No.35-IR/2001
5th April, 2006

Dear Colleagues,

Please find attached a brief on the INTOSAI Guidelines for the 'Internal Control Standards for the Pubic Sector' for your reference. The full document may be seen at www.intosai.org under "sub-committee on Internal Control Standards" of the "Professional Standards Committee".

With regards,

Yours sincerely,

Khalid Jamal

A brief on the INTOSAI Guidelines for the Internal Control Standards for the Public Sector

1.1 Definition

Internal control is an integral process that is effected by an entity's management and personnel and is designed to address risks and to provide reasonable assurance that in pursuit of the entity's mission, the following general objectives are being achieved:

- executing orderly, ethical, economical, efficient and effective operations;
- fulfilling accountability obligations;
- complying with applicable laws and regulations;
- safeguarding resources against loss, misuse and damage.

Management and personnel at all levels have to be involved in this process to address risks and to provide reasonable assurance of the achievement of the entity's mission and general objectives.

1.2 Limitations on Internal Control Effectiveness

Internal control cannot by itself ensure the achievement of the general objectives defined earlier. An effective internal control system, no matter how well conceived and operated, can provide only reasonable – not absolute – assurance to management about the achievement of an entity's objectives or its survival. An effective system of internal control reduces the probability of not achieving the objectives. Because internal control depends on the human factor, it is subject to flaws in design, errors of judgment or interpretation, misunderstanding, carelessness, fatigue, distraction, collusion, abuse or override. The design of an internal control system faces resource constraints. The benefits of controls must consequently be considered in relation to their costs. The management needs to continually review and update controls, communicate changes to personnel and set an example by adhering to those controls.

2 Components of Internal Control

Internal control consists of five interrelated components:

-control environment
- risk assessment
- control activities
- information & communication
- monitoring.

2.1 Control Environment

The control environment sets the tone of an organization, influencing the control consciousness of its staff. It is the foundation for all other components of internal control, providing disciplne and structure.

Elements of the control environment are:

(1) the personal and professional integrity and ethical values of management and staff, including a supportive attitude toward internal control at all times throughout the organization

Every person involved in the organisation—among managers and employees—has to maintain and demonstrate personal and professional integrity and ethical values and has to comply with the applicable codes of conduct at all times. Public organizations have to maintain and demonstrate integrity and ethical values,and they should make those visible to the public in their mission and core values.

(2) commitment to competence

Managers and employees are to maintain a level of competence that allows them to understand the importance of developing, implementing, and maintaining good internal control and to perform their duties in order to accomplish the general internal control objectives and the entity's mission. Managers and their staffs must therefore maintain and demonstrate a level of skill necessary to assess risk and help ensure effective and efficient performance, and an understanding of internal control sufficient to effectively discharge their responsibilities.

(3) the "tone at the top" (i.e. management's philosophy and operating style)

The "tone at the top" reflects – a supportive attitude toward internal control at all times, independence, competence and leading by example ; a code of conduct set out by management, and counseling and performance appraisals that support the internal control objectives and in particular, that of ethical operations. If top management believes that internal control is important, others in the organisation will sense that and will respond by conscientiously observing the controls established.

(4) organisational structure

The organisational structure of an entity provides: assignment of authority and responsibility; empowerment and accountability; appropriate lines of reporting. The organisational structure defines the entity's key areas of authority and responsibility. Empowerment and accountability relate to the manner in which this authority and responsibility are delegated throughout the organisation. There can be no empowerment or accountability without a form of reporting. Therefore, appropriate lines of reporting need to be defined

(5) human resource policies and practices.

Human resource policies and practices include hiring and staffing, orientation, training (formal and on-the-job) and education, evaluating and counselling, promoting and compensating, and remedial actions. An important aspect of internal control is personnel. Competent, trustworthy personnel are necessary to provide effective control. Therefore, the methods by which persons are hired, trained, evaluated, compensated, and promoted, are an important part of the control environment. Managers and employees who have a good understanding of internal control and are willing to take responsibility, are vital to effective internal control. Human resource management promotes an ethical environment by developing professionalism and enforcing transparency in daily practice. This becomes visible in recruitment, performance appraisal and promotion processes.

2.2 Risk Assessment

Risk assessment is the process of identifying and analysing relevant risks to the achievement of the entity's objectives and determining the appropriate response.
It implies:

(1) risk identification: related to the objectives of the entity; comprehensive; includes risks due to external and internal factors, at both the entity and the activity levels

A strategic approach to risk assessment depends on identifying risks against key organisational objectives. Risks relevant to those objectives are then considered and evaluated, resulting in a small number of key risks. This is also important to allocate responsibility for management of these risks. The risk assessment should consider all risks that might occur (including the risk of fraud and corruption). It is therefore important that risk identification is comprehensive. Risk identification should be an ongoing, iterative process and is often integrated with the planning process. It is often useful to consider risk from a 'clean sheet of paper' approach, and not merely realte it to the previous review. It is necessary to adopt appropriate tools for the identification of risk. Two of the most commonly used tools are commissioning a risk review and a risk self assessment

(2) risk evaluation: estimating the significance of a risk; assessing the likelihood of the risk occurrence

In order to decide how to handle risk, it is essential not only to identify in principle that a certain type of risk exists, but also to evaluate its significance and assess the likelihood of the risk event occurring. The methodology for analysing risks can vary, largely because many risks are difficult to quantify (e.g. reputation risks) while others lend themselves to a numerical diagnosis (particularly financial risks). For the former, a much more subjective view is the only possibility. In this sense, risk evaluation is more of an art than a science. However, the use of systematic risk rating criteria will mitigate the subjectivity of the process by providing a framework for judgements to be made in a consistent manner. One of the key purposes of risk evaluation is to inform management about areas of risk where action needs to be taken and their relative priority. Therefore, it will usually be necessary to develop some framework for categorising all risks, for example, as high, medium, or low.

(3) assessment of the risk appetite of the organization

Risk appetite is the amount of risk to which the entity is prepared to be exposed before it judges action to be necessary. Both inherent and residual risks need to be considered to determine the risk appetite.The risk appetite of an organisation will vary according to the perceived importance of the risks. For example, tolerable financial loss may vary in accordance with a range of features, including the size of the relevant budget, the source of the loss, or associated other risks such as adverse publicity. Identification of risk appetite is a subjective issue, but it is nevertheless an important stage in formulating the overall risk strategy.

(4) *development of responses: four types of responses to risk must be considered: transfer, tolerance, treatment or termination; of these, risk treatment is the most relevant to these guidelines because effective internal control is the major mechanism to treat risk; the appropriate controls involved can be either detective or preventive.*

The result of the actions outlined above will be a risk profile for the organisation. Having developed a risk profile, the organisation can then consider an appropriate response. In some instances the risk can be transferred, tolerated or terminated. However in most cases the risk will have to be treated and the entity will need to implement and maintain an effective internal control system to keep risk at an acceptable level. The procedures that an organisation establishes to treat risk are called internal control activities. In designing an internal control system, it is important that the control activity established is proportionate to the risk. Apart from the most extreme undesirable outcome, it is normally sufficient to design a control that provides a reasonable assurance of confining loss within the risk appetite of the organisation. Every control has an associated cost and the control activity must offer value for its cost in relation to the risk that it is addressing.

As governmental, economic, industry, regulatory and operating conditions are in constant change, risk assessment should be an ongoing iterative process. It implies identifying and analysing altered conditions and opportunities and risks (risk assessment cycle) and modifying internal control to address changing risk.

2.3 Control Activities

Control activities are the policies and procedures established to address risks and to achieve the entity’s objectives.

To be effective, control activities need to be appropriate (that is, the right control in the right place and commensurate risks involved); function consistently according to plan throughout the period (that is, be complied w ith carefully by all employees involved and not bypassed when key personnel are away or the workload is heavy); be cost effective, comprehensive, reasonable and directly relate to the control objectives.

Control activities include a range of detective and preventive control activities as diverse, for example, as:

(1) authorization and approval procedures

Authorization is the principal means of ensuring that only valid transactions and events are initiated as intended by management. Authorization procedures, which should be documented and clearly communicated to managers and employees, should include the specific conditions and terms under which authorizations are to be made.

(2) segregation of duties (authorizing, processing, recording, reviewing)

To reduce the risk of error, waste, or wrongful acts and the risk of not detecting such problems, no single individual or team should control all key stages of a transaction or event. Duties and responsibilities should be assigned systematically to a number of individuals to ensure that effective checks and balances exist. Key duties include authorizing and recording transactions, processing, and reviewing or auditing transactions. Rotation of employees may help ensure that one person does not deal with all the key aspects of transactions or events for an undue length of time.

(3) controls over access to resources and records

Access to resources and records is limited to authorized individuals who are accountable for the custody and/or use of the resources. Accountability for custody is evidenced by the existence of receipts, inventories, or other records assigning custody and recording the transfer of custody. Restricting access to resources reduces the risk of unauthorized use or loss to the government and helps achieve management directives. When determining an asset's vulnerability, its cost, portability and exchangeability should be considered.

(4) verifications
Transactions and significant events are verified before and after processing, e.g. when goods are delivered, the number of goods supplied is verified with the number of goods ordered. Afterwards, the number of goods invoiced is verified with the number of goods received. The inventory is verified as well by performing stock-takes.

(5) reconciliations
Records are reconciled with the appropriate documents on a regular basis, e.g. the accounting records relating to bank accounts are reconciled with the corresponding bank statements

(6) reviews of operating performance
Operating performance is reviewed against a set of standards on a regular basis, assessing effectiveness and efficiency.

(7) reviews of operations, processes and activities
Operations, processes and activities should be periodically reviewed to ensure that they are in compliance with current regulations, policies, procedures, or other requirements.

(8) supervision (assigning, reviewing and approving, guidance and training).
Competent supervision helps to ensure that internal control objectives are achieved. Assigning, reviewing, and approving an employee's work encompasses: clearly communicating the duties, responsibilities and accountability assigned to each staff member; systematically reviewing each member's work to the extent necessary; and approving work at critical points to ensure that it flows as intended.

Entities should reach an adequate balance between detective and preventive control activities. Corrective actions are a necessary complement to control activities in order to achieve the objectives.

2.3.1 Information Technology Control Activities

Information systems imply specific types of control activities. Therefore information technology controls consist of two broad groupings: (1) General controls and (2) application controls

(1) General Controls
General controls are the structure, policies and procedures that apply to all or a large segment of an entity's information systems - such as mainframe, minicomputer, network, and end-user environments - and help ensure their proper operation. They create the environment in which application systems and controls operate. The major categories of general controls are: (i) entity wide security program planning and management (ii) access controls (iii) Controls on the development, maintenance and change of application software (iv) System software controls (v) Segregation of duties and (6) Service continuity

(2) Application Controls

Application controls are the structure, policies, and procedures that apply to separate, individual application systems - such as accounts payable, inventory, payroll, grants, or loans - and are designed to cover the processing of data within specific applications software. These controls are generally designed to prevent, detect, and correct errors and irregularities as information flows through information systems. Application controls and the manner in which information flows through information systems can be categorized into three phases of a processing cycle: input, processing and output.

General and application controls over computer systems are interrelated and both are needed to help ensure complete and accurate information processing. The effectiveness of general controls is a significant factor in determining the effectiveness of application controls. While the basic objectives of control do not change, rapid changes in information technology require that controls evolve to remain effective.

2.4 Information and Communication

Information and communication are essential to realising all internal control objectives.

Information is needed at all levels of the organization in order to have effective internal control and achieve the entity's objective. The information should be appropriate, timely, current, accurate, and accessible. A precondition for reliable and relevant information is the prompt recording and proper classification of transactions and events. Pertinent information should be identified, captured and communicated in a form and timeframe that enables staff to carry out their internal control and other responsibilities (timely communication to the right people). Therefore, the internal control system as such and all transactions and significant events should be fully documented.

Effective communication should flow down, across, and up the organisation, throughout all components and the entire structure. All personnel should receive a clear message from top management that control responsibilities should be taken seriously. One of the most critical communications channels is between the staff and the management. Communication should raise the awareness about the importance of internal control, communicate the entity's risk appetite and risk tolerances and make the personnel aware of their own role in the internal control system, as well as how their individual activities relate to the work of others. There also needs to be effective communication with external parties.

2.5 Monitoring

Monitoring internal control is aimed at ensuring that controls are operating as intended and that they are modified appropriately for changes in conditions. This is accomplished through ongoing monitoring activities, separate evaluations or a combination of both.

Ongoing monitoring of internal control is built into the normal, recurring operating activities of an entity. It includes regular management and supervisory activities, and other actions personnel take in performing their duties. Ongoing monitoring activities cover each of the internal control components and involve action against irregular, unethical, uneconomical, inefficient and ineffective internal control systems.

The scope and frequency of separate evaluations will depend primarily on an assessment of risks and the effectiveness of ongoing monitoring procedures. Specific separate evaluations cover the evaluation of the effectiveness of the internal control system and ensure that internal control achieves the desired results based on predefined methods and procedures. Internal control deficiencies should be reported to the appropriate level of management.

All deficiencies found during monitoring should be communicated to those positioned to take necessary action. Deficiency may present a perceived, potential or real short coming or an opportunity to strengthen internal control. Monitoring should ensure that audit findings and recommendations are adequately and promptly resolved.

3 Roles and Responsibilities

Everyone in an organisation has some responsibility for internal control.

Managers are directly responsible for all activities of an organisation, including designing, implementing, supervising proper functioning of, maintaining and documenting the internal control system. Their responsibilities vary depending on their function in the organisation and the organisation's characteristics.

Internal auditors examine and contribute to the ongoing effectiveness of the internal control system through their evaluations and recommendations and therefore play a significant role in effective internal control. However they do not have management's primary responsibility for designing, implementing, maintaining and documenting internal control.

Staff members contribute to internal control as well. Internal control is an explicit or implicit part of everyone's duties. All staff members play a role in effecting control and should be responsible for reporting problems of operations, non-compliance with the code of conduct, or violations of policy.

External parties also play an important role in the internal control process. They may contribute to achieving the organisation's objectives, or may provide information useful to effect internal control. However, they are not responsible for the design, implementation, proper functioning, maintenance or documentation of the organisation's internal control system.

Supreme Audit Institutions (SAIs) encourage and support the establishment of effective internal control in the government. The assessment of internal control is essential to the SAI's compliance, financial and performance audits. They communicate their findings and recommendations to interested stakeholders. Auditors' assessment of internal control implies determining the significance and the sensitivity of the risk for which controls are being assessed; assessing the susceptibility to misuse of resources, failure to attain objectives regarding ethics, economy, efficiency and effectively, or failure to fulfill accountability obligations, and non-compliance with laws and regulations; identifying and understanding the relevant controls; determining what is already known about control effectiveness; assessing the adequacy of the control design; determining, through testing, if controls are effective; reporting on the internal control assessments and discussing the necessary corrective actions.

The SAI also needs to develop a good working relationship with the internal audit units so that experience and knowledge can be shared and work mutually can be supplemented and complemented. The SAI should develop procedures for assessing the internal audit unit's work to determine to what extent it can be relied upon. A strong internal audit unit could reduce the audit work of the SAI and avoid needless duplication of work. In countries where internal audit lacks independence, is weak or non-existent, the SAI should, whenever possible offer guidance and assistance. SAIs should also play a leadership role for the rest of the public sector by establishing their own organisation’s internal control framework in a manner consistent with the principles set out in this guideline.

External auditors audit certain government organisations in some countries. They and their professional bodies should provide advice and recommendations on internal control.

Legislators and regulators establish rules and directives regarding internal regulators control. They should contribute to a common understanding of internal control.

Other parties interact with the organisation (beneficiaries, suppliers, etc.) and provide information regarding achievement of its objectives.