Principles of Auditing: An Introduction to International Standards on Auditing

Chapter 7 – Internal Control and Control Risk

Rick Hayes, Hans Gortemaker and Philip Wallage

COSO says internal control is

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 categories: effectiveness and efficiency of operations, reliability of financial reporting, compliance with applicable laws and regulations and safeguarding of assets against unauthorised acquisition, use or disposition.

International Federation of Accountants Internal control definition

Internal control – The process designed, implemented and maintained by those charged with governance, management and other personnel to provide reasonable assurance about the achievement of an entity's objectives with regard to reliability of financial reporting, effectiveness and efficiency of operations and compliance with applicable laws and regulations.

Internal control is geared to the *achievement of objectives* in one or more separate overlapping categories:

1. *Effective operations* – relating to effective and efficient use of the entity's resources.
2. *Financial reporting* – relating to preparation of reliable published financial statements.
3. *Compliance* – relating to the entity's compliance with applicable laws and regulations.
4. *Safeguarding of assets.*

Management control objectives

- Effective operations: Goal safeguarding of assets (cash, accounts receivable, accounting records).
- Financial reporting: Need for accurate information because management has a responsibility to see that statements are prepared fairly in accordance with accounting standards. Auditor is interested primarily in financial reporting controls (especially controls over transactions).
- Compliance: Companies must comply with many laws and regulations including company law, tax law and environmental protection regulations.

Which of the three categories of management control objectives is the most important to:

- The external auditors?
- Management?
- Government auditors?
- Internal auditors?
- The shareholders?
- Employees?

US Securities Exchange Commission rules require that management must base its evaluation of the effectiveness of the company's internal control over financial reporting on a suitable, recognised control framework established by a body or group that followed due-process procedures, including the broad distribution of the framework for public comment. Two frameworks:

- The report of the Committee of Sponsoring Organizations of the Treadway Commission (known as the COSO report).
- The Financial Reporting Council, Internal Control Revised Guidance for Directors on the Combined Code, October 2005 (known as the Turnbull Report).

Auditor's primary control consideration and emphasis

- To understand an entity's internal control, the auditor will evaluate the design and implementation of a control.
- The auditor's primary consideration is whether, and how, a specific control prevents, or detects and corrects, *material misstatements* in *classes of transactions,* account balances or disclosures.
- The heaviest emphasis by auditors is on controls over classes of transactions rather than account balances or disclosures.

Design and implementation of controls

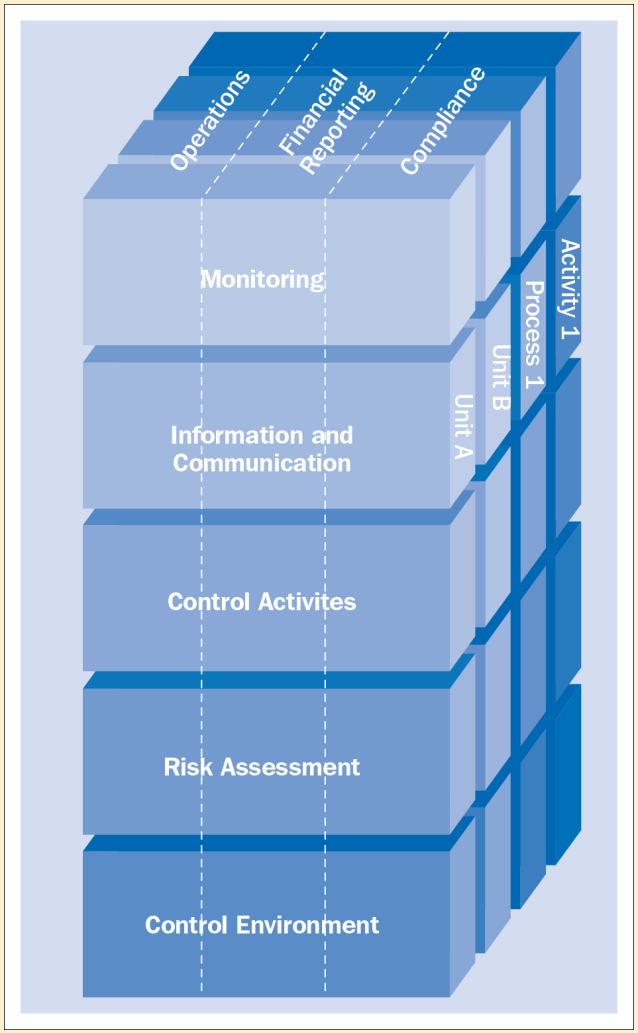

Illustration 7.1 Components of Internal Control – COSO Report

Design and implementation of controls (Continued)

- To understand the entity's internal control the auditor will evaluate the design of a control and judge whether it has been implemented.
- He determines if the control is designed to prevent, detect or correct transactions that misstate the account balances.
- Implementation of a control means that the control exists and that the entity is using it.

Why do you think internal controls are important to a business?

Importance of internal control

- Management identifies the risk of not achieving their objectives.
- To minimise these risks, management designs and puts in place a set of rules, physical constraints and activities called ‘internal controls’ which, if they are implemented properly, will minimise the risks of not meeting objectives.

Information technology controls – General

General IT controls are policies and procedures that relate to many applications and support the effective functioning of application controls by helping to ensure the continued proper operation of information systems. For example:

- controls over data centre and network operations; system software acquisition, change and maintenance; access security; back-up and recovery; and application system acquisition, development and maintenance.

IT controls – Application controls

Application controls are controls that apply to applications that initiate, record, process and report transactions (such as MS Office, SAP, QuickBooks), rather than the computer system in general. Examples are chart of accounts, edit checks of input data, numerical sequence checks and manual follow-up of exception reports.

Chart of Accounts

Assets	Liabilities	Stockholders' Equity	Revenues	Expenses
Cash	**Notes payable**	**Common Stock**	**Service Revenue**	**Salaries Expense**
Accounts Receivable	**Accounts Payable**	**Retained Earnings**		Supplies Expense
Advertising Supplies	Interest Payable	**Dividends**		**Rent Expense**
Prepaid Insurance	**Unearned Service Revenue**	Income Summary		Insurance Expense
Office Equipment	Salaries Payable			Interest Expense
Accumulated Depreciation – Office Equipment				Depreciation Expense

IT risks

- Reliance on systems or programs that are inaccurately processing data, processing inaccurate data or both.
- Unauthorised access to data that may result in destruction of data or improper changes to data.
- The possibility of IT personnel gaining access privileges beyond those necessary to perform their assigned duties thereby breaking down segregation of duties.
- Unauthorised changes to data in master files.

IT risks (Continued)

- Unauthorised changes to systems or programs.
- Failure to make necessary changes to systems or programs.
- Input by people or systems without authorised access.
- Potential loss of data or inability to access data as required.
- Management's failure to commit sufficient resources to address IT security risks may adversely affect internal control by allowing improper changes to be made to computer programs or to data, or unauthorised transactions to be processed.
- Inconsistencies between the entity's IT strategy and its business strategies.
- Changes in the IT environment.

Components of COSO internal control are

- Control environment
- Risk assessment
- Information and communication
- Control activities/control procedures
- Monitoring.

Components of internal control

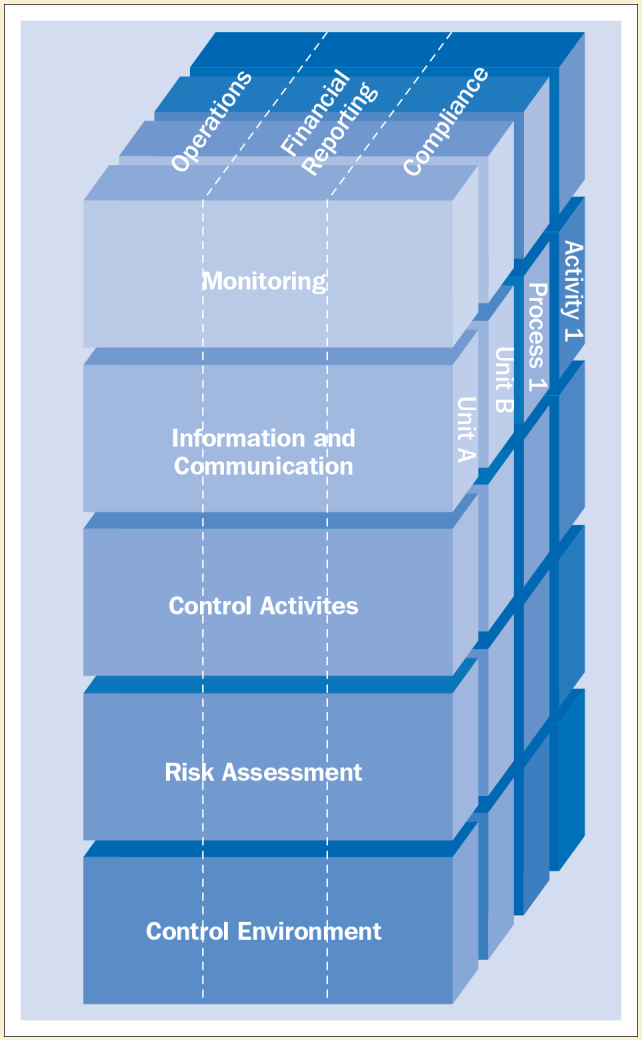

Illustration 7.1 Components of Internal Control – COSO Report

Control environment

Control environment – includes the governance and management functions and the attitudes, awareness and actions of those charged with governance and management concerning the entity's internal control and its importance in the entity.

Cumulative effect of controls

When analysing the control environment, the auditor must think about the collective effect of various control environment elements. Strengths in one of the elements might mitigate weaknesses in another element.

For example, an active and independent board of directors may influence the philosophy and operating style of senior management. Alternatively, human resource policies directed towards hiring competent accounting personnel might not mitigate a strong bias by top management to overstate earnings.

Factors on which to assess internal control

Integrity and Ethical Values
(Communication and enforcement of integrity and ethical values)

- Existence and implementation of codes of conduct and other policies regarding acceptable business practice, conflicts of interest, or expected standards of ethical and moral behaviour.
- Dealings with employees, suppliers, customers, investors, creditors, insurers, competitors and auditors, etc. (e.g. whether management conducts business on a high ethical plane, and insists that others do so, or pays little attention to ethical issues).
- Pressure to meet unrealistic performance targets – particularly for short-term results – and extent to which compensation is based on achieving those performance targets.

Commitment to Competence

- Formal or informal job descriptions or other means of defining tasks that comprise particular jobs.
- Analysis of the knowledge and skills needed to perform jobs adequately.

Board of Directors or Audit Committee
(Participation by those charged with governance)

- An entity's control consciousness is influenced significantly by those charged with governance. Independence from management.
- Frequency and timeliness with which meetings are held with chief financial and/or accounting officers, internal auditors and external auditors.
- Sufficiency and timeliness with which information is provided to board or committee members, to allow monitoring of management's objectives and strategies, the entity's financial position and operating results, and terms of significant agreements.
- Sufficiency and timeliness with which the board or audit committee is apprised of sensitive information, investigation and improper acts (e.g. travel expenses of senior officers, significant litigation, investigations of regulatory agencies, defalcations, embezzlement or misuse of corporate assets, violations of insider trading rules, political payments, illegal payments).
- Oversight of the design and effective operation of whistle blower procedures and the process for reviewing the effectiveness of the entity's internal control.

Illustration 7.4 Factors on Which to Assess Internal Control Environment

Factors on which to assess internal control

Management's Philosophy and Operating Style

- Nature of business risks accepted, for example, whether management often enters into particularly high-risk ventures, or is extremely conservative in accepting risks.
- Frequency of interaction between senior management and operating management, particularly when operating from geographically removed locations.
- Attitudes and actions towards financial reporting, including disputes over application of accounting treatments (e.g. selection of conservative versus liberal accounting policies, whether accounting principles have been misapplied, important financial information not disclosed, or records manipulated or falsified).

Organisational Structure

- Appropriateness of the entity's organisational structure and its ability to provide the necessary information flow to manage its activities.
- Adequacy of definition of key managers' responsibilities and their understanding of these responsibilities.

Illustration 7.4 Factors on Which to Assess Internal Control Environment (Continued)

Factors on which to assess internal control (Continued)

Assignment of Authority and Responsibility

- Assignment of responsibility and delegation of authority to deal with organisational goals and objectives, operating functions and regulatory requirements, including responsibility for information systems and authorisations for changes.
- Appropriateness of control-related standards and procedures, including employee job descriptions.
- Appropriate numbers of people, particularly with respect to data processing and accounting functions, with the requisite skill levels related to the size of the entity and nature and complexity of activities and systems.

Human Resource Policies and Practices

- Extent to which policies and procedures for hiring, training, promoting, and compensating employees are in place.
- Appropriateness of remedial action taken in response to departures from approved policies and procedures.
- Adequacy of employee candidate background checks, particularly with regard to prior actions and activities considered to be unacceptable by the entity.
- Adequacy of employee retention and promotion criteria and information-gathering techniques (e.g. performance evaluations) and relation to the code of conduct or other behavioural guidelines.

Illustration 7.4 Factors on Which to Assess Internal Control Environment (Continued)

Elements contributing to a successful control environment

- Communication and enforcement of integrity and ethical values
- Commitment to competence
- Participation by those charged with governance – independence and integrity of the board of directors
- Management's philosophy and operating style – leadership via control by example
- Organisational structure
- Assignment of authority and responsibility
- Human resource policies and practices.

Integrity and ethical values and commitment to competence

- The integrity and ethical values of the people who create, administer and monitor controls determines their effectiveness.
- Management might remove incentives and temptations that prompt personnel to engage in fraudulent or unethical behaviour.
- A company's control environment will be more effective if its culture is one in which quality and competence are openly valued.

Participation of those charged with governance

- The guidance and oversight responsibilities of an active and involved board of directors who possess an appropriate degree of management, technical and other expertise is critical to effective internal control.
- Because the board must be prepared to question and scrutinise management's activities, present alternative views and have the courage to act in the face of obvious wrongdoing, it is necessary that the board contain at least a critical mass of independent (non-executive) directors.

Management's philosophy and operating style and organisational structure

- Management's philosophy and operating style is their attitude about, and approach to, financial reporting, accounting issues and to taking and managing business risk. Management philosophy may create significant risk.
- Important organisational considerations are clarity of lines of authority and responsibility; the level at which policies are established; adherence to these policies; adequacy of supervision; and appropriateness of organisational structure for the entity.

Assignment of authority and responsibility; Human resource policies and practices

- Responsibility and delegation of authority should be clearly assigned. How responsibility is distributed is usually spelled out in formal company policy manuals.
- With trustworthy and competent employees, weaknesses in other controls can be compensated and reliable financial statements might still result. Honest, efficient people are able to perform at a high level even when there are few other controls to support them.

Risk assessment

Managements risk assessment differs from, but is closely related to, the auditor's risk assessment.

- Management assesses risks as part of designing and operating the internal control system to minimise errors and irregularities.
- Auditors assess risks to decide the evidence needed in the audit.

If management effectively assesses and responds to risks, the auditor will typically need to accumulate less audit evidence than when management fails to, because control risk is lower.

Identify risks

A technique to **identify risks** involves identifying and prioritising high risk activities:

1. Identify the essential resources of the business and determine which are most at risk.
2. Identify possible liabilities which may arise.
3. Review the risks that have arisen in the past.
4. Consider any additional risks imposed by new objectives or new external factors.
5. Seek to anticipate change by considering problems and opportunities on a continuing basis.

Information systems, communication and related business processes

Every enterprise must capture pertinent information related to both internal and external events and activities in both financial and non-financial forms. The information must be identified by management as relevant and then communicated to people who need it in a form and time frame that allows them to do their jobs.

Communication

- Not just a matter of reporting, communication occurs in a broader sense, flowing down, across and up the organisation. All personnel must receive a clear message from top management that control responsibilities must be taken seriously.
- Employees must understand their own role in the internal control system, as well as how individual activities relate to the work of others, and how to report significant information to senior management.

Sub-systems (contents) of an information system

- Accounting system
- Production system
- Personnel system
- Systems software
- Applications for word-processing, presentations, data bases, etc. and all records and files generated by these applications
- Information about external events, activities and conditions.

Two elements of control procedures

Control procedures may be divided into two elements: a **policy** establishing what should be done and **procedures to effect that policy**. Examples are:

- A policy is that a securities dealer retail branch manager must monitor (conduct performance reviews of) customer trades.
- A procedure to effect that policy world be a review of daily reports of customer trade activities with attention given to the nature and volume of securities traded.

Control activities (control procedures)

Control procedures implement the control policies by specific routine tasks, performed at particular times by designated people, held accountable by adequate supervision and evidence of performance.

- **P**erformance reviews
- **I**nformation processing: accuracy, adequate documents and records, application controls
- **P**hysical control over assets and records
- Adequate **S**egregation of duties
- **A**uthorisation of transactions and activities, general controls.

Performance reviews

Performance reviews are independent checks on performance by a third party not directly involved in the activity. These control activities include reviews and analyses of actual performance *vs.* budgets, forecasts and prior period performance; relating different sets of data – operating or financial – to one another; comparing internal data with external sources of information; and review of functional or activity performance.

Information processing adequate documents

- Well-designed documents in a manual system and *preformatted* input screens in a CIS.
- Assets are properly controlled and all transactions correctly recorded.
- Document prepared at the time a transaction takes place.
- Document simple enough to be clearly understood.
- Document designed for multiple use to minimise the number of different forms.
- Document constructed in a manner that encourages correct preparation.

Information processing: Application controls

- The chart of accounts
- Use of serial numbers on documents and input transactions
- Checks, tickets, sales invoices, purchase orders, stock certificates and many other business papers
- Systems manuals for computer accounting software should provide sufficient information to make the accounting functions clear
- Passwords that allow only authorised people admittance to the computer software online.

Physical controls

- Physical controls are procedures to ensure the physical security of assets.
- Only individuals who are properly authorised should be allowed access to the company's assets.
- Direct physical access to assets may be controlled through physical precautions.

Segregation of duties

Segregation of duties entail three fundamental functions which must be separated and adequately supervised:

- Authorisation
- Recording
- Custody

Authorisation

- Proper authorisation
  - Appropriate delegation of authority sets limits on what levels of risk are acceptable.
- General controls
  - Access to the computer system is limited to people who have a right to the information
  - Back-up and recovery procedures
  - User ID and general system access.

Monitoring of controls

- Monitoring is assessing the design of controls and their operation on a timely basis and taking necessary corrective actions.
- Ongoing monitoring information comes from several sources: exception reporting on control activities, reports by government regulators, feedback from employees, complaints from customers and most importantly from internal auditor reports.

Evaluation of monitoring

When evaluating the ongoing monitoring the following issues might be considered:

- Periodic comparisons of amounts recorded with the accounting system and with physical assets.
- Responsiveness to internal and external auditor recommendations to strengthen internal controls.
- Extent to which training seminars, planning sessions and other meetings provide information on effective operation of controls.
- Effectiveness of internal audit activities.
- Extent to which personnel obtain evidence on internal control function.

Hard and soft control

- Management designs and sets in place a set of rules, physical constraints and activities called ‘internal controls’. Due to the explicit, formal and tangible character of these controls, these controls are generally referred to as **hard controls**.
- **Soft controls** are the intangible factors in an organisation that influence the behaviour of managers and employees.
- Whereas soft controls are founded in the culture or climate of an organisation, the hard-controls are more explicit, formal and visible.

Seven factors influence the way people examine their control activities

1. Clarity for directors, managers and employees as to what constitutes desirable and undesirable behaviour.
2. Role-modelling among administrators, management or immediate supervisors.
3. Achievability of goals, tasks and responsibilities set.
4. Commitment in the organisation.
5. Transparency of behaviour.
6. Openness to discussion of viewpoints, emotions, dilemmas and transgressions.
7. Enforcement of behaviour, such as appreciation of desirable behaviour, sanctioning of undesirable behaviour.

Design and implementation of internal control

- The auditor is required to evaluate the design of a controls and determine whether they have been implemented.
- Evaluating the design of a control involves considering whether the control is capable of effectively preventing or detecting and correcting, material misstatements.

Methods for obtaining controls audit evidence

Risk assessment procedures to obtain audit evidence about the design and implementation of relevant controls may include:

a. Inquiring of entity personnel

b. Observing and re-performing the application of a specific control

c. Inspecting documents and reports

d. Tracing transactions through the information system.

Preliminary assessment of control risk

- Consider the results of previous audits that involved evaluating the operating effectiveness of internal control.
- Discuss the possibility of audit risk with audit firm personnel.
- Interview entity personnel to find evidence of management's commitment to the design, implementation and maintenance of sound internal control.
- Knowledge of the industry and the environment.

Thank you for your attention

Any Questions?