9. Internal control

Internal control, as defined in accounting and auditing, is a process for assuring achievement of an organization's objectives in operational effectiveness and efficiency, reliable financial reporting, and compliance with laws, regulations and policies. A broad concept, internal control involves everything that controls risks to an organization.

It is a means by which an organization's resources are directed, monitored, and measured. It plays an important role in detecting and preventing fraud and protecting the organization's resources, both physical (e.g., machinery and property) and intangible (e.g., reputation or intellectual property such as trademarks).

At the organizational level, internal control objectives relate to the reliability of financial reporting, timely feedback on the achievement of operational or strategic goals, and compliance with laws and regulations. At the specific transaction level, internal control refers to the actions taken to achieve a specific objective (e.g., how to ensure the organization's payments to third parties are for valid services rendered.) Internal control procedures reduce process variation, leading to more predictable outcomes. Internal control is a key element of the Foreign Corrupt Practices Act (FCPA) of 1977 and the Sarbanes–Oxley Act of 2002, which required improvements in internal control in United States public corporations. Internal controls within business entities are also referred to as operational controls.

9.1 Early history of internal control

Internal controls have existed from ancient times. In Hellenistic Egypt there was a dual administration, with one set of bureaucrats charged with collecting taxes and another with supervising them. In the Republic of China, the Control Yuan (監察院; pinyin: Jiānchá Yùan), one of the five branches of government, is an investigatory agency that monitors the other branches of government.

9.2 Definitions

There are many definitions of internal control, as it affects the various constituencies (stakeholders) of an organization in various ways and at different levels of aggregation.

Under the COSO Internal Control-Integrated Framework, a widely used framework in not only the United States but around the world, internal control is broadly defined 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 relating to operations, reporting, and compliance..

COSO defines internal control as having five components:

Control Environment-sets the tone for the organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control.

Risk Assessment-the identification and analysis of relevant risks to the achievement of objectives, forming a basis for how the risks should be managed

Information and Communication-systems or processes that support the identification, capture, and exchange of information in a form and time frame that enable people to carry out their responsibilities

Control Activities-the policies and procedures that help ensure management directives are carried out.

Monitoring-processes used to assess the quality of internal control performance over time.

The COSO definition relates to the aggregate control system of the organization, which is composed of many individual control procedures.

Discrete control procedures, or controls are defined by the SEC as: "...a specific set of policies, procedures, and activities designed to meet an objective. A control may exist within a designated function or activity in a process. A control's impact...may be entity-wide or specific to an account balance, class of transactions or application. Controls have unique characteristics – for example, they can be: automated or manual; reconciliations; segregation of duties; review and approval authorizations; safeguarding and accountability of assets; preventing or detecting error or fraud. Controls within a process may consist of financial reporting controls and operational controls (that is, those designed to achieve operational objectives)."

9.3 Context

More generally, setting objectives, budgets, plans and other expectations establish criteria for control. Control itself exists to keep performance or a state of affairs within what is expected, allowed or accepted. Control built within a process is internal in nature. It takes place with a combination of interrelated components – such as social environment effecting behavior of employees, information necessary

in control, and policies and procedures. Internal control structure is a plan determining how internal control consists of these elements.

The concepts of corporate governance also heavily rely on the necessity of internal controls. Internal controls help ensure that processes operate as designed and that risk responses (risk treatments) in risk management are carried out (COSO II). In addition, there needs to be in place circumstances ensuring that the aforementioned procedures will be performed as intended: right attitudes, integrity and competence, and monitoring by managers.

9.4 Roles and responsibilities in internal control

According to the COSO Framework, everyone in an organization has responsibility for internal control to some extent. Virtually all employees produce information used in the internal control system or take other actions needed to affect control. Also, all personnel should be responsible for communicating upward problems in operations, noncompliance with the code of conduct, or other policy violations or illegal actions. Each major entity in corporate governance has a particular role to play:

9.4.1 Management

The Chief Executive Officer (the top manager) of the organization has overall responsibility for designing and implementing effective internal control. More than any other individual, the chief executive sets the "tone at the top" that affects integrity and ethics and other factors of a positive control environment. In a large company, the chief executive fulfills this duty by providing leadership and direction to senior managers and reviewing the way they're controlling the business. Senior managers, in turn, assign responsibility for establishment of more specific internal control policies and procedures to personnel responsible for the unit's functions. In a smaller entity, the influence of the chief executive, often an owner-manager, is usually more direct. In any event, in a cascading responsibility, a manager is effectively a chief executive of his or her sphere of responsibility. Of particular significance are financial officers and their staffs, whose control activities cut across, as well as up and down, the operating and other units of an enterprise.

9.4.2 Board of directors

Management is accountable to the board of directors, which provides governance, guidance and oversight. Effective board members are objective, capable and inquisitive. They also have a knowledge of the entity's activities and environment, and commit the time necessary to fulfil their board responsibilities. Management

may be in a position to override controls and ignore or stifle communications from subordinates, enabling a dishonest management which intentionally misrepresents results to cover its tracks. A strong, active board, particularly when coupled with effective upward communications channels and capable financial, legal and internal audit functions, is often best able to identify and correct such a problem.

9.4.3 Auditors

The internal auditors and external auditors of the organization also measure the effectiveness of internal control through their efforts. They assess whether the controls are properly designed, implemented and working effectively, and make recommendations on how to improve internal control. They may also review Information technology controls, which relate to the IT systems of the organization. There are laws and regulations on internal control related to financial reporting in a number of jurisdictions. In the U.S. these regulations are specifically established by Sections 404 and 302 of the Sarbanes-Oxley Act. Guidance on auditing these controls is specified in PCAOB Auditing Standard No. 5 and SEC guidance, further discussed in SOX 404 top-down risk assessment. To provide reasonable assurance that internal controls involved in the financial reporting process are effective, they are tested by the external auditor (the organization's public accountants), who are required to opine on the internal controls of the company and the reliability of its financial reporting.

9.4.4 Audit committee

The role and the responsibilities of the audit committee, in general terms, are to: (a) Discuss with management, internal and external auditors and major stakeholders the quality and adequacy of the organization’s internal controls system and risk management process, and their effectiveness and outcomes, and meet regularly and privately with the Director of Internal Audit; (b) Review and discuss with management and the external auditors and approve the audited financial statements of the organization and make a recommendation regarding inclusion of those financial statements in any public filing. Also review with management and the independent auditor the effect of regulatory and accounting initiatives as well as off-balance sheet issues in the organization’s financial statements; (c) Review and discuss with management the types of information to be disclosed and the types of presentations to be made with respect to the Company's earning press release and financial information and earnings guidance provided to analysts and rating agencies; (d) Confirm the scope of audits to be performed by the external and

internal auditors, monitor progress and review results and review fees and expenses. Review significant findings or unsatisfactory internal audit reports, or audit problems or difficulties encountered by the external independent auditor. Monitor management's response to all audit findings; (e) Manage complaints concerning accounting, internal accounting controls or auditing matters; (f) Receive regular reports from the Chief Executive Officer, Chief Financial Officer and the Company's other Control Committees regarding deficiencies in the design or operation of internal controls and any fraud that involves management or other employees with a significant role in internal controls; and (g) Support management in resolving conflicts of interest. Monitor the adequacy of the organization's internal controls and ensure that all fraud cases are acted upon.

9.4.5 Personnel benefits committee

The role and the responsibilities of the personnel benefits, in general terms, are to: (a) Approve and oversee administration of the Company's Executive Compensation Program; (b) Review and approve specific compensation matters for the Chief Executive Officer, Chief Operating Officer (if applicable), Chief Financial Officer, General Counsel, Senior Human Resources Officer, Treasurer, Director, Corporate Relations and Management, and Company Directors; (c) Review, as appropriate, any changes to compensation matters for the officers listed above with the Board; and (d)Review and monitor all human-resource related performance and compliance activities and reports, including the performance management system. They also ensure that benefit-related performance measures are properly used by the management of the organization.

9.4.6 Operating staff

All staff members should be responsible for reporting problems of operations, monitoring and improving their performance, and monitoring non-compliance with the corporate policies and various professional codes, or violations of policies, standards, practices and procedures. Their particular responsibilities should be documented in their individual personnel files. In performance management activities they take part in all compliance and performance data collection and processing activities as they are part of various organizational units and may also be responsible for various compliance and operational-related activities of the organization.

Staff and junior managers may be involved in evaluating the controls within their own organisational unit using a control self-assessment.

9.5 Limitations

Internal control can provide reasonable, not absolute, assurance that the objectives of an organization will be met. The concept of reasonable assurance implies a high degree of assurance, constrained by the costs and benefits of establishing incremental control procedures.

Effective internal control implies the organization generates reliable financial reporting and substantially complies with the laws and regulations that apply to it. However, whether an organization achieves operational and strategic objectives may depend on factors outside the enterprise, such as competition or technological innovation. These factors are outside the scope of internal control; therefore, effective internal control provides only timely information or feedback on progress towards the achievement of operational and strategic objectives, but cannot guarantee their achievement.

9.6 Describing internal controls

Internal controls may be described in terms of: a) the pertinent objective or financial statement assertion; and b) the nature of the control activity itself.

9.6.1 Objective or assertions categorization

Controls may be defined against the particular financial statement assertion to which they relate. There are five such assertions:

Existence/Occurrence/Validity: Only valid or authorized transactions are processed.

Completeness: All transactions are processed that should be.

Rights and obligations: Assets are the rights of the organization and the liabilities are its obligations as of a given date.

Valuation: Transactions are valued accurately using the proper methodology, such as a specified means of computation or formula.

Presentation and disclosure: Accounts and disclosures are properly described in the financial statements of the organization.

For example, a validity control objective might be: "Payments are made only for authorized products and services received." A typical control procedure would be:

"The payable system compares the purchase order, receiving record, and vendor invoice prior to authorizing payment." Management is responsible for implementing appropriate controls that apply to all transactions in their areas of responsibility.

9.6.2 Activity categorization

Control activities may also be explained by the type or nature of activity. These include (but are not limited to):

Segregation of duties – separating authorization, custody, and record keeping roles to prevent fraud or error by one person.

Authorization of transactions – review of particular transactions by an appropriate person.

Retention of records – maintaining documentation to substantiate transactions.

Supervision or monitoring of operations – observation or review of ongoing operational activity.

Physical safeguards – usage of cameras, locks, physical barriers, etc. to protect property, such as merchandise inventory.

Top-level reviews-analysis of actual results versus organizational goals or plans, periodic and regular operational reviews, metrics, and other key performance indicators (KPIs).

IT general controls – Controls related to: a) Security, to ensure access to systems and data is restricted to authorized personnel, such as usage of passwords and review of access logs; and b) Change management, to ensure program code is properly controlled, such as separation of production and test environments, system and user testing of changes prior to acceptance, and controls over migration of code into production.

IT application controls – Controls over information processing enforced by IT applications, such as edit checks to validate data entry, accounting for transactions in numerical sequences, and comparing file totals with control accounts.

9.6.3 Control precision

Control precision describes the alignment or correlation between a particular control procedure and a given control objective or risk. A control with direct impact on the achievement of an objective (or mitigation of a risk) is said to be more precise than

one with indirect impact on the objective or risk. Precision is distinct from sufficiency; that is, multiple controls with varying degrees of precision may be involved in achieving a control objective or mitigating a risk.

Precision is an important factor in performing a SOX 404 top-down risk assessment. After identifying specific financial reporting material misstatement risks, management and the external auditors are required to identify and test controls that mitigate the risks. This involves making judgments regarding both precision and sufficiency of controls required to mitigate the risks.

Risks and controls may be entity-level or assertion-level under the PCAOB guidance. Entity-level controls are identified to address entity-level risks. However, a combination of entity-level and assertion-level controls are typically identified to address assertion-level risks. The PCAOB set forth a three-level hierarchy for considering the precision of entity-level controls.[5] Later guidance by the PCAOB regarding small public firms provided several factors to consider in assessing precision.

9.7 Fraud and internal control

Internal control plays an important role in the prevention and detection of fraud. Under the Sarbanes-Oxley Act, companies are required to perform a fraud risk assessment and assess related controls. This typically involves identifying scenarios in which theft or loss could occur and determining if existing control procedures effectively manage the risk to an acceptable level. The risk that senior management might override important financial controls to manipulate financial reporting is also a key area of focus in fraud risk assessment.

The AICPA, IIA, and ACFE also sponsored a guide published during 2008 that includes a framework for helping organizations manage their fraud risk.

9.8 Internal controls and process improvement

Controls can be evaluated and improved to make a business operation run more effectively and efficiently. For example, automating controls that are manual in nature can save costs and improve transaction processing. If the internal control system is thought of by executives as only a means of preventing fraud and complying with laws and regulations, an important opportunity may be missed. Internal controls can also be used to systematically improve businesses, particularly in regard to effectiveness and efficiency.

9.9 Continuous controls monitoring

Advances in technology and data analysis have led to the development of numerous tools which can automatically evaluate the effectiveness of internal controls. Used in conjunction with continuous auditing, continuous controls monitoring provides assurance on financial information flowing through the business processes.