

Preface

The Auditing Standards of IAAD specify that audit should report on deficiencies noted in Internal Controls. The Perspective Plan of the department for 2003-08 stresses on formulation of standards for review of Internal Controls on the lines of the good practices articulated by INTOSAI and IIA, assessment of Internal Controls of selected agencies against these norms and communication of detailed guidelines for review of Internal Controls. In July 2003, CAG reiterated the importance of audit review of Internal Control systems including Internal Audit. It was decided to report upon Internal Control/ Internal Audit arrangements of the audited entities, and since the audit report cycle 2004-05, an appraisal of Internal Controls of a specified Department is appearing in a separate section in the Civil Audit Reports.

Pending development of guidelines on audit internal control, a Committee was set up in April 2005, consisting of Shri A.K. Awashti, Pr.AG, Shri Ashutosh Joshi and Ms Parama Sen, Directors, to develop a template for auditing and reporting the findings on Internal Control systems. Given that the audit objectives, scope and audit findings would largely shape the audit reports on Internal Controls, and considering the diverse range of government activities, it is difficult to frame a reporting template capable of encompassing the entire range of possible audit issues regarding internal control activities. The template presented in this volume is essentially an audit process template rather than a reporting template. A reporting template can only express a management perspective as the prime responsibility and accountability for internal controls rest with the management. In developing the process template some pointers regarding reporting audit findings related to internal control issues have also been included.

The basis of the process template presented here is the COSO (Committee of Sponsoring Organizations of the National Commission on Fraudulent Financial Reporting or the Treadway Commission) Internal Control – an Integrated Framework. This work was jointly prepared and issued in 1992 by the American Institute of Certified Public Accountants, the Institute of Internal Auditors, the American Accounting Association, the Institute of Management Accountants and the Financial Executives Institute. The COSO study and the resulting report was initiated to provide a unified insight into internal control to supplant the then pervasive different definitions of internal control, disparate views on the role of internal control in an entity and how it should be established, and varying opinions on how internal control effectiveness should be determined.

Internal controls are not clerical procedures or red tape and many procedures thought to be "internal controls" are simply processing procedures required to capture and record

data, but they provide no effective "control." Effective internal controls do not require redundant clerical checking or voluminous and detailed forms, both of which conditions can be ineffective and counterproductive. COSO framework takes internal controls beyond its traditional accounting (or financial reporting) objectives and relates it to the fundamental objectives of any organization. By laying stress on 'soft' aspects of Internal Control like 'tone at the top', risk assessments, efficient communications, employee attitudes and performance outcomes the COSO framework provides a paradigm shift in the management perspective on controls.

A related issue which deserves mention is the responsibility and accountability for evaluation of Internal Controls. The COSO framework emphasizes the management perspective and is primarily meant to be employed by the management to ensure compliance with laws, achievement of objectives and fair financial reporting. Internal Auditors use it to provide assurance to senior management and governing bodies regarding adequacy and effectiveness of internal controls. The role of external auditors comes in for providing assurances to the legislative body and other stakeholders. Unlike our country, these procedures are explicitly embedded in laws regulating business and government practice in most countries of the world. The Sarbanes Oxley Act 2002 in USA prescribes a template for reporting on controls over financial reporting by CEO/CFO of business enterprises. Similar procedures exist in UK. A US Presidential OMB circular of December 2004 states clearly that

'Management is responsible for establishing and maintaining internal control to achieve the objectives of effective and efficient operations, reliable financial reporting, and compliance with applicable laws and regulations. Management shall consistently apply the internal control standards to meet each of the internal control objectives and to assess internal control effectiveness. When assessing the effectiveness of internal control over financial reporting and compliance with financial-related laws and regulations, management must provide assurances on internal control in its Performance and Accountability Report, including a separate assurance on internal control over financial reporting, along with a report on identified material weaknesses and corrective actions.'

The time has perhaps come to prescribe similar routines for the managers in the Government sector. This would be consistent with the declared objective of the present executive government to establish administrative practices contributing to 'good governance'.

The COSO framework has met with phenomenal success since its publication in 1992 and has been widely adopted the world over as a benchmark criterion by professional

bodies and regulatory agencies. INTOSAI has also adopted it in its latest 'Report on Internal Controls' in 2004 and hence the proposed process template is in line with the Perspective Plan of our department. INTOSAI has extended the COSO objectives of internal control to explicitly include governance, ethical and VFM perspectives. Though these objectives have been integrated to the extent possible in our proposals, a lot of work still remains to be done. We hope that the proposed template would be used only as a starting point and would continue to be refined further in the light of our dispersed audit experiences and the evolving socio-economic and regulatory environment of the nation.

Ashutosh Joshi
Parama Sen
Arvind K. Awasthi

August 8, 2005

Introduction

Internal controls are essential to 'good governance' and may be understood as activities and safeguards that are in place to provide reasonable assurance that things are "going as planned." The credit for providing a versatile framework for the contemporary professional practice of internal controls goes to the COSO initiative.

COSO or the 'Committee of Sponsoring Organisations' was originally formed in 1985 in USA to sponsor the National Commission on Fraudulent Financial Reporting, an independent private sector initiative which studied the causal factors that can lead to fraudulent financial reporting. An array of concepts and views of internal control had developed over the years, expressed in various legislation, regulation, professional standards and guidelines, public and private reports, and a substantial and diverse body of academic literature. The scope of these writings was as broad as the wide variety of purposes internal control could serve and the many perspectives from which it could be viewed. COSO was primarily an effort to integrate and unify the concepts of internal control. It emphasized the importance of the control environment, codes of conduct, competent and involved audit committees and an active and objective internal audit function. The COSO study and the resulting 1992 report (Internal Control - Integrated Framework) was initiated to provide a common basis for the understanding of internal control among all parties and to assist management to exercise better control over an enterprise. Since its publication in 1992, the COSO framework has had exceptional success and is widely accepted as the global standard for Internal Controls in both public and private sectors. The COSO framework for internal control has been adopted by the INTOSAI and several other SAIs for evaluation of internal control within organizations. In many countries like the U.S. a series of legislations have been enacted that require public agencies to institute and support internal control mechanisms and to explicitly acknowledge the responsibility for internal controls over accurate financial and operational reporting.

Definition:

Internal control is broadly defined by COSO as a process, effected by people and designed to provide reasonable assurance regarding the achievement of the following three objectives that all organisations strive for:

- Economy and efficiency of operations, including achievement of performance goals and safeguarding of assets against loss;
- Reliable financial and operational data and reports; and
- Compliance with laws and regulations

From the above definition it is important to note the following key concepts

- Internal control is a process. It is a means to an end, not an end in itself.
- Internal control is effected 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.

To achieve quality, processes must first be in control. To improve quality, controlled processes must be measured and evaluated to identify obstacles to success. Effective internal control opens the door that leads to achievement of success. The approach presented by the COSO Framework goes directly to the one key issue of any organisation - is there reasonable assurance of achieving our mission, objectives, goals and desired outcomes, while adhering to laws and regulations; and can we accurately report our success and outcomes to the public and interested third parties.

INTOSAI Guidelines for Internal Control

In its latest guidelines, INTOSAI has completely integrated the COSO concepts of Internal Control. The definition and objectives of Internal Control have, however been extended to include the following

- 'fulfilling accountability obligations' in place of 'reliable financial data and reports'
- 'executing orderly, ethical, economical, efficient and effective operations' in place of 'economy and efficiency of operations including achievement of performance goals'

- 'Safeguarding resources against loss' has been added as a distinct and separate objective in place of the earlier 'safeguarding assets against loss' included as a part of the operational objective in the COSO definition.

Ethics has been made an important control objective as ethical behaviour by public servants is considered a keystone of good governance. A practical dimension of this objective would be to have fraud control measures in place. Orderly and effective terms bring in systems and performance outcome aspects. Since budgetary accounting on a cash basis (common in the public sector) does not provide sufficient assurance relating to maintenance of records of assets/resources, safeguarding of resources has been made an important control objective and the word 'assets' has been replaced by the word 'resources' which has a wider connotation.

Accountability obligations in the corporate sector are fairly well defined in law (as well as professional accounting/reporting standards) and the Annual Reporting requirements including the Directors Report and Annual Financial Statements are well established practices. For the public sector, accountability is realized by maintaining reliable financial and non-financial information and fair reporting to internal and external stakeholders. For instance, budgetary assumptions, internal policy formulations, qualitative reports on performance, replies to legislative queries could all be brought within the orbit of internal controls.

Audit of internal control: Indian context

In India, no specific internal control legislations have been enacted. In the absence of specific legislation, the requirement for maintaining internal control is not clearly recognised as an explicit management responsibility. The traditional view that internal controls are the manualised rules and procedures guiding departmental functions still persists. Many procedures thought to be "internal controls" are simply processing procedures required to capture and record data, but they provide no effective "control." An audit of internal controls relevant to an audit objective is very often an exercise to secure compliance with applicable laws and regulations. The control environment is usually a given endemic situation and there is very little managerial flexibility in improving the situation. Risk identification and assessment is informal and rudimentary; and very often only an intuitive exercise motivated by the desire to cover short-term personal/departmental risks to career/reputation. Adoption of the COSO

framework would involve a paradigm shift in the managerial approach towards internal controls and internal audits. A moot point is whether the COSO framework could be utilized for the audit process when far from being a statutory requirement it is not even a general expectation from the managerial class.

The Committee felt that in the current global scenario of converging professional practices, it was inevitable that COSO would emerge as the benchmark criterion for the management of internal controls. Accordingly through our audits we could recommend adoption of better practices in this area.

Components of Internal Control

Internal controls are “the whole system of controls, financial or otherwise, established by the management in order to carry on the business of the organization in an orderly and an efficient manner, ensure adherence to management policies, safeguard assets and secure, as far as possible, the completeness and accuracy of records”. Internal controls broadly consist of the control environment and control procedures. While the former reflect the attitude and commitment of the management towards running the organization, the latter are the processes established to reassure that the specific objectives of the organization are met.

For control procedures to work in the fashion envisaged the various functionaries in the organization must perform their jobs correctly. Errors of judgment or misinterpretation, negligence and the like can undermine the effectiveness of internal controls. More serious impairment can arise out of abuse of authority or from collusion between functionaries to circumvent controls for perpetrating fraud. Therefore, the mere fact that internal controls are in place is not enough. The internal controls must be periodically assessed for their adequacy to ensure that they are being adhered to in the manner envisaged.

Internal Control is an intrinsic part of all systems within the organization. It is built in to the systems and is used by the managers to guide its operations on a continuous basis, it should not be thought of as a separate system within the organisation.

Internal Control consists of five components (1) Control Environment (2) Risk Assessment (3) Information & Communication (4) Monitoring (5) Control Activities.

The first four components are generally called the broad components of internal control inasmuch as these are wider and relate to the broad frameworks for internal control whereas control activities are the specific procedures etc. established to achieve identified control objectives of the organization as may emanate from the first four. The broad components can influence effectiveness of control activities.

Considering relevance of internal controls to audit using the internal control assessment template

The purpose of the template is to help audit parties during audit planning to determine if internal control is significant to their audit objectives. The template should be used in conjunction with the auditing standards, performance auditing guidelines and other relevant circulars and guidelines issued from time to time.

Generally audits whose objectives are to evaluate issues such as:

- How effectively and efficiently are organizational or scheme goals, and objectives being achieved?
- Whether the organization has complete, accurate, and relevant information that it needs to support performance and decision-making?
- Whether organizational resources are being used in compliance with applicable laws and regulations?
- Whether organizational resources are safeguarded against misuse?

are likely to involve audit of internal control. The audit party should consider the nature, scope and focus of their audit objectives to arrive at a conclusion regarding relevance of internal controls to audit.

The audit party should examine the internal controls significant to the audit objectives and determine if specific internal control procedures have been properly designed and implemented. Based on the effectiveness of internal control the audit party should consider if it needs to modify the nature, timing, or extent of audit.

Components of internal control or any weakness therein is significant to an audit's objectives if it is likely to significantly affect the (1) nature and/or presentation of other potential findings and conclusions that may result from carrying out the audit or (2) the auditor's judgments (either positively or negatively) about the sufficiency, competence, or relevance of planned audit evidence required to satisfy the audit's objectives.

The audit party should go through part A and B of the template and consider whether the components of internal control are significant to their audit objectives by answering in 'yes' or 'no' to the questions listed against each. In case the answers to all questions for all audit objectives is no the audit party should include a note to explain why internal control is not significant.

Part A.

Broad Components of Internal Control

Components Of Internal Control	Is the Internal Control component significant to the audit objectives?
<p>1. Control Environment—</p> <ul style="list-style-type: none"> • The program’s organizational structure and delegation of authority and responsibility, • The integrity and ethical values maintained and demonstrated by management, and • Management’s commitment to competence as well as its philosophy and operating style. 	<p>Y N</p>
<p>2. Risk Assessment—</p> <ul style="list-style-type: none"> • Reliance on information received from branch offices of the organization • Peculiar economic or geographic or other factors that impact the program. 	<p>Y N</p>
<p>3a. Information— Availability of pertinent, reliable, and timely information to authorities for decision-making and for external reporting purposes.</p>	<p>Y N</p>
<p>3b. Communications— Existence of effective and timely internal communications within the organization for enabling management and staff to discharge their internal control and other duties and external communications with concerned parties.</p>	<p>Y N</p>
<p>4. Monitoring— existence of effective monitoring for assessing quality and performance over time and including supervisory monitoring activities, like,</p> <ul style="list-style-type: none"> • Reviews of results by the management, • Rectification of previously identified deficiencies, and • Effectiveness of internal audit 	<p>Y N</p>

Part B.

Specific Internal Control Procedures

Internal Control Activities	Are the control procedures significant to the audit objectives?
<p>Internal Control Activities—</p> <ol style="list-style-type: none"> 1. Design and implementation of policies and procedures for managing the program, 2. Establishment and review of performance measures and indicators, 3. Appropriate separation of duties, 4. Physical control over assets, 5. Safeguarding of program resources and funds from misuse or unauthorized disposal 6. Grantees are properly screened for eligibility and monitored for performance and program goals, 7. Recipients of aid are properly screened for eligibility 8. General and application controls over information processing, 9. Accurate and timely recording and documentation of transactions and events, and 10. Others (please specify) <p>_____</p>	<p>Consider each question and answer in 'yes' or 'no' and attach to your design template</p>

	<p>Adherence to the conduct rules?</p> <p>What is the nature of values reflected in the behavior?</p> <p>Existence of a formal code of conduct.</p> <p>Are declarations as required by the applicable conduct rules being made as and when required.(e.g. annual statement of immovable property under conduct rules.</p> <p>Codes/guidelines exist for issues such as conflict of interest etc.</p> <p>How are vigilance issues being dealt with by the organization (raised through complaints, CVC, public media)</p> <p>Reports issued by the organization to public legislature, regulatory bodies are accurate and proper (not intentionally misleading).</p> <p>The management cooperates with auditors and evaluators</p> <p>Overpayments by buyers or under billing by suppliers is rectified quickly</p> <p>What is the organizations track record in dealing with disciplinary cases?</p> <p>Orders/guidelines exist giving the circumstances (and frequency) when</p>	<p>Examine codes of conduct To see if the guidelines therein are being followed</p> <p>Examine records of cases</p> <p>Examine reports and cross check data from the original sources</p> <p>Examine relevant records</p> <p>Examine relevant</p>
--	---	---

<p>C) Management's commitment to competence as well as its philosophy and operating style</p>	<p>normal procedures can be bypassed by individuals and the level at which this can be done</p> <p>Proper documentation exists for all cases where individuals have exceeded their powers giving specific action taken and reasons therefor.</p> <p>Lower level employees do not over ride internal control except in emergencies. (All circumstances are documented and management notified immediately)</p> <p>The organization has set realistic goals for its employees and does not pressure employees to meet unrealistic ones?</p> <p>The incentives provided are fair so as to help employees to maintain integrity?</p> <p>Are rewards are linked to performance?</p> <p>Managements approach towards human resource issues?</p> <p>The turnover rate of persons in important management position, is not too rapid to adversely affect internal control due to several new people</p>	<p>documentary evidence</p> <p>Examine human resource policies for their contents and their active application.</p> <p>Examine the turn over in the organization.</p> <p>Examine the succession planning.</p>
---	--	---

	<p>(occupying key posts) being unfamiliar with their jobs</p> <p>How decision making is done in the organization?</p> <p>How problem solving is approached?</p> <p>Job descriptions for posts have been drawn and the consideration has been given to the extent of delegation and supervision required.</p> <p>The organization attempts to ensure that persons selected for particular posts have the requisite background, experience. (say, a person to manage a finance related post has competence and experience in the area)</p> <p>Appropriate training programs exist to meet the needs of the organization</p> <p>Is training used by the organization for upgrading skills? Mechanism exists to monitor that all employees actually receive appropriate training.</p> <p>Evidence exists that accounts and budget reports are used for exercising control over and monitoring of activities and also for decision making</p> <p>What is the system to address personnel grievances and other</p>	<p>Examine procedures of decision making. Are inputs from subordinates taken and used?</p> <p>Is the process participative, or directive or a mixture of both?</p>
--	--	--

	<p>employee related issues?</p> <p>What importance is given to internal audit/external audit and other studies</p> <p>How does the management look upon issues raised by internal audit/external audit/other studies?</p> <p>Examine response of the organization towards audit findings</p>	
<p>2) Risk assessment</p> <p>The management comprehensively identifies risk</p>	<p>Does the management of the organization periodically analyze risks affecting it?</p> <p>Are major risks as identified, communicated to the staff? The staff is also informed on how to mitigate risks?</p> <p>Does risk identification find a place in formulation of long term/short term planning and in strategic planning?</p> <p>Does the organization use audit reports, evaluations and other assessments to identify risks?</p>	<p>Examine documents, records of meetings etc. to see if evidence exists to support that risk assessment is being done</p>
<p>Identification of risks from external factors</p>	<p>Does the organization evaluate risks that may be associated with technological advances?</p> <p>Does the organization consider risks arising from changing needs and expectations of the</p>	<p>As above</p>

<p>Risk Identification on account of internal factors</p>	<p>legislature/public?</p> <p>Does the organization identify risks that may be associated with new legislation regulations, changing business, political and economic conditions?</p> <p>Does the organization identify risks arising out of natural calamities, criminal activity etc?</p> <p>Does the organization consider risks that may be associated with major suppliers and contractors?</p> <p>Does the organization identify risks associated with business process reengineering or with changing operational procedures?</p> <p>Does the organization identify risks on account of failure of computer systems?</p> <p>Does the organization identify risks due to decentralization of operations?</p> <p>Does the organization identify risks due to geographical spread of operations?</p> <p>Has the organization considered risks on that relate to past failures?</p> <p>Does the organization have a past history of improper,</p>	<p>As above</p>
---	--	-----------------

<p>Risk evaluation</p>	<p>excess expenditure or non-compliance with rules regulations?</p> <p>During appraisals of projects, periodic meetings to review status of work, are the identified risks to activities analyzed?</p> <p>Does the organization have criteria to grade (classify) risks as low, medium or high? Is the impact of risk analyzed? Is the impact and likelihood of risk assessed?</p> <p>Is the risk analysis being done at appropriate levels of management?</p> <p>Have control activities been instituted to monitor and mitigate risks that have been identified?</p>	
<p>Reliance on information supplied by third parties/ contractors</p> <p>Limitations on ability to substantiate eligibility data</p>	<p>Is the information supplied reliable?</p> <p>Does the organisation evaluate data supplied?</p> <p>Is the information generated by the agency itself correct / self-checked?</p>	<p>Examine procedures for data verification</p> <p>Have the procedures been adhered to</p> <p>What has been done in case data turned out to be inaccurate</p>
<p>Peculiar demographic /geographic/budgetary or other factors that affect the program</p>	<p>Has a lot of money been injected into the program or vice versa?</p>	<p>Examine funding</p> <p>In case funds have been cut what has been the impact on internal control i.e. have they been diluted or simply done away with if</p>

<p>Managing risk during change</p>	<p>Have all activities that are significantly affected been considered?</p> <p>Do risks that arise due to change in legislation, regulations or other macro factors get considered at appropriately high levels so that the impact on the organization as a whole is considered?</p> <p>Are Risks on account of introduction of new charged information systems/new technologies considered?</p>	<p>so what are the risks?</p> <p>Examine documents, records of meetings etc. to see if evidence exists to support that risk assessment is being done</p>
<p>Information—Relevant, reliable, and timely information is available for management decision-making and for external reporting purposes.</p>	<p>Examine the data used for decisions.</p> <p>Are any cross checks of data carried out?</p> <p>Does the organization have proper information management systems that gather important data needed for decision-making?</p> <p>Also examine reliance placed upon the system if it exists?</p> <p>Is the information/data, supplied by personnel through reports, accurate?</p> <p>Do the personnel reported inaccurately to meet targets?</p> <p>Are the budgetary estimates fair?</p> <p>Is the capacity of the grantee to deliver</p>	<p>Examine documentary evidence to see how data has been used / cross checks done and capacity assessed</p>

	assessed?	
<p>Communications— Effective and timely internal communications enable an organization’s management and staff to carry out their internal control and other responsibilities and external communications with stakeholders</p>	<p>Does the organization allow for easy flow of information back and forth? Process for notifying the management of the problems. Does the management disclose all financial, budgetary and program information needed for proper understanding of finances and operations about the organisation to the legislature, regulatory bodies, audit etc? Does the organizational structure help the flow of information throughout the Organisation? Have proper reporting relationships been established and are they effective in providing information to management for effective functioning? What is the mechanism for conveying risks, problems etc that are identified by lower level functionaries to senior management?</p>	<p>Interview persons Examine documents to see if the stated procedure is adhered to Examine documentary evidence to see if the problems reported are considered and acted upon</p>
<p>Monitoring— existence of effective monitoring for assess sing quality and performance over time and including supervisory monitoring activities, like, Reviews of results by the</p>	<p>The mechanism of monitoring The extent of reviews, Their periodicity The level at which these are conducted Who sees the reports What action is taken on the</p>	<p>Examine procedures Examine documentary evidence to see if the stated procedures are actually implemented The follow up action on the deficiencies noticed in the reviews</p>

management	reports	
Rectification of previously identified deficiencies, and		
Effectiveness of internal audit		

Internal control activities

Control element	Issues examined	Evidence gathering technique
Design & implementation of policies and procedures for managing the program	Details of specific procedures that are being examined in depth after being assessed as important to audit objectives	Examination of documentation of procedures and evidence to see if they have been adhered to.
Top level reviews	<p>Are the progress reports of expenditure compared against the budget as well as operational targets of the whole entity submitted to the head of the organization regularly?</p> <p>Are progress reports for important / significant projects/ activities submitted regularly to the head of the organization?</p> <p>Are the actions suggested by the head of the organization followed up?</p>	<p>Study of entity manuals laying down procedure for review and follow up of review.</p> <p>Examination of entity documentation regarding review and their follow up.</p> <p>Conducting interviews</p>
Review at the activity/ functional level	<p>Are managers at the activity level receiving information regarding financial and physical progress of activities within their control?</p> <p>Is this information reconciled</p>	<p>Study of entity manuals for laid down procedures.</p> <p>Examination of entity documentation.</p> <p>Conducting interviews</p>

<p>.Management of human capital</p>	<p>with the supporting documents for checking accuracy?</p> <p>Are the reported performances benchmarked against expected performances/ results (targets)?</p> <p>Are the reasons for shortfall in achievement of targets analyzed?</p> <p>Are actions taken for correction and is there a follow up mechanism?</p> <p>Does the entity have a strategic plan and an annual plan?</p> <p>Is there a human resource plan linked to the strategic plan that lays down the human resource requirement for the entity, both in skill and quantity terms?</p> <p>Does the requirement include specific understanding of the competencies needed? Is the requirement of each role established?</p> <p>Is there a mechanism of</p>	<p>Study of entity strategic and annual plans linked to personnel requirements.</p> <p>Study of human resource policies and plans of the entity.</p> <p>Study of entity documentation to understand implementation of human resource plan.</p>
-------------------------------------	--	--

	<p>recruiting personnel with necessary skill set?</p> <p>Are the employees being trained for enhancing their capabilities to meet organizational needs</p> <p>Are the compensation/ incentives sufficient to retain and encourage personnel?</p> <p>Are there adequate employee friendly measures that would enhance employee satisfaction and commitment?</p> <p>Is there adequate supervision to ensure that control objectives are being met?</p> <p>Are the roles and duties of employees clearly defined and are they being assessed for achieving the set targets?</p> <p>Is there adequate planning to ensure continuity of skills and abilities?</p>	
<p>Establishment and review of performance measures and indicators and review of performance measures and indicators</p>	<p>1) Have indices have been established to monitor performance at organization, unit and individual level?</p> <p>2) Are performance measures reviewed</p>	<p>Examine documentary evidence to see how performance measures and targets have been established.</p>

	<p>periodically for correctness and reliability?</p> <p>3) Are the performance measurement assessment factors related to mission goals and objectives?</p> <p>4) Performance data are continually monitored and analyzed?</p>	<p>Examine the reports on performance and targets.</p> <p>Examine documents to see if the program has been modified due to evaluations done on basis of performance of the program.</p>
Appropriate separation of duties	<p>Are all key aspects of a transaction under a single persons' control?</p> <p>Examples of some key roles that need to be segregated:</p> <ol style="list-style-type: none"> 1. Authorization of expenditure, processing, recording, making payments 2. Custody of cash and bank reconciliation 3. Custody and handling of assets. <p>Are duties assigned to a number of persons for ensuring checks and balances?</p> <p>Is the management alert towards avoiding collusion?</p> <p>Have surprise checks been instituted to detect collusions?</p>	<p>Examine delegation of duties to see if any conflict or overlap exists</p> <p>Examine organisation record to see the extent of senior management supervision over staff in sensitive areas</p> <p>Study of Organizational chart</p> <p>Examination of documents of entity</p> <p>Conducting interviews</p>
Physical control over assets.	<p>Do policies to safeguard assets exist and are these known to all?</p> <p>Has the organization</p>	<p>Examine agencies procedures for inventory verification</p> <p>Examine documents</p>

	<p>identified and ensured adequate protection for its critical assets?</p> <p>Are assets like cash which are vulnerable to loss, theft adequately guarded?</p> <p>Are the stock verification procedures adequate and are they adhered to?</p> <p>Does the entity have adequate mechanisms for dealing with failures in security?</p> <p>Are the inventories, supplies and finished goods protected for companies/ other entities which have production activity?</p> <p>Is the access to facilities restricted?</p>	<p>(reports) and interview persons to see if the checks instituted are adhered to.</p>
<p>Safeguarding of program resources and funds against unauthorized acquisition, use, or disposition by employees, and recipients of program benefits</p>	<p>Do policies to safeguard program resources and funds exist and are these known to all?</p> <p>Has the organization identified and ensured adequate protection for its resources and funds?</p> <p>Are assets like cash, which are vulnerable to loss, theft adequately, guarded?</p> <p>Are the funds and resources verification procedures adequate and are they adhered to?</p>	<p>Examine agencies procedures for verifying resources and funds</p> <p>Examine documents (reports) to see if the checks instituted are adhered to.</p> <p>Study of manuals, procedures laid down in the entity</p> <p>Examination of documents of the entity</p> <p>Conducting interviews</p>

<p>Execution of transactions</p>	<p>Are transactions carried out in the manner intended? (e.g., orders of the competent authority taken before action)</p> <p>Does the level sanctioning the transaction have the authority to do so?</p> <p>Are terms of authorization and conditions attached to the sanction communicated along with the sanction?</p> <p>Are the terms of authorization compliant with law, established practices and procedures?</p>	<p>Examination of procedures, organizational chart</p> <p>Study of documents of the entity, e.g., annual physical inventory report.</p> <p>Conducting interviews</p>
<p>Accountability for resources and records</p>	<p>Has the custody of records been assigned to specific individuals?</p> <p>Are there access restrictions to records and are the custody arrangements reviewed from time to time?</p> <p>Is the degree of restriction to access placed commensurate with the asset value, portability, and exchangeability?</p> <p>Is there regular comparison of actual resources with the recorded values and</p>	

	examination of differences, if any examined	
Grantees are properly screened for eligibility and monitored for performance and program goals,	Has the organization established criteria for identifying grantees How is their performance monitored for achievement set goals	Examine documentary evidence to see if criteria for selection have been made, the target setting and monitoring mechanism put in place Is it being adhered to
Recipients of aid are properly screened for eligibility	Has the organization established criteria for identifying the recipients for aid? Is each case examined to see if the criteria have been met?	Examine documentary evidence to see if the grant has been disbursed only for eligible cases
General and application controls over information processing,	Are risk assessments performed and documented when systems are changed Is data sensitivity and integrity considered in risk assessments Does an entity wide security program exist Is access to information, software codes suitably restricted Do procedures for managing software change exist Does proper segregation of duties exist Does a contingency plan exist for ensuring continuity of the service Are the accounting/	See if security manuals exist and they lay down requisite safety procedures Check to see if the manualized procedures have been adhered to

	<p>operational information being processed in the correct sequence as laid down in the entity manual/ rules/ procedures? (Whether the control totals are checked at each stage, exceptions pointed out and steps taken for correction)</p> <p>Is the access to files controlled? (These could be confidential files, tenders, etc.)</p>	
<p>Accurate and timely recording and documentation of transactions and events, and Internal control procedures</p>	<p>Are transactions properly and promptly classified Are the supporting records properly maintained</p> <p>Are the transactions recorded in the appropriate format?</p> <p>Are there excessive adjustments to numbers or account classifications?</p> <p>Is the internal control structure of the entity adequately documented? (Written code of procedure/ manual covering significant transactions in the entity including management directives, administrative policies, accounting procedures, etc.)</p> <p>Can the documentation of</p>	<p>Examine transaction records and trace flow of transactions.</p> <p>Study of manuals, codes applicable to the entity.</p> <p>Examination of entity documentation of transactions and events.</p> <p>Examination of returns and reports submitted to management based on the documentation.</p>

	<p>transactions and events be traced through the entire process – from authorization and initiation through processing?</p> <p>Are the reports and returns based on the documentation submitted to the managers regularly?</p> <p>Is the documentation properly maintained and periodically updated?</p>	
Others (please specify)		

Reporting on Internal Control

Our Auditing Standards stipulate that 'On the completion of each audit assignment, the Auditor should prepare a written report setting out the audit observations and conclusions in an appropriate form; its content should be easy to understand, free from ambiguity and supported by sufficient, competent and relevant audit evidence and be independent, objective, fair, complete, accurate, constructive and concise'.

These standards apply in their entirety to reporting on internal controls. The Audit of Internal controls have three broad objectives to check for A) efficiency and effectiveness of operations B) compliance with laws and regulations, and C) Accurate financial reporting. The committee felt that for the time being we should adopt only a limited definition of Internal Control. The application of INTOSAI definition is likely to create problems of comprehension for all stakeholders to the audit process in the prevalent Indian circumstances.

The audit of internal control of an entity would result in a report. The report includes all 'reportable' matters and presents the audit assessment/ opinion regarding the adequacy and effectiveness of internal controls under study. Adequacy relates to the optimality of controls while effectiveness relates to the manner in which the controls are operationalised.

Normally internal controls should be designed to monitor itself. The greater the degree and more effective the ongoing monitoring is, the less need for separate evaluations. These matters should generally fall within the scope of the Internal Audit function and the external audit process would often result in a recommendation to put in place a proper framework for Internal Controls (including Internal Audit).

The Institute of Internal Auditors 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.' The committee felt that since Internal Audit functions are not properly developed in most public organisations, external audit reports may need to integrate elements of consultancy (relating to internal control) as a way of providing added value and to improve an organization's operations

The following aspects need emphasis in a report on evaluation of internal controls of an entity:

- Specify the background and objective of the study: An internal control audit in an entity within the scope of regularity audit could cover three components: assessment of financial reporting, operations and compliance. It is essential to define clearly the audit intent at the beginning, whether the audit assessment extends to all the three aspects or addresses issues selectively. It should also be specified whether the assessment covers all the five components of internal control as per the COSO framework. A brief background of the entity along with the reason why the audit objective is important for the entity under study would add perspective to the audit report.
- Define the scope: The scope over which the audit study and assessment extends should be specified. For example, specific departments of the entity could be covered or the study could be restricted to a particular geographical area. The time period over which the controls are being assessed also needs to be specified in the study. A study with a well-defined scope will clearly add to the relevance and focus of the assessment.
- Mention audit methodology: The methodology adopted for the internal control audit should be mentioned. This would involve a discussion of the evaluation criteria used and the mechanism adopted for collecting evidence.
- Report significant audit findings: Audit findings would highlight a deficiency or a material weakness in the elements of internal control. A 'deficiency' is a condition within the internal control which is worthy of attention. A deficiency may represent a perceived, potential or real problem or an opportunity to strengthen the organisation's internal control. All internal control deficiencies that can significantly affect the attainment of control objectives should be reported. In case of a lapse/ lack of control, responsibility for establishment and maintenance of the control element should preferably be indicated. The reply of the entity to audit findings also needs to be incorporated with a suitable rebuttal if required.

To form an opinion as to whether control systems provide managers with reasonable assurance that desired organisational outcomes will be achieved, the auditor has to consider the issue of materiality. No control system is perfect or one hundred percent effective. But an effective control system should always prevent, or detect and correct, material errors, omissions, fraud or other adversities that impact on achieving desired outcomes. The Institute of Internal Auditors, defines materiality as "any condition that has caused, or is likely to cause, errors, omissions, fraud or other adversities of such magnitude as to force senior managers to undertake immediate corrective actions to mitigate the associated business risk and possible

consequent damages to the organization". Material weaknesses are persistent if the same problem appeared in prior periods; or the same problem has arisen elsewhere in the organization. Material weaknesses are pervasive if the effects of the problem seriously imperil safeguarding of assets; or the effects of the problem seriously imperil the achievement of operating, reporting or compliance objectives. A condition is "serious" if it has caused, or is likely to cause, errors, omissions, fraud or other adversities that increase business risk and possible consequent damages to the organization, but does not require senior managers to undertake immediate corrective actions to mitigate the associated impact on operations or outcomes. A "reportable condition" means that:

- the problem is serious, but not material; or
- the problem is material but not persistent or pervasive; or
- the problem is material and persistent or pervasive.
- For financial audits (objective C above) the reportable conditions may include
 - Absence of appropriate segregation of duties consistent with appropriate control objectives:
 - Absence of appropriate reviews and approvals of transactions, accounting entries, or systems output;
 - Inadequate provisions for the safeguarding of assets
 - Evidence of failure to safeguard assets from loss, damage, or misappropriation;
 - Evidence of system failure to provide complete and accurate output consistent with the control objectives of the audited entity due to misapplication of control activities
 - Evidence of intentional override of internal controls by those in authority to the detriment of the overall objectives of the system
 - Evidence of failure to perform tasks that are a significant part of internal control such as reconciliations not prepared or not done on time.

- A weakness in the control environment at an entity such as absence of positive and supportive attitude towards internal control by the management within the organisation.
 - Deficiencies in the design or operation of internal control that could result in violation of laws regulations provisions or contract or grant conditions: fraud; or abuse that has a material effect on the audit objectives or the financial reports.
 - Failure to correct deficiencies identified earlier
- For the other objectives the reportable conditions would include any significant deficiencies in the internal control, all acts of fraud and illegal acts unless absolutely inconsequential, significant violations of provisions of contracts or grant agreements and significant abuse.
 - Derive audit conclusion: The audit conclusions flow from and highlight the significance of the audit findings. This would indicate whether the internal controls under audit study are adequate and performing satisfactorily and highlight weaknesses noticed. The assurance with regard to internal controls could be a negative assurance - a statement that nothing came to the auditor's attention that would indicate inadequate controls.
 - Recommendations: The recommendations flow from the findings and conclusions. Recommendations set out the actions that need to be taken to correct the lapse. It is prudent to discuss the recommendations with the entity. While lack/ inadequacy of a control element may leave an uncovered risk to the entity, the cost of correcting the problem could be high when compared to the benefits. The practicality of the recommendations is crucial to their acceptance by the entity. Recommendations need to be discussed with the entity. The findings and recommendations could be arranged in order of their significance/ impact.

Appendix I

The concepts underlying the elements of the template

These fundamental concepts providing an understanding of the elements of internal control

Internal control is not one event, but a series of actions and activities that occur throughout an entity's operations and on an ongoing basis. Internal control should be recognized as an integral part of each system that management uses to regulate and guide its operations rather than as a separate system within a department. In this sense, internal control is management control that is built into the entity as a part of its infrastructure to help managers run the entity and achieve their aims on an ongoing basis.

People make internal control work. The responsibility for good internal control rests with all managers. Management sets the objectives, puts the control mechanisms and activities in place, and monitors and evaluates the control. However, all personnel in the organization play important roles in making it happen.

Management should design and implement internal control based on the related cost and benefits. No matter how well designed and operated, internal control cannot provide absolute assurance that all department objectives will be met. Factors outside the control or influence of management can affect the entity's ability to achieve all of its goals. For example, human mistakes, judgment errors, and acts of collusion to circumvent control can affect meeting department objectives. Therefore, once in place, internal control provides reasonable, not absolute, assurance of meeting department's objectives.

Control Environment

A positive control environment is the foundation for all other standards. It provides discipline and structure as well as the climate which influences the quality of internal control. Several key factors affect the control environment. One factor is the integrity and ethical values maintained and demonstrated by management and staff. Department management plays a key role in providing leadership in this area, especially in setting and maintaining the organization's ethical tone, providing guidance for proper behavior,

removing temptations for unethical behavior, and providing discipline when appropriate. Another factor is management's attitude to competence. All personnel need to possess and maintain a level of competence that allows them to accomplish their assigned duties, as well as understand the importance of developing and implementing good internal control. Management needs to identify appropriate knowledge and skills needed for various jobs and provide needed training, as well as candid and constructive counseling, and performance appraisals.

Management's philosophy and operating style also affect the environment. This factor determines the degree of risk the department is willing to take and management's philosophy towards performance-based management. Further, the attitude and philosophy of management toward information systems, accounting, personnel functions, monitoring, and audits and evaluations can have a profound effect on internal control.

Another factor affecting the environment is the department's organizational structure. It provides management's framework for planning, directing, and controlling operations to achieve department objectives. A good internal control environment requires that the department's organizational structure clearly define key areas of authority and responsibility and establish appropriate lines of reporting.

The environment is also affected by the manner in which the department delegates authority and responsibility throughout the organization. This delegation covers authority and responsibility for operating activities, reporting relationships, and authorization protocols.

Good human resource policies and practices are another critical environmental factor. This includes establishing appropriate practices orienting, training, evaluating, and disciplining personnel. It also includes providing a proper amount of supervision.

A final factor is the attitude towards Internal and External Audit, and other watchdog bodies such as the Vigilance commission etc.

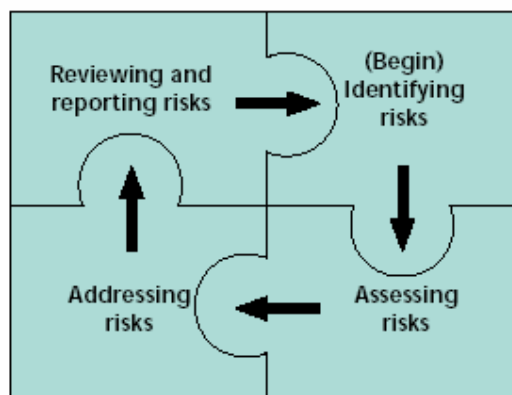
Risk Assessment

Governments have always had a critical role in protecting their citizens from risks. The key factors include: addressing difficulties in handling risks to the public; recognition of the importance of early risk identification in policy development; risk management in programmes and projects; and the complex issues of risk transfer to and from the private sector.

Governments have three clear roles in managing risk. Where individuals or businesses impose risks on others, government's role is mainly as a regulator, setting the rules of the game. Where risks cannot be attributed to any specific individual or body, governments may take on a stewardship role to provide protection or mitigate the consequences. In relation to their own business, including provision of services to citizens, governments are responsible for the identification and management of risks.

In each of these areas there are no wholly reliable formulae for defining risk. Governments need to make judgments in as open a way as possible about the nature of risk and how responsibilities should be allocated, recognising that there will always be some unavoidable uncertainty. This element of control relates to the threats (risks) that may prevent the organization from achieving its goals. This is relevant as improper appreciation of threats (risks) can lead to misallocation of resources by the management. As available resources are usually limited, this hampers the achievement of objectives.

The risk cycle starting from identification to reviewing and reporting is shown in the graphic below:



Risk identification requires that the managers acquire a clear understanding of the activities and the environment within which they operate. Without knowledge and understanding of the activities, full appreciation of the threats (risks) that maybe present is not possible. These risks may be on account of internal or external factors and may impact concrete assets like financial or physical assets or intangible assets like knowledge, skills, and reputation. Risk identification requires that clear goals/objectives be defined and then the threats (risks) that may hinder achievement of these goals be identified and analyzed.

The focus of the risk assessment process is two fold:

- (i) What is the probability that the risk will materialize i.e. something will go wrong?
- (ii) What is the impact if the untoward event happens?

The greater the probability of occurrence and higher the impact, the larger will be the share of resources assigned to manage the element of risk. The probability of occurrence of a negative event is influenced by other elements of internal control such as integrity and ethical values of the personnel, competence of staff, information and communication system etc. The more effective each component is the lower is the probability of occurrence of a negative event. Thus the close interrelationship among the elements of internal control holds for Risk Assessment also, for example good Risk Assessment requires a good information and communication system. Once the risks are identified and assessed, control activities are instituted to manage the risks and monitoring must be introduced to ensure that system is working as required.

After identification and assessment of risks, management has to decide among any or more of the following four responses to address the risk:

- (a) Transfer the risk, say buy insurance to cover for the risk of failure in a satellite launch; protect the organization from sudden cost escalations through appropriate clauses in the contracts.
- (b) Tolerate the risk, and take no steps to mitigate the risk i.e. accept the negative consequences. This may be done when the cost of managing risk outweighs benefits or when the risk is unavoidable.
- (c) Terminate the risk, by ending the activity, e.g. a tourism company that also runs beer shops closes them on finding that the managers are focusing on beer sale to the detriment of the main business objective of catering and hotel management. However, such responses may not be always possible for government organizations.
- (d) Manage risk, through introduction of appropriate control procedures and activities; this is by far the most common response.

Risk management can help Government departments to improve their performance in a number of ways by way of better service delivery, more efficient use of resources, better project management, minimizing waste, fraud and poor value for money.

Risk management may also involve devising an innovative response to address challenges, especially where the cost or downside of not taking a risk may involve foregoing an opportunity to make significant gains. As change is a normal feature of the environment in which Government departments operate failure to innovate suitably may be a serious risk to the reputation and credibility of government. This caveat is necessary especially in the case of Government entities and managers who are generally considered 'risk averse'.

Pitfalls of Inappropriate Risk management in Government

Risk management primarily designed to limit liability or avoid blame to particular public organizations could encourage public organizations to shuffle blame onto others. Such risk displacement practices may result in the greatest exposure to risk being borne by organizations that are politically weakest rather than those best placed (through knowledge or resource access) to assume responsibility for risk. There should be an emphasis on overall problem-solving instead of blame-shifting by developing procedures to bring in a cross-organisational focus or 'getting the whole system in a room'.

Public organizations often respond to changes in their environment by applying new procedures in ways that reflect what is readily do-able or protects existing operations. For instance, government officials have a tendency to stick to procedural rules that may be ill-adapted to particular real-life problems. Risk management may then be used a convenient excuse for policy inaction, administrative rigidity and even corruption. This may defeat the generally perceived role of Government as risk-bearers of the last resort.

Inappropriate risk management in government may undermine other public sector values like openness, transparency and learning from experience. There may be a tendency to restrict public or auditor access to information about errors or malfeasance. This would defeat the basic tenets of 'good governance'

Information and Communications

For an entity to run and control its operations, it must have relevant, reliable, and timely communications relating to internal as well as external events. Information is needed throughout the department to achieve all of its objectives.

Program managers need both operational and financial data to determine whether they are meeting their agencies' strategic and annual performance plans and meeting their goals for accountability for effective and efficient use of resources. For example, operating information is required for development of financial reports. This covers a broad range of data from purchases, subsidies, and other transactions to data on fixed assets, inventories, and receivables. Operating information is also needed to determine whether the department is achieving compliance requirements under various laws and regulations. Financial information is needed for both external and internal uses. It is required to develop financial statements for periodic external reporting, and, on a day-to-day basis, to make operating decisions, monitor performance, and allocate

resources. Pertinent information should be identified, captured, and distributed in a form and time frame that permits people to perform their duties efficiently.

Effective communications should occur in a broad sense with information flowing down, across, and up the organization. In addition to internal communications, management should ensure there are adequate means of communicating with, and obtaining information from, external stakeholders that may have a significant impact on the department achieving its goals. Moreover, effective information technology management is critical to achieving useful, reliable, and continuous recording and communication of information.

Monitoring

Internal control should generally be designed to assure that ongoing monitoring occurs in the course of normal operations. It is performed continually and is ingrained in the department's operations. It includes regular management and supervisory activities, comparisons, reconciliations, and other actions people take in performing their duties.

Separate evaluations of control can also be useful by focusing directly on the controls' effectiveness at a specific time. The scope and frequency of separate evaluations should depend primarily on the assessment of risks and the effectiveness of ongoing monitoring procedures. Separate evaluations may take the form of self-assessments as well as review of control design and direct testing of internal control. Separate evaluations also may be performed by the department internal auditor or an external auditor. Deficiencies found during ongoing monitoring or through separate evaluations should be communicated to the individual responsible for the function and also to at least one level of management above that individual. Serious matters should be reported to top management.

Monitoring of internal control should include policies and procedures for ensuring that the findings of audits and other reviews are promptly resolved. Managers are to (1) promptly evaluate findings from audits and other reviews, including those showing deficiencies and recommendations reported by auditors and others who evaluate agencies' operations, (2) determine proper actions in response to findings and recommendations from audits and reviews, and (3) complete, within established time frames, all actions that correct or otherwise resolve the matters brought to management's attention. The resolution process begins when audit or other review results are reported to management, and is completed only after action has been

taken that (1) corrects identified deficiencies, (2) produces improvements, or (3) demonstrates the findings and recommendations do not warrant management action.

Control Activities

Control activities are the policies, procedures, techniques, and mechanisms that enforce management's directives, such as the process of adhering to requirements for budget development and execution. They help ensure that actions are taken to address risks. Control activities are an integral part of an entity's planning, implementing, reviewing, and accountability for stewardship of government resources and achieving effective results.

Control activities occur at all levels and functions of the entity. They include a wide range of diverse activities such as approvals, authorizations, verifications, reconciliations, performance reviews, maintenance of security, and the creation and maintenance of related records which provide evidence of execution of these activities as well as appropriate documentation. Control activities may be applied in a computerized information system environment or through manual processes.

Activities may be classified by specific control objectives, such as ensuring completeness and accuracy of information processing.

Examples of Control Activities

There are certain categories of control activities that are common to all agencies.

Examples include the following:

- Top Level Reviews of actual performance
- Management should track major department achievements and compare these to the plans, goals, and objectives established under the Government Performance and Results Act.
- Reviews by Management at the Functional or Activity Level
- Managers also need to compare actual performance to planned or expected results throughout the organization and analyze significant differences.

Management of Human Resources

Effective management of an organization's workforce is essential to achieving results and an important part of internal control. Management should view human resources as an asset rather than a cost. Only when the right personnel for the job are on board and are provided the right training, tools, structure, incentives, and responsibilities is operational success possible. Management should ensure that skill needs are continually assessed and that the organization is able to obtain a workforce that has the required skills that match those necessary to achieve organizational goals. Training should be aimed at developing and retaining employee skill levels to meet changing organizational needs. Qualified and continuous supervision should be provided to ensure that internal control objectives are achieved. Performance evaluation and feedback, supplemented by an effective reward system, should be designed to help employees understand the connection between their performance and the organization's success. As a part of its human resource planning, management should also consider how best to retain valuable employees, plan for their eventual succession, and ensure continuity of needed skills and abilities.

Controls over Information Processing

A variety of control activities are used in information processing. Examples include edit checks of data entered, accounting for transactions in numerical sequences, comparing file totals with control accounts, and controlling access to data, files, and programs.

Physical Control over Vulnerable Assets

A department must establish physical control to secure and safeguard vulnerable assets. Examples include security for and limited access to assets such as cash, securities, inventories, and equipment which might be vulnerable to risk of loss or unauthorized use. Such assets should be periodically counted and compared to control records.

Establishment and Review of Performance Measures and Indicators

Activities need to be established to monitor performance measures and indicators. These controls could call for comparisons and assessments relating different sets of data to one another so that analyses of the relationships can be made and appropriate actions taken. Controls should also be aimed at validating the propriety and integrity of both organizational and individual performance measures and indicators.

Segregation of Duties

Key duties and responsibilities need to be divided or segregated among different people to reduce the risk of error or fraud. This should include separating the responsibilities for authorizing transactions, processing and recording them, reviewing the transactions, and handling any related assets. No one individual should control all key aspects of a transaction or event.

Proper Execution of Transactions and Events

Transactions and other significant events should be authorized and executed only by persons acting within the scope of their authority. This is the principal means of assuring that only valid transactions to exchange, transfer, use, or commit resources and other events are initiated or entered into. Authorizations should be clearly communicated to managers and employees.

Accurate and Timely Recording of Transactions and Events

Transactions should be promptly recorded to maintain their relevance and value to management in controlling operations and making decisions. This applies to the entire process or life cycle of a transaction or event from the initiation and authorization through its final classification in summary records. In addition, control activities help to ensure that all transactions are completely and accurately recorded.

Access Restrictions to and Accountability for Resources and Records

Access to resources and records should be limited to authorized individuals, and accountability for their custody and use should be assigned and maintained. Periodic comparison of resources with the recorded accountability should be made to help reduce the risk of errors, fraud, misuse, or unauthorized alteration.

Appropriate Documentation of Transactions and Internal Control

Internal control and all transactions and other significant events need to be clearly documented, and the documentation should be readily available for examination. The documentation should appear in management directives, administrative policies, or operating manuals and may be in paper or electronic form. All documentation and records should be properly managed and maintained.

These examples are meant only to illustrate the range and variety of control activities that may be useful to department managers. They are not all-inclusive and may not include particular control activities that an department may need.

Furthermore, an department's internal control should be flexible to allow agencies to tailor control activities to fit their special needs. The specific control activities used by a given department may be different from those used by others due to a number of factors. These could include specific threats they face and risks they incur; differences in objectives; managerial judgment; size and complexity of the organization; operational environment; sensitivity and value of data; and requirements for system reliability, availability, and performance.

Control Activities Specific for Information Systems

- General Control
- Application Control

There are two broad groupings of information systems control - general control and application control. General control applies to all information systems—mainframe, minicomputer, network, and end-user environments. Application control is designed to cover the processing of data within the application software.

General Control This category includes department - wide/ organization- wide security program planning, management, control over data center operations, system software acquisition and maintenance, access security, and application system development and maintenance. More specifically:

- Data center and client-server operations controls include backup and recovery procedures, and contingency and disaster planning. In addition, data center operations controls also include job set-up and scheduling procedures and controls over operator activities.
- System software control includes control over the acquisition, implementation, and maintenance of all system software including the operating system, data-based management systems, telecommunications, security software, and utility programs.
- Access security control protects the systems and network from inappropriate access and unauthorized use by hackers and other trespassers or inappropriate use by organization's personnel. Specific control activities include frequent changes of dial-up numbers; use of dial-back access; restrictions on users to allow access only to system functions that they need; software and hardware "firewalls" to restrict access to assets, computers, and networks by external persons; and frequent changes of passwords and deactivation of former employees' passwords.

- Application system development and maintenance control provides the structure for safely developing new systems and modifying existing systems. Included are documentation requirements; authorizations for undertaking projects; and reviews, testing, and approvals of development and modification activities before placing systems into operation. An alternative to in-house development is the procurement of commercial software, but control is necessary to ensure that selected software meets the user's needs, and that it is properly placed into operation.

Application Control

This category of control is designed to help ensure completeness, accuracy, authorization, and validity of all transactions during application processing. Control should be installed at an application's interfaces with other systems to ensure that all inputs are received and are valid and outputs are correct and properly distributed. An example is computerized edit checks built into the system to review the format, existence, and reasonableness of data.

General and application control over computer systems is interrelated. General control supports the functioning of application control, and both are needed to ensure complete and accurate information processing. If the general control is inadequate, the application control is unlikely to function properly and could be overridden.

Because information technology changes rapidly, controls must evolve to remain effective. Changes in technology and its application to electronic commerce and expanding Internet applications will change the specific control activities that may be employed and how they are implemented, but the basic requirements of control will not have changed. As more powerful computers place more responsibility for data processing in the hands of the end users, the needed controls should be identified and implemented

APPENDIX II

Considering Whether Fraud Is Significant To the Audit Objectives

Fraud is a type of illegal act that involves obtaining something of value through willful misrepresentation.

The audit party should answer the following question as part of the audit party's consideration of the risk due to fraud that could significantly affect their audit objectives and the results of their audit.

<p>Consideration of Risk Due to Fraud</p>	<p>If yes, the risk of fraud is relevant, and potentially significant to the audit objectives.</p>
<p>Has the auditor identified that the program or activity covered by the audit objectives is susceptible to a significant risk of fraud from</p> <ul style="list-style-type: none"> • Intentional misappropriation or misuse of program assets, or • Intentional misstatement or misrepresentation of program information or results in order to obtain or continue receiving government funding or benefits. 	<p>Y N</p>

<p>Has the team identified indications that specific fraud risk factors could significantly affect answers to the key questions for the audit?</p> <p>Weak management that fails to enforce existing internal control or provide adequate supervision over the control processes;</p> <p>Inadequate separation of duties, especially those that relate to controlling and safeguarding resources;</p> <p>Transactions that are out of the ordinary and are not satisfactorily explained, such as unexplained adjustment in performance or financial information;</p> <p>Instances when employees of the program refuse to take vacations or accept promotions;</p> <p>Missing or altered documents, or unexplained delay in providing information;</p> <p>False or misleading information; or</p> <p>A history of impropriety, revealed by past audits or investigations with findings of questionable or criminal activity.</p>	<p>Y N</p>
--	---------------

Considering Whether Abuse Is Significant To the Audit Objectives

Abuse involves behavior that is deficient or improper when compared with behavior that a prudent person would consider reasonable and necessary business practice given the facts and circumstances. There is frequently a fine line between abuse and fraud, and

many of the considerations for fraud would also apply in situations of abuse or potential abuse.

The auditors should answer the following question to determine whether the team should extend audit procedure to determine if abuse has occurred and to determine potential effects on audit results.

	Yes	No
Has the audit party encountered any indication of abuse that relates to the key questions of the audit?	<input type="checkbox"/>	<input type="checkbox"/>

Impact of the abuse on Audit: If the audit party answers this question “yes”, the auditor should consider whether the possible abuse affects the results of the audit significantly. If indications of abuse exists that significantly affect the audit results, the auditor should extend the audit procedures as necessary to (1) determine whether the abuse has occurred and, if so, (2) determine its effect on the audit results

Documenting the impact of abuse on the Audit: In completing the Design Matrix the audit party should identify those aspects of our planned work (i.e. the nature, timing, and extent of procedures) that are impacted by the auditor’s consideration of abuse in relation to the audit objectives. This may be accomplished by citing in the design Matrix the specific aspect of the planned work that relates to abuse. Alternatively, audit teams may document in a brief planning memo their impact on the nature, timing and extent of audit procedures.

Changing mindset towards frauds

The contemporary global environment relating to 'frauds' is characterized by a decided shift from compliance-driven identification and investigation of incidents to a proactive prevention and detection embedded into an organisation's internal controls. The COSO framework of control environment, risk assessment, control activities, information and communications, and monitoring can be applied to the evaluation of antifraud programmes and controls. Of all the players in the financial reporting chain, internal audit has a critical role in putting into operation the new emphasis on fraud prevention and detection. As SAI we have the responsibility of catalyzing this process through our audit recommendations. This could also be done by an audit of the Vigilance function, which is usually present in all major public organisations.