act upon the results of an auditor's evaluation.

#### **Audit Team**

An internal audit is generally conducted by a team of auditors (i.e., more than one auditor). As internal audits vary in size and content, the size of the internal audit teams working on each audit also fluctuate. One of the auditors acts as team lead who is responsible for planning and overseeing the audit, as well as communicating with the auditees, while other audit team members execute the audit activities (for the organization of audit teams, see Section A, Chapter 4.4).

#### **Reporting**

After the internal audit, the results and findings are reported to the Audit Committee, senior management, and the manager responsible for the audited unit. The results are also shared with the employees concerned. As necessary, other parties with interests in the audit may be informed of the results; these parties may include creditors, strategic partners and external auditors (for reporting on completed audits, see Section B, Chapter 5).

#### **COSO**

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) has defined criteria for audits on which the work of Internal Audit should be based. COSO is “*a private-sector organization dedicated to improving the quality of financial reporting through business ethics, effective internal controls, and corporate governance*” (see [www.coso.org](http://www.coso.org)).

#### **Key COSO Internal Control Concepts**

COSO provides criteria for establishing internal control and evaluating its effectiveness. Further, COSO defines key concepts that explain the purpose and performance of internal control as follows:

- *Internal control is a process. It is a means to an end, not an end in itself.*
- *Internal control is affected by people. It's not merely policy manuals and forms, but people at every level of an organization.*
- *Internal control can be expected to provide only reasonable assurance, not absolute assurance.*
- *Internal control is geared to the achievement of objectives in one or more separate but overlapping categories.* ([www.coso.org/key.htm](http://www.coso.org/key.htm))

#### **HINTS AND TIPS**



- The internal audit function should remain independent from all other departments within the organization. This allows internal auditors to maintain objectivity as they perform their audit activities.
- Internal auditors should familiarize themselves with their organizational position within the company and when necessary, clearly communicate to their

auditees how they fit in the organization and what their primary service is to the organization.

- Internal Audit must meet the needs of the organization. Therefore, the organization's strategy, objectives, and structure must be understood before determining how Internal Audit will fit into it.

#### LINKS AND REFERENCES



- COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION (COSO). 1992. *Internal Control Integrated Framework*. New York, NY: AICPA.
- COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION (COSO). 2004. *Enterprise Risk Management Integrated Framework*. New York, NY: AICPA.
- INSTITUTE OF INTERNAL AUDITORS. 2004. *Standards for the Professional Practice of Internal Auditing*. Altamonte Springs, FL: The Institute of Internal Auditors.
- KEITH, J. 2005. Killing the Spider. *Internal Auditor* (April 2005): 25–27.
- MESSIER, W.F. 2003. *Auditing and Assurance Services: A Systematic Approach*. 3<sup>rd</sup> ed. Boston, MA: McGraw-Hill.
- REDDING, K., P. SOBEL, U. ANDERSON, et al. 2007. *Internal Assurance and Consulting Services*. Altamonte Springs, FL: The Institute of Internal Auditors.
- RITTENBERG, L. E. AND B. J. SCHWEIGER. 2005. *Auditing: Concepts for a Changing Environment*. 5<sup>th</sup> ed. Boston, MA: Thompson.
- ROBERTSON, J. C. AND T. J. LOUWERS. 1999. *Auditing*. 9<sup>th</sup> ed. Boston, MA: Irwin/McGraw-Hill.

### 1.3 Regulatory and Organizational Framework

#### KEY POINTS



- Internal audits are subject to a large number of regulatory and organizational requirements. Recent notable regulations and guidance have been developed in the US, Germany, UK, Canada, Japan, China, and Hong Kong.
- Independence of both internal and external auditors is more important than ever before. Therefore, Internal Audit should be an independent staff department.
- The internal audit function can either be centralized or decentralized based on the needs of the organization.

Audits are subject to a variety of regulatory and organizational conditions. Regulatory standards have undergone particularly rapid development in recent years as a result of several new legislative initiatives.

#### Overview

## Regulatory Standards

A number of new regulations have been passed in recent years, which affect not only external auditing, but also the internal audit function. Many standards and legal requirements now address the internal audit process directly, or the internal control structure of organizations. For the internal audit function, the following laws, standards and guidance provide the most explicit directives (details regarding internal audit and internal control are provided below):

- United States:
  - Sarbanes Oxley Act of 2002 (SOX),
  - NYSE Listing Standards,
  - COSO Internal Control Integrated Framework,
  - COSO Enterprise Risk Management Integrated Framework,
  - COBIT® Control Objectives for Information and related Technology.
- Germany:
  - Act on Control and Transparency in Business (KonTraG),
  - German Corporate Governance Code (DCGK),
  - Transparency and Disclosure Act (TransPuG),
  - Accounting Legislation Reform Act (BilReG).
- United Kingdom: The Turnbull Report: Internal Control Requirements of the Combined Code.
- Canada: Canadian Securities Administration Rules.
- Japan: Financial Instruments and Exchange Law.
- China: Code of Corporate Governance.
- Hong Kong:
  - Rules Governing the Listing of Securities on the Stock Exchange of Hong Kong Limited,
  - Rules Governing the Listing of Securities on the Growth Enterprise Market of the Stock Exchange of Hong Kong Limited.

**SOX** The Sarbanes-Oxley Act of 2002 (SOX) was enacted by the United States Congress in response to several major accounting scandals in 2001 and 2002. The explicit purpose of the Act is to “protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws” (US Congress 2002). The Act is applicable to all publicly registered companies listed on U.S. stock exchanges and under the jurisdiction of the U.S. Securities and Exchange Commission (SEC). This includes any foreign firm that is listed on a U.S. stock exchange. SOX has several sections, the most important to Internal Audit are section 302, requiring the CEO and CFO (Chief Financial Officer) to certify the validity of the financial statements, section 404, which requires that management assess and report on the effectiveness of the internal controls over financial reporting and that the independent external auditor attest to that assessment, and section 806, which protects employees, known as whistleblowers, who report fraudulent behavior (see Section A, Chapter 2.6 and Section D, Chapter 13).

**NYSE Listing Standards**

New York Stock Exchange (NYSE) Final Corporate Governance Rules require that all listed companies have an internal audit function to “provide management and the audit committee with ongoing assessments of the company’s risk management processes and system of internal control” (NYSE 2003). Compliance with NYSE listing standards has been mandatory since November 2003.

**COSO IC**

The COSO Internal Control Integrated Framework (IC) was developed in 1992 to provide a model for evaluating internal controls and is recognized as the standard against which organizations should measure the effectiveness of their internal control systems. COSO defines internal control as:

*A process, effected by an entity’s board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following three categories:*

- effectiveness and efficiency of operations,
- reliability of financial reporting,
- compliance with applicable laws and regulations (COSO 1992).

COSO defines internal control as consisting of five interrelated components:

- control environment,
- risk assessment,
- control activities,
- information and communication, and
- monitoring.

COSO’s broad definition of control marks a significant departure from the previously held notion that Internal Audit should be concerned only with retrospective audits of financial and accounting data. Instead, Internal Audit’s responsibilities include internal controls over strategy and operating effectiveness and regulatory compliance, as well as reliability of financial reporting (COSO 1992). For more information on COSO IC and its relation to SOX see Section D, Chapter 14.1.2.

**COSO ERM**

More recently, in 2003, COSO released a framework for enterprise risk management (ERM) that encompasses and enhances COSO IC. COSO defines ERM as:

*A process, effected by an entity’s Board of Directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risks to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives (COSO 2003).*

An ongoing ERM approach helps management effectively deal with uncertainty and associated risk and opportunity throughout the organization, and therefore helps the organization achieve its objectives. The COSO ERM model is illustrated using a cube, which shows how the objectives, internal control components and organization levels are interrelated.

**COSO ERM Cube**

COSO ERM expands upon the objectives set forth in the IC framework and provides four categories for an organization’s objectives:

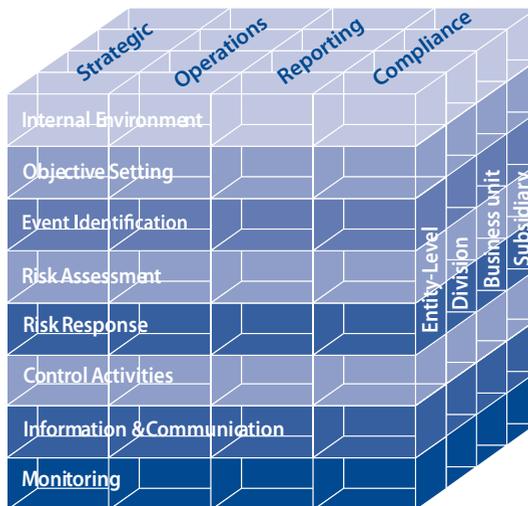
- strategic,
- operations,

- reporting, and
- compliance.

Further, COSO ERM describes eight interrelated components that are integrated within the management process:

- internal environment,
- objective setting,
- event identification,
- risk assessment,
- risk response,
- control activities,
- information and communication, and
- monitoring.

COSO ERM clearly affects the entire organization at all levels: the entity as a whole, each division, all business units, and any subsidiaries (COSO 2004).



**Fig. 1** COSO Cube (ERM)

Adapted from SOX-Online, [http://www.sox-online.com/coso\\_cobit\\_coso\\_cube-new.html](http://www.sox-online.com/coso_cobit_coso_cube-new.html)

Copyright © 2001 by the Committee of Sponsoring Organizations for the Treadway Commission

**COBIT®**

The COBIT® (Control Objectives for Information and related Technology) framework is particularly useful in an organization with a strong information technology environment. The COBIT® framework was issued and is maintained by the Information Systems Audit and Control Association (ISACA). COBIT® supplements

COSO and SOX by focusing on the governance of IT resources and processes. It is especially helpful because it provides a framework and supporting tool set that bridges control requirements, technical issues and business risks (for more information on COBIT® see Section A, Chapter 6.2.5).

The German Act on Control and Transparency in Business (*Gesetz zur Kontrolle und Transparenz im Unternehmensbereich – KonTraG*) was introduced in 1998 with the aim of eliminating potential weaknesses in the internal control systems in German public companies, including in the internal and external audit functions. This was achieved primarily by redefining the roles of Executive Board and Supervisory Board (which function in lieu of the Board of Directors in German corporations), as well as the role of the external auditors. The key stipulation requires the Executive Board to ensure that an adequate risk management system and an adequate internal audit function are in place. This law marks the first time that the internal audit function has been codified in German law, thus recognizing its place as an integral part of the financial reporting system.

**KonTraG (Germany)**

The German Corporate Governance Code (DCGK), which was established in 2005, does not refer to the internal audit function directly, but it does oblige the Supervisory Board of a company to set up an Audit Committee. This Committee is tasked primarily with issues of accounting and risk management including the budgeting and monitoring of the external auditors. The chairman of the Audit Committee “shall have specialist knowledge and experience in the application of accounting principles and internal control processes” (Government Commission German Corporate Governance Code 2006). This establishes the basis for cooperation between the Audit Committee and Internal Audit.

**German Corporate Governance Code (DCGK)**

As a result of the German Transparency and Disclosure Act (2002) the Standards of the German Corporate Governance Code have been incorporated into law. Thus Executive Boards of listed companies must confirm annually whether the company complies with the recommendations of the Commission of the German Corporate Governance Code and state which recommendations have not been implemented.

**German Transparency and Disclosure Act (TransPuG)**

The German Accounting Legislation Reform Act of 2004 (*BilReG – Bilanzrechtsreformgesetz*) has made a significant contribution to strengthening the independence of the external auditors. Specifically, sections 319 and 319a of the *Handelsgesetzbuch* (HGB - German Commercial Code) list a number of advisory services that the external auditors are not allowed to perform for a company if they audit the company. This concept can also be applied to Internal Audit. Here, too, the consulting function has gained importance in recent years and now forms an important part of Internal Audit’s responsibilities. On the other hand, however, all internal audit work also must comply with the postulate of independence. If a close relationship between auditing and consulting is regarded as inappropriate for external auditors and is not permitted for this reason, it must be assumed that such a relationship could also damage Internal Audit’s effectiveness if auditor independence is not guaranteed and conflicts of interest arise.

**German Accounting Legislation Reform Act (BilReG)**

## **The Turnbull Report (UK)**

In the United Kingdom the Turnbull Report (Internal Control Requirements of the Combined Code) requires that the Board of Directors “maintain a sound system of internal control to safeguard shareholders’ investment and the company’s assets.” Annually, directors must conduct a review of the effectiveness of the internal control system, including all controls (financial, operational and compliance) and risk management, and must report this evaluation to shareholders. Further, companies without internal audit functions must periodically assess their need for such a function. In general, the Combined Code requires that listed companies disclose how they apply the principles in the code (including those related to internal controls) and confirm that they comply with the code or – where they do not comply – issue an explanation for that deviation. The Combined Code on Corporate Governance was originally issued in June of 1998 and revised in 2005 (Institute of Chartered Accountants in England and Wales 2005).

## **Rules of the Canadian Securities Administration**

In 2004, the Canadian Securities Administrators developed rules to improve investor confidence. The rules require the development of an independent Audit Committee, that has a written charter and communicates directly with the internal audit function (Canadian Securities Administrators 2004).

## **Financial Instruments and Exchange Law (Japan)**

In Japan, the Financial Instruments and Exchange Law, legislation similar to the U.S. Sarbanes Oxley Act, was developed in 2006. This law, nicknamed J-Sox, is effective for fiscal years beginning on or after April 2008. Standards developed by the Business Accounting Council of the Financial Services Agency require all listed companies in Japan to prepare and submit internal control reports based on management’s evaluation of internal controls over financial reporting. J-Sox has a broader definition of financial reporting than US SOX, which includes other items disclosed in Securities Reports that use financial statement data. Further, company management must evaluate controls at any affiliates that are consolidated under the equity-method of accounting. Internal controls are to be evaluated using a formal control framework such as the J-Sox framework, which is based upon the COSO IC framework. Finally, the auditor must report on management’s evaluation of internal controls.

## **Code of Corporate Governance for Listed Companies in China**

The Code of Corporate Governance for Listed Companies in China was developed by the China Securities Regulatory Commission in 2001. The code requires that one third of the members of the Board of Directors be independent and suggests the (optional) appointment of an Audit Committee. The majority of the Audit Committee members must be independent and one member must be a financial expert. The principal responsibilities of the Audit Committee include overseeing the internal audit function (Chinese Securities Regulatory Commission 2001).

## **Rules Governing the Hong Kong Stock Exchanges**

The Rules Governing the Listing of Securities on the Stock Exchange of Hong Kong Limited and the Rules Governing the Listing of Securities on the Growth Enterprise Market of the Stock Exchange of Hong Kong Limited were established to ensure investor confidence in the market. These rules require that listed companies establish an Audit Committee whose responsibilities include overseeing the financial reporting system and internal control procedures. For listed companies with an

internal audit function, the Audit Committee must review and monitor Internal Audit's effectiveness and ensure it has sufficient resources. Further, the Audit Committee must report to shareholders about its review of internal control effectiveness annually (Hong Kong Exchange 2007).

IIA Standard 1100 clearly states that the organization's internal audit function must be independent, and internal auditors should be objective in performing their work. Independence is achieved through organizational status and objectivity and is a decisive factor in ensuring that internal auditors can perform their tasks in line with requirements. The Chief Audit Executive (CAE) should report to a level within the organization that allows Internal Audit to achieve independence. Ideally, the CAE should report functionally to the Audit Committee and administratively to the CEO of the organization. Further, the CAE should have direct and unrestricted communication with the Board of Directors and Audit Committee. Specifically, the CAE should regularly attend Board of Directors meetings and should have the opportunity to meet privately with the Audit Committee. Independence is strengthened when the CAE is appointed and terminated by the Board of Directors, not management.

**IIA Standard 1100**

To maintain independence, the internal audit function should be managed as a separate staff department without the authority to manage or direct employees of other units. This ensures that Internal Audit does not audit any processes or scenarios that it has been involved in creating. In addition, this organizational structure also enhances the standing of Internal Audit within the organization as all employees of the company accept and respect this department and the work it does. As an independent department, Internal Audit can evaluate operations and provide recommendations for improvement, but cannot implement them. Implementing Internal Audit's recommendations, as well as designing and implementing control solutions, is the responsibility of management.

**Staff Department**

Internal Audit must decide whether to establish a centralized or a decentralized internal audit function. This decision depends on the specific needs of the organization. Centralized internal audit services are managed and controlled by one Internal Audit management team with one audit plan for the entire function. The audit activities, tools and reporting methods are standardized for the entire function. A decentralized internal audit function may be organized into multiple divisions, each of which has the authority to develop individual audit plans, design differing audit techniques and division-specific reporting procedures. Alternatively, some organizations may use a hybrid internal audit department with characteristics of both centralized and decentralized internal audit functions. SAP's internal audit department for example is a centrally organized staff department with a decentralized, regional structure, i.e. with teams in Germany, the United States, Singapore, and Japan (see Section A, Chapter 4).

**Centralization vs.  
Decentralization of  
Internal Audit Services**

## HINTS AND TIPS



- Before beginning internal audit activities, the auditors should be aware of any laws, regulations or applicable standards that relate to the specific audit objectives. For global organizations, this may include international guidance.

## LINKS AND REFERENCES



- *Aktiengesetz (AktG) vom 6. September 1965 zuletzt geändert durch Artikel 13 des Gesetzes vom 5. Januar 2007*. <http://bundesrecht.juris.de/bundesrecht/aktg/gesamt.pdf> (accessed May 31, 2007).
- BUSINESS ACCOUNTING COUNCIL. 2007. *Standard for Implementation of Evaluation and Audit for Internal Control over Financial Reporting*. <http://www.fsa.go.jp/en/news/2007/20070420.pdf> (accessed May 31, 2007).
- CANADIAN SECURITIES ADMINISTRATORS. March 29, 2004. *New Rules Promote Investor Confidence, Change Issuers' Disclosure and Governance practices*. Press Release.
- CHINESE SECURITIES REGULATORY COMMISSION. 2001. *Code of Corporate Governance for Listed Companies in China*. [http://www.ecgi.org/codes/documents/code\\_en.pdf](http://www.ecgi.org/codes/documents/code_en.pdf) (accessed May 31, 2007).
- COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION (COSO). 1992. *Internal Control Integrated Framework*. New York, NY: AICPA.
- COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION (COSO). 2004. *Enterprise Risk Management Integrated Framework*. New York, NY: AICPA.
- FINANCIAL SERVICES AGENCY. 2006. *New Legislative Framework for Investor Protection: Financial Instruments and Exchange Law*. <http://www.fsa.go.jp/en/policy/fiel/20060621.pdf> (accessed May 31, 2007).
- Gesetz zur Einführung internationaler Rechnungslegungsstandards und zur Sicherung der Qualität der Abschlussprüfung (Bilanzrechtsreformgesetz – BilReG) vom 4. Dezember 2004. *Bundesgesetzblatt I* 65 (9.12.2004): 3166–3182. <http://www.bmj.bund.de/media/archive/834.pdf> (accessed May 31, 2007).
- Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) vom 27. April 1998. *Bundesgesetzblatt I* 24 (30.04.1998): 786–794. <http://217.160.60.235/BGBL/bgb1f/b198024f.pdf> (accessed May 31, 2007).
- Gesetz zur weiteren Reform des Aktien- und Bilanzrechts, zur Transparenz und Publizität (Transparenz- und Publizitätsgesetz) vom 19. Juli 2002. *Bundesgesetzblatt I* 50 (25.07.2002): 2681–2687. <http://217.160.60.235/BGBL/bgb1f/bgb102s2681.pdf> (accessed May 31, 2007).
- GOVERNMENT COMMISSION GERMAN CORPORATE GOVERNANCE CODE. 2006. *German Corporate Governance Code as amended on June 12, 2006 (convenience translation)*. [http://www.corporate-governance-code.de/eng/download/E\\_CorGov\\_Endfassung\\_June\\_2006.pdf](http://www.corporate-governance-code.de/eng/download/E_CorGov_Endfassung_June_2006.pdf) (accessed May 31, 2007).

- HONG KONG EXCHANGE. 2007. *Rules Governing the Listing of Securities on the Growth Enterprise Market of the Stock Exchange of Hong Kong Limited*. [http://www.hkex.com.hk/rule/gemrule/GEM-App15%20\(E\).pdf](http://www.hkex.com.hk/rule/gemrule/GEM-App15%20(E).pdf) (accessed May 31, 2007).
- INSTITUTE OF CHARTERED ACCOUNTANTS IN ENGLAND AND WALES. 2005. *Turnbull Report – Internal Control Guidance for Directors on the Combined Code*. London: The Institute of Chartered Accountants in England and Wales.
- INSTITUTE OF INTERNAL AUDITORS. 2007. *International Standards for the Professional Practice of Internal Auditing*. <http://www.theiia.org/guidance/standards-and-practices/professional-practices-framework/standards/standards-for-the-professional-practice-of-internal-auditing> (accessed May 31, 2007).
- INSTITUTE OF INTERNAL AUDITORS. 2002. *Practice Advisory 1100-1: Independence and Objectivity*. Altamonte Springs, FL: The Institute of Internal Auditors.
- NEW YORK STOCK EXCHANGE. 2003. *Final NYSE Corporate Governance Rules*. <http://www.nyse.com/pdfs/finalcorpgovrules.pdf> (accessed May 31, 2007).
- PROTIVITI. 2007. *J-SOX Flash Report – Japanese Guidelines for Internal Control Reporting Finalized – Differences in Requirements Between the U.S. Sarbanes-Oxley Act and J-SOX*. [http://www.protiviti.jp/downloads/flashreport/JSOX\\_Flash\\_Report0221E.pdf](http://www.protiviti.jp/downloads/flashreport/JSOX_Flash_Report0221E.pdf) (accessed May 31, 2007).
- PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD (PCAOB). 2004. *Auditing Standard No. 2: An Audit of Internal Control Over Financial Reporting Performed in Conjunction With an Audit of Financial Statements*. [http://www.pcaobus.org/Standards/Standards\\_and\\_Related\\_Rules/Auditing\\_Standard\\_No.2.aspx](http://www.pcaobus.org/Standards/Standards_and_Related_Rules/Auditing_Standard_No.2.aspx) (accessed May 31, 2007).
- PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD (PCAOB). 2005. *Staff Questions and Answers: Auditing Internal Control over Financial Reporting*. [http://www.pcaob.org/standards/staff\\_questions\\_and\\_answers/2005/01-21.pdf](http://www.pcaob.org/standards/staff_questions_and_answers/2005/01-21.pdf) (accessed May 31, 2007).
- REDDING, K., P. SOBEL, U. ANDERSON, M. HEAD, S. RAMAMOORTI, AND M. SALAMASIK. 2007. *Internal Assurance and Consulting Services*. Altamonte Springs, FL: The Institute of Internal Auditors.
- RITTENBERG, L. E. AND B. J. SCHWEIGER. 2005. *Auditing: Concepts for a changing environment*. 5<sup>th</sup> ed. Boston, MA: Thompson.
- SAWYER, L., M. DITTENHOFER, AND J. SCHEINER. 2003. *Sawyer's Internal Auditing*. 5<sup>th</sup> ed. Altamonte Springs, FL: The Institute of Internal Auditors.
- SEARS, B. 2002. *Internal Auditing Manual*. New York, NY: Warren, Gorham & Lamont.
- US CONGRESS. 2002. *Sarbanes-Oxley Act of 2002. 107<sup>th</sup> Congress of the United States of America. HR 3763*. Washington DC: Government Printing Office.



<http://www.springer.com/978-3-540-70886-5>

Internal Audit Handbook

Management with the SAP®-Audit Roadmap

Kagermann, H.; Kinney, W.; Küting, K.; Weber, C.-P.

(Eds.)

2008, XXVIII, 610 p., Hardcover

ISBN: 978-3-540-70886-5