Internal Control
and the
IC System in Philippines

PA 208
Public Fiscal Administration and Budgeting

Prepared by
Johny Sauro Natad

September 2008
Introduction - Control in Organizations

♦ Controls are restraining and directive influences over the activities of a system
♦ General principles of control are applied in business organizations
♦ Accounting systems assist management in controlling operations
♦ Accounting internal controls assure that all transactions are authorized, all transactions are recorded, access to assets is allowed only for authorized purposes and accounting records describe only real assets.

Brief History of Internal Control

• First defined in 1949, by the American Institute of Accountants (now the AICPA)
• In 1958, distinguish between accounting controls and administrative controls
  o Accounting controls relate to safeguarding assets and reliability of financial records
  o Administrative controls relate to operational efficiency and adherence to managerial policies
• In 1972, clarification of controls, accounting controls provide reasonable assurance that
  o transactions executed as authorized
  o transactions recorded to permit GAAP statements and maintain accountability for assets
  o access to assets only as authorized
  o regularly compare recorded assets with actual assets
• Foreign Corrupt Practices Act: Took the language of the 1972 AICPA pronouncement and made it law. Since 1977, all publicly owned corporations legally required to:
  o keep books which accurately and fairly reflect transactions and dispositions of assets and
  o devise and maintain a system of internal accounting controls sufficient to provide reasonable assurances that transactions are authorized by management
  o transactions are recorded so GAAP statements can be prepared and maintain accountability for assets
  o access to assets is authorized by management
  o periodic inventory is required to compare recorded assets with existing assets
• Statement on Auditing Standards No. 48, effective for periods beginning after August 31, 1984.

Definitions

In accounting and organizational theory, Internal control is defined as a process effected by an organization's structure, work and authority flows, people and management information systems, designed to help the organization accomplish specific goals or objectives. It is a means by which an organization's resources are directed, monitored, and measured. It plays an important role in preventing and detecting 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.

There are a variety of 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 the United States, internal control is broadly defined as a process, affected 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:

a) Effectiveness and efficiency of operations;

b) Reliability of financial reporting; and

c) Compliance with laws and regulations.

Objectives of Internal Control

Internal controls are established to further strengthen:

♦ The reliability and integrity of information.
♦ Compliance with policies, plans, procedures, laws and regulations.
♦ The safeguarding of assets.
♦ The economical and efficient use of resources.
♦ The accomplishment of established objectives and goals for operations or programs.
**Purposes & Principles**

The purposes of internal control are to:

a) Promote orderly, economical, efficient and effective operations, and produce quality services and outcomes consistent with the agency’s mission.

b) Safeguard resources against loss due to waste, abuse, errors and fraud.

c) Promote adherence to laws, regulations, policies, procedures and contracts.

d) Develop and maintain reliable financial and management data and accurately present that data in timely reports to decision makers.

**Internal Control Myths and Facts**

**MYTHS:**

- Internal control starts with a strong set of policies and procedures.
- Internal control: That’s why we have internal auditors!
- Internal control is a finance thing.
- Internal controls are essentially negative, like a list of “thou-shalt-nots.”
- Internal controls take time away from our core activities of making products, selling, and serving customers.

**FACTS:**

- Internal control starts with a strong control environment.
- While internal auditors play a key role in the system of control, management is the primary owner of internal control.
- Internal control is integral to every aspect of the business process.
- Internal control makes the right things happen the first time.
- Internal controls should be built “into,” not “onto” business processes. They are integral!

**Source:** Institute of Internal Auditors

**Why are Internal Controls Important?**

- Compliance with applicable laws and regulations.
- Accomplishment of the entity’s mission.
- Relevant and reliable financial reporting.
- Effective and efficient operations.
- Safeguarding of assets.

- Internal control protects you by catching small mistakes before they become big problems.
- Internal control protects the organization by removing opportunities for innocent mistakes or intentional fraud.
- Effective internal controls result in improved performance, efficiency, and business process reengineering.

**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.

Internal control involves human action, which introduces the possibility of errors in processing or judgment. Internal control can also be overridden by collusion among employees or coercion by top management.

**Key concepts of the COSO framework**
The COSO framework involves several key concepts:

- **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, to an entity’s management and board.
- Internal control is geared to the achievement of objectives in one or more separate but overlapping categories.

COSO defines internal control as having five components:

1. **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.
2. **Risk Assessment**—the identification and analysis of relevant risks to the achievement of objectives, forming a basis for how the risks should be managed.
3. **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.
4. **Control Activities**—the policies and procedures that help ensure management directives are carried out.
5. **Monitoring**—processes used to assess the quality of internal control performance over time.

The **control environment** reflects the board of directors’ and management’s commitment to internal control. It provides discipline and structure to the control system. Elements of the control environment include:

1. The organizational structure of the institution. Is the bank’s organization centralized or decentralized? Are authorities and responsibilities clear? Are reporting relationships well designed?
2. Management’s philosophy and operating style. Are the bank’s business strategies formal or informal? Is its philosophy and operating style conservative or aggressive? Have its risk strategies been a successful?
3. The integrity, ethics, and competence of personnel.
4. The external influences that affect the bank’s operations and risk management practices (e.g., independent audits).
5. The attention and direction provided by the board of directors and its committees, especially the audit or risk management committees.
6. The effectiveness of human resources policies and procedures.

**Risk assessment** is the identification, measurement, and analysis of risks, internal and external, controllable and uncontrollable, at individual business levels and for the bank as a whole. Management must assess all risks facing the bank because uncontrolled risk-taking can prevent the bank from reaching its objectives or can jeopardize its operations. Effective risks assessments help determine what the risks are, what controls are needed, and how they should be managed.

**Control activities** are the policies, procedures, and practices established to help ensure that bank personnel carry out board and management directives at every business level throughout the bank. These activities help ensure that the board and management act to control risks that could prevent a bank from attaining its objectives. They should include:

1. Reviews of operating performance and exception reports. For example, senior management regularly should review reports showing financial results to date versus budget amounts, and the loan department manager should review weekly reports on delinquencies or documentation exceptions.
2. Approvals and authorization for transactions and activities. For example, an appropriate level of management should approve and authorize all transactions over a specified limit, and authorization should require dual signatures.
3. Segregation of duties to reduce a person’s opportunity to commit and conceal fraud or errors. For example, assets should not be in the custody of the person who authorizes or records transactions.
4. The requirement that officers and employees in sensitive positions be absent for two consecutive weeks each year.
5. Design and use of documents and records to help ensure that transactions and events are recorded. For example, using pre-numbered documents facilitates monitoring.
6. Safeguards for access to and use of assets and records. To safeguard data processing areas, for example, a bank should secure facilities and control access to computer programs and data files.
7. Independent checks on whether jobs are getting done and recorded amounts are accurate. Examples of independent checks include account reconciliation, computer-programmed controls, management review of reports that summarize account balances, and user review of computer generated reports. Banks are required to develop and maintain written procedures or controls for certain areas, including real estate lending, asset management, and emerging market and trading activities, as well as areas subject to insider transactions, the Bank Secrecy Act, and the Bank Bribery Statute. Although the OCC encourages banks to have written internal control procedures in all areas, having them is not enough. Personnel must understand control procedures and follow them conscientiously.

Accounting, information, and communication systems capture and impart pertinent and timely information in a form that enables the board, management, and employees to carry out their responsibilities. Accounting systems are the methods and records that identify, assemble, analyze, classify, record, and report a bank's transactions. Information and communication systems enable all personnel to understand their roles in the control system, how their roles relate to others, and their accountability. Information systems produce reports on operations, finance, and compliance that enable management and the board to run the bank. Communication systems impart information throughout the bank and to external parties such as regulators, examiners, shareholders, and customers.

Self-assessment or monitoring is the bank's own oversight of the control system's performance. Self-assessments are evaluations of departmental or operational controls by persons within the area. Ongoing monitoring should be part of the normal course of daily operations and activities. Internal and external audit functions, as part of the monitoring system, may provide independent assessments of the quality and effectiveness of a control system's design and performance. All bank personnel should share responsibility for self-assessment or monitoring; everyone should understand his or her responsibility to report any breaches of the control system. Strong control cultures typically incorporate qualified personnel, effective risk identification and analysis, clear designation and appropriate separation of responsibilities, accurate and timely information flow, and established monitoring and follow-up processes. For example, the lending area should have

1. a board of directors active in approving and monitoring loan policies and practices;
2. a loan review function that evaluates the risk and quality of loan portfolios;
3. policies and procedures governing, among other things, types of loans, loan approvals, maturity limits, rate structure, and collateral requirements; and
4. information systems that allow for proper management and monitoring of the lending area.

Redefining the control focus

The new approach to controlling business risks may be characterized by the "new rules" of "prevent and monitor" and "build in quality" as opposed to the "old rules" of "detect and correct" and "inspect in quality." This means a paradigm shift in the traditional viewpoint of control as illustrated in the following table:

<table>
<thead>
<tr>
<th>Old Paradigm</th>
<th>New Paradigm</th>
</tr>
</thead>
<tbody>
<tr>
<td>Only AUDITORS and TREASURY are concerned about risks and controls</td>
<td>EVERYONE, including operations, is concerned about managing business risks</td>
</tr>
<tr>
<td>FRAGMENTATION – Every function and department does its own thing (&quot;SILO MANAGEMENT&quot;)</td>
<td>Business risk assessment and control are FOCUSED and COORDINATED with senior level OVERSIGHT</td>
</tr>
<tr>
<td>NO BUSINESS RISK CONTROL POLICY</td>
<td>FORMAL BUSINESS RISK CONTROL POLICY approved by management and the board</td>
</tr>
<tr>
<td>INSPECT for and DETECT business risk and REACT to it</td>
<td>ANTICIPATE and PREVENT business risk at the source and MONITOR business risk controls continuously</td>
</tr>
<tr>
<td>Ineffective PEOPLE are the primary source of business risk</td>
<td>Ineffective PROCESSES are the primary source of business risk</td>
</tr>
</tbody>
</table>

Protiviti KnowledgeLeader (www.knowledgeleader.com)

Roles and responsibilities in internal control

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

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 effect 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:

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.

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 knowledge of the entity's activities and environment, and commit the time necessary to fulfill 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.

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. 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.

Describing Internal Controls
Internal controls may be described in terms of: a) the objective they pertain to; and b) the nature of the control activity itself.

A.) Objective categorization
Internal control activities are designed to provide reasonable assurance that particular objectives are achieved, or related progress understood. The specific target used to determine whether a control is operating effectively is called the control objective. Control objectives fall under several detailed categories; in financial auditing, they relate to particular financial statement assertions, but broader frameworks are helpful to also capture operational and compliance aspects:

1. Existence (Validity): Only valid or authorized transactions are processed (i.e., no invalid transactions)
2. Occurrence (Cutoff): Transactions occurred during the correct period or were processed timely.
3. Completeness: All transactions are processed that should be (i.e., no omissions)
4. Valuation: Transactions are calculated using an appropriate methodology or are computationally accurate.
5. Rights & Obligations: Assets represent the rights of the company, and liabilities its obligations, as of a given date.
6. Presentation & Disclosure (Classification): Components of financial statements (or other reporting) are properly classified (by type or account) and described.
7. Reasonableness: transactions or results appear reasonable relative to other data or trends.

For example, a control objective for an accounts payable function might be: "Payments are only made to authorized vendors for goods or services received." This is a validity objective. A typical control procedure designed to achieve this objective is: "The accounts 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 transactions in their areas of responsibility. Internal auditors perform their audits to evaluate whether the controls are designed and implemented effectively to address the relevant objectives.

B) Key Internal Control Activities
Internal Control in the Philippines

What is an Internal Control System?
Comprises the plan of organization and all the methods and measures adopted within an agency to ensure that resources are:
- used consistent with laws, regulations and policies;
- resources are safeguarded against loss, wastage and misuse;
- financial and non-financial information are reliable, accurate and timely;
- operations are economical, efficient and effective.

Importance of ICS in Government Offices
- All resources of the government shall be managed, expended or utilized in accordance with laws and regulations, and safeguard against loss or wastage, illegal or improper disposition, with a view to ensuring efficiency, economy and effectiveness in the operations of government.

Distinction from the other systems within the organization
Except for the Internal Audit Office which is part of the internal control system, internal controls are not separate specialized systems within an agency. They consist of control features interwoven into and made an integral part of each system that management uses to regulate and guide its operations. In this sense, internal controls are management controls.

Need for Strengthening Internal Control
An adequate internal Control system is essential in any organization.
- Adequate and strong internal controls in government have been found to be more effective than detailed audit in ensuring the integrity of operations of the agency and the entire range of administrative, financial, operating and reporting systems.
- Weak internal controls lead to waste and misuse of government resources and non-achievement of objectives.

Responsibilities of Agency Management for IC
The responsibilities are shared by the following:
1. Agency Head
   - To develop and install the internal control structure of the agency to include the control environment, accounting system and control procedures.
To maintain the internal control environment in order to safeguard assets, produce reliable accounting data and promote operational efficiency and effectiveness.

To evolve a system of evaluation and to implement appropriate corrective action.

2. Financial Chief Officer
- To review and assess the applicability of proposed system improvements.
- To identify laws, regulations and policies which need amendment/revision to improve the ICS.

3. Operating Chief Officers
- To identify inherent risks and potential errors and irregularities in their areas of operations.
- To ensure compliance with specific internal control policies and applicable laws and regulations.
- To evaluate existing systems.
- To review the proposed system improvements including the cost and benefit aspects.
- To identify laws, regulations and/or policies which need amendment/revision to improve controls or eliminate unnecessary controls.

4. Internal Control Office
- To identify potential errors, risks or irregularities, instances of inadequate or excessive controls and breakdowns in controls.
- To document the existing ICS.
- To monitor the agency’s compliance with laws, regulations and internal policies.
- To document and evaluate the ICS.
- To recommend measures to improve the existing controls.

The Role of Commission on Audit in IC
The COA is mandated by the 1987 Constitution to audit all government agencies. Where the ICS of any audited agency is inadequate, the Commission may:
- adopt such measures, including temporary or special pre-audit, as are necessary and appropriate to correct the deficiencies,
- shall ascertain the installation of an adequate ICS by the agency,
- shall be responsible for the design and preparation of the accounting system
- have the authority to evaluate the ICS of any agency to determine its adequacy

Components of IC
ICS basically consist of two components:
1. Plan of Organization
   - Consists of organizational structure that defines and distributes powers, functions and responsibilities to the various units and personnel which enable the organization to carry out and meet the overall objectives
2. Coordinate Methods and Measure
   - Pertains to systems of authorization, policies, standards, accounting systems and procedures and reports used by the agency to control its operations and resources and enable the various units to meet its objectives.

Types of IC
1. Accounting Controls - pertain to the plan of organization, the procedures and record that ensures the accuracy and the reliability of financial records.
2. Financial Controls - include the methods and procedures concerned with the safeguarding of assets and are designed to ensure transactions are executed, access to assets is permitted and recorded accountability for assets is compared with existing assets at reasonable intervals and appropriate action is taken.
3. Administrative Controls - include, but are not limited to, plan of organization, the procedures and records concerned with the management decision processes authorizing the transactions. They include controls over administrative offices such as personnel records and administrative functions.

Limitations of ICS
ICS only provide reasonable assurance that transactions are being executed in accordance with the objectives of IC. Consider the following limitations:
1. IC’s must be attained at reasonable cost. Some necessary controls may be sacrificed to avoid additional costs in terms of personnel, time and material.
2. Good internal control methods and measures are not foolproof. They are vulnerable to collusion.
3. Strong IC’s are still subject to human fallibility such as negligence, errors of judgment and lack of complete understanding.
4. Organizational changes may render ICS’s and manuals obsolete. Thus ICS’s and manuals must be constantly reviewed and updated to be relevant and effective.
5. The degree of compliance with ICS’s strongly influences their effectiveness. Too often, expensive IC manuals remain unused because of management’s non-implementation.

General Standards of Internal Control

**Purpose** - ICS must be evaluated and measured against standards to determine their adequacy. Standards define the minimum level of quality acceptable for ICS’s and the criteria to evaluate these systems. These established standards cover the traditional management areas and the conduct of operations. While the standards are applicable to all government operations and administrative functions, they do not intend to limit or interfere with prescribed agency policies or with pertinent legislations.

**Control Objectives**

Internal Control objectives are to be defined or developed for each agency activity. They are to be logical, applicable and reasonably complete. All operations of an agency can be generally be grouped into one or more categories called cycles. Examples of cycles are:

1. **Agency Management Cycle** – covers the overall policy and planning, organization, data processing and audit functions;
2. **Financial Cycle** – covers the traditional control areas concerned with the flow of funds (revenues and expenditures), related assets, and financial information;
3. **Program (Operational) Cycle** – refers to agency activities that relate to the missions of the agency.

**Control Techniques**

IC techniques are to be designed for and operated in all agency activities to accomplish the control objectives consistently, efficiently and effectively. There are two groupings of controls are:

1. **Basic controls** - ensure that transactions are recorded completely and accurately and the errors in execution of recording are detected as soon as possible, regardless of whether the error is the processing of an unauthorized transaction, the failure to process and authorized one, or the failure to process such a transaction accurately.
2. **Disciplinary controls** – ensure that proper and continued functioning of the basic controls and include supervision, segregation of duties and custodial arrangement.

There are five (5) frequently recurring “common control techniques, namely:

1. Control over completeness of processing
2. Maintenance of subsidiary records supporting a control account
3. Posting to inventory records
4. Supervisory review and approval
5. Checking of extensions and additions

**Example of Conventional Internal Control Techniques:**

<table>
<thead>
<tr>
<th>Internal Control Techniques</th>
<th>Accounting Control Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Physical Safeguard Controls:</strong></td>
<td></td>
</tr>
<tr>
<td>• Burglar Alarms</td>
<td>Deterrence or detection of theft of assets</td>
</tr>
<tr>
<td>• Plant Security Guards</td>
<td>To deter or detect theft of assets by outsiders and by employees seeking unauthorized access to assets</td>
</tr>
<tr>
<td><strong>Organizational Controls:</strong></td>
<td></td>
</tr>
<tr>
<td>• Bonding of employees occupying position of trust</td>
<td>To deter fraud and theft</td>
</tr>
<tr>
<td>• Define written assignments of responsibilities for the performance of each duty required to transact business</td>
<td>Deterrence of fraud, theft, and errors; assurance that duties will be carried out by qualified personnel; and assurance of smooth continuity of operations in the event of personnel changes</td>
</tr>
<tr>
<td><strong>Accounting Policies:</strong></td>
<td></td>
</tr>
<tr>
<td>• Use of control accounts</td>
<td>Deterrence and detection of fraud, theft and error</td>
</tr>
<tr>
<td>• Strict adherence to generally accepted accounting principles</td>
<td>Avoidance of disclosure errors and improper financial reporting</td>
</tr>
<tr>
<td><strong>Clerical Practices:</strong></td>
<td></td>
</tr>
<tr>
<td>• Vertical and horizontal addition of accounting work sheets</td>
<td>Assurance against clerical error</td>
</tr>
<tr>
<td>• Independent verification of clerical operations performed</td>
<td>To deter and detect fraud and error</td>
</tr>
</tbody>
</table>

**Reasonable Assurance and Cost**

ICS are to provide reasonable assurance that the objectives of the system will be accomplished at a reasonable cost.
Specific Standards of IC

**Documentation**
The agency ICS, policies, procedures, accountability for resources and all financial transactions shall be clearly documented and adequately supported.

**Recording Transactions and Events**
Financial transactions and events shall be promptly recorded in accordance with the state accounting standards. This would permit timely preparation of required financial statements and reports and maintaining adequate accountability for assets.

**Authorization and Execution of Transactions**
All transactions shall be executed by persons acting within the scope of their authority.

**Segregation of Duties and Functions**
Key duties and functions such as authorization, custody and accounting shall be assigned to separate offices and individuals to eliminate opportunities to conceal errors and irregularities.

**Supervision Scheme**
Qualified and continuous supervision of subordinates shall be provided to assure adherence to approved policies and procedures.

**Agency Resources: Physical Control and Access**
Tangible assets and records should be physically safeguarded. Access to these assets and records, both direct physical access and access through document processing, shall be in accordance with management’s authorization.

**Asset Accountability**
Accountability for the custody and use of an asset is to be assigned and maintained and periodic comparison shall be made of the existing asset with the recorded accountability and appropriate action taken on any differences.

**Built-In Checks**
Proofs of accuracy and documented trail transactions are features that should be built in to the execution and recording of transactions to assure the correctness.

**Presence of Appraisal Activity**
Reviews of transactions and internal control shall be performed on an on-going basis for proper monitoring of adherence to prescribed policies and procedures.

**Prompt Resolution of Audit Findings**
Officers shall promptly evaluate findings and recommendations reported by auditors, determine proper actions in response to audit findings and recommendations and complete within established time frames all actions that correct or otherwise resolve the matters brought to management’s attention.

**ICS Evaluation**

**Why is there a need to evaluate the ICS?**
Evaluation of the ICS is a means to determine effectiveness, correct deficiencies and improve the system.

It shall be conducted periodically:
- to ensure that the agency’s IC procedures and methods are operating as planned;
- to determine conditions call for revisions in the system;
- whether the prescribed procedures are being observed correctly.

The objectives of evaluating an ICS vary depending the evaluation purpose; timing and frequency of the evaluation shall depend on the evaluators and his objectives.

<table>
<thead>
<tr>
<th>Objectives of the Evaluation</th>
<th>Timing of the Evaluation</th>
</tr>
</thead>
<tbody>
<tr>
<td>The internal Auditor or the internal control office staff of the agency undertakes the ICS evaluation as a normal part of their work to monitor and improve internal controls.</td>
<td>For Internal Auditor or ICS Staff, review shall be done on a continuous basis.</td>
</tr>
<tr>
<td>The COA evaluates the ICS of the agency</td>
<td>For the Resident Auditor, an evaluation</td>
</tr>
</tbody>
</table>
Objectives of the Evaluation

under his jurisdiction to establish a basis for reliance that the laws and regulations are complied with and to provide for efficient, economical and effective operations.

Timing of the Evaluation

shall be done periodically as part of his regular audits before he prepares the detailed audit program.

• COA Central Operating Offices and Regional Offices evaluate ICS to provide a basis for a decision on withdrawal of the resident auditor.

• The COA Systems and Consultancy Division may also conduct ICS evaluation in connection with
  a. An operation review project
  b. A system and procedures manualization project
  c. Determining the advisability of installing an Internal Control Office.

Steps for IC Evaluation

1. Familiarization with the agency’s operations

   a. includes gathering of information and obtaining a good understanding of the agency operation, its goals and objectives, relevant laws, rules and regulations, the organizational and functional structures and the policies and procedures.
   b. Involves desk review of the pertinent materials such as previous audit reports, outputs of past studies, the charter creating the agency, manuals of procedures and organizational/functional charts.
   c. For automated system, the review process differs on the detailed procedures rather than general methods.
   d. Materials gathered at this stage shall form part of the permanent file of the agency and is a good reference for future evaluation.

2. Identification of Areas for Evaluation

   a. The ICS shall be divided into transaction categories depending on the scope of the evaluation.
   b. No material difference in financial areas subject to evaluation is notable whether the agency is a national, local or corporate entity.
   c. It is preferable to have no restriction in the scope of the ICS evaluation.
   d. Selection of areas shall not be determined by incidence of irregularity.
   e. Once the scope of the evaluation has been determined, the ICS shall be divided into areas for evaluation.
      - By organizational;
      - By cycle/process;
      - By elements of IC;
      - By financial statement (trial balance)
   f. The recommended approach divides the ICS into processes/cycles.

3. Documentation of Existing ICS

   The identified areas for evaluation shall be documented or recorded by the evaluator using any or a combination of or all of the following tools:

   a. Narrative Description - Consist of narrative statements regarding the existing IC’s of the agency.
   b. Flowchart - a schematic drawing or a map of interrelated operations specially arranged to show the movement of documents or flow of procedures/work from origin to its final disposition/completion
   c. Questionnaire - a review technique which consists of a series of questions to evaluate the client’s system of IC.

4. Confirmation of Documented ICS

   a. To ensure that the reviewers’ understanding of the ICS is adequate and correct, validation of this understanding shall be made.
   b. There are several ways of validating the documented ICS:
      - Confirmation statements of the system description from the information provided.
➢ Walkthrough procedures or the tracing of one or a few of the different types of transactions through the related documents and records.

c. The confirmation of the documented ICS may reveal discrepancies either because the flowchart and related narrative are wrong or because the system has broken down.

5. Analysis of the documented ICS

The most critical and difficult part is the analysis portion wherein the auditor has to answer “what is wrong or what is strong about the system.” This stage involves the following major steps:

a. Establishment of attributes of control objectives for each area documented.
b. Testing relevance to or compliance with control objectives. Here, sampling may be applied particularly with IC procedures that leave an audit trail in form of documentary evidence of compliance.
c. Determination of the deviation between the actual existing system vis-à-vis the ideal one. Deviation may result into either a positive or negative deviation.

6. Formulation of Recommendation

A determination to implement new control procedure shall be based upon consideration of the cost of additional controls in relation to the benefits to be derived from reduction of risk. Recommendations shall seek to achieve:

a. Reduced costs;
b. Improved service delivery;
c. Improved operations;
d. Reduced errors;
e. Improved policy, planning and decision-making process;
f. Compliance with laws, rules and regulations.

7. Conclusion and Decisions

a. Where the evaluation has indicated that controls exist and that they meet specified overall control objectives, the evaluation may decide to place reliance on these controls.
b. Where the evaluation has disclosed weaknesses in, or the absence of, IC, the evaluator will not able to restrict his substantive testing. He will have to extend his tests of transactions to obtain reasonable assurance that accounting records accurately reflect the transactions of the agency.

8. Reporting on IC’s

The evaluator shall report and communicate to agency management as soon as practicable, the results of the evaluation, reporting among others:

a. An over-all statement of the adequacy or inadequacy of the ICS;
b. An identification of material or significant IC weakness; and
c. Recommendations to improve the internal control systems.

Organization Benefits from Strong Internal Controls by:

➢ Reducing and preventing errors in a cost-effective manner.
➢ Ensuring priority issues are identified and addressed.
➢ Protecting employees & resources.
➢ Providing appropriate checks and balances.
➢ Having more efficient audits, resulting in shorter timelines, less testing, and fewer demands on staff.

Weak Internal Controls Increase Risk through…

➢ Business Interruption. System breakdowns or catastrophes, excessive re-work to correct for errors.
➢ Erroneous Management Decisions. Based on erroneous, inadequate or misleading information.
➢ Fraud, Embezzlement and Theft. By management, employees, customers, vendors, or the public-at-large.
➢ Statutory Sanctions. Penalties arising from failure to comply with regulatory requirements, as well as overt violations.
- **Excessive Costs/Deficient Revenues** expenses which could have been avoided, as well as loss of revenues to which the organization is entitled.
- **Loss, Misuse or Destruction of Assets** unintentional loss of physical assets such as cash, inventory, and equipment.

**Effective Internal Controls…**
- Make sense within each organization’s unique operating environment.
- Benefit rather than encumber management.
- Are not stand-alone practices; they are woven into day-to-day responsibilities.
- Are cost-effective.

The Dept of Finance & Management provides organizations with guidance & support to **improve Internal Controls through the following resources**:

- Self-Assessment of Internal Control
- Internal Control Standards Guide
- “Best Practices” series
- Quarterly Newsletter
- VISION Procedures
- Operational Reviews

**Sources/References of Report:**

http://en.wikipedia.org/wiki/Internal_control
Protiviti KnowledgeLeader (www.knowledgeleader.com)
Institute of Internal Auditors
www.cacubo.org/pdf/2007Chicago/dkm%20chicago%205.ppt

http://johnysnatad.wordpress.com