# Chapter-5

## INTERNAL CONTROL STANDARDS

### 5.01 Internal Control

### 5.01.01 Definition

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

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

Internal control is a dynamic integral process that is being continuously adapted to the changes an organisation is facing. Management and personnel at all levels have to be involved in this process to provide reasonable assurance of the achievement of the objectives.

**An Integral process**

Internal control is not an event or circumstance, but a series of actions that permeate an entity's activities. These actions occur throughout an entity's operations on an ongoing basis. They are pervasive and inherent in the way the management runs the organisation. Internal control is therefore different from the perspective of observers who view it either as something added on to an entity's activities, or as a necessary burden. The internal control system is intertwined with an entity's activities and is most effective when it is built into the entity's infrastructure and is an integral part of the essence of the organisation. Internal control should be built in rather than built on. By building in internal control, it becomes part of and integrated within the basic management processes of planning, executing and monitoring. Built in internal control also has important implications for cost containment. Adding new procedures that are separate from existing operations and their contribution to effective internal control, and by integrating controls into basic operating activities, an organisation often can avoid unnecessary procedures and costs.

**Effected by management and other personnel**

People are what make internal control work. It is accomplished by individuals within an organisation, by what they do and say. Consequently, internal control is effected by people. People must know their roles and responsibilities, and limits of authority.

An organisation's people include the management and other personnel. Although the management primarily provides oversight, they also set the entity's objectives and have overall responsibility for the internal control system. As internal control provides the mechanisms needed to help understand risk in the context of the entity's objectives, the management will put internal control activities in place and monitor and evaluate them. Therefore, internal control is a tool used by the management and directly related to the entity's objectives. Such management is an important element of internal control. However, all personnel in the organisation play important roles in making it happen.

Similarly, internal control is affected by human nature. Internal control guidelines recognize that people do not always understand, communicate or perform consistently. Each individual brings to the workplace a unique background and technical ability, and has different needs and priorities. These realities affect, and are affected by, internal control.

### Provides reasonable assurance

No matter how were designed and operated, internal control cannot provide management absolute assurance regarding the achievement of an entity's objectives.

Reasonable assurance equates to a satisfactory level of confidence under given considerations of costs, benefits and risks. Determining how much assurance is reasonable, requires judgment. In exercising that judgment, managers should identify the risks inherent in their operations and the acceptable levels of risk under varying circumstances, and assess risk both quantitatively and qualitatively.

Reasonable assurance reflects the notion that uncertainty and risk relate to the future, which no one can predict with certainty. Also factors outside the control or influence of the organisation can affect the ability to achieve the objectives. Limitations also result from the following realities: human judgment in decision making can be faulty; breakdowns can occur because of simple errors or mistakes; controls can be circumvented by collusion of two or more people; management can override the internal control system; and decisions on risk responses and establishing controls need to consider the relative costs and benefits. These limitations preclude management from having absolute assurance that objectives will be achieved.

Reasonable assurance recognizes that the cost of internal control should not exceed the benefit derived. Cost refers to the financial measure of resources consumed in accomplishing a specified purpose and to the economic measure of a last opportunity, such as a delay in operations, a decline in service levels or productivity, or low employee morale. A benefit is measured by the degree to which the risk of failing to achieve a stated objective is reduced. Examples include increasing the probability of detecting fraud, waste, abuse, or error; preventing an improper activity; or enhancing regulatory compliance.

Designing internal controls that are cost beneficial while reducing risk to an acceptable level requires that managers clearly understand the overall objectives to be achieved. Government managers may design systems with excessive controls in one area of their operations that adversely affect other operations. For example, employees may try to circumvent burdensome procedures, inefficient operations may cause delays, excessive procedures may stifle employee creativity and problem solving or impair the timeliness, cost or quality of services provided to beneficiaries. Thus, benefits derived from excessive controls in one area may be outweighed by increased costs in other activities.

### Achievement of objectives

Internal control is geared to the achievement of a separate but interrelated series of general

entity level objectives. These general objectives are through numerous specific sub-objectives, functions, processes, and activities.
The general objectives are fulfilling accountability obligations Accountability is the process whereby public service bodies and the individuals within them are held to account for their decisions and actions, including their stewardship of public funds, fairness, and all aspects of performance.
This will be realized by developing and maintaining reliable and relevant financial and non-financial information and by means of a fair disclosure of that information in timely reports to internal as well as external stakeholders.
Non-financial information may relate to the economy, efficiency and effectiveness of policies and operations (performance information), and to internal control and its effectiveness.

- **Complying with laws and regulations**

Organisations are required to follow many laws and regulations Examples include the Budget Act. international treaties laws on proper administration, accounting law environmental protection and civil rights law income tax regulations and anti-fraud and corruption acts.

- **Executing orderly ethical, economical, efficient and effective operations.**

The entity's operations should be orderly, ethical, economical, efficient and effective. They have to be consistent with the organisation’s mission.

- **Orderly means in a well organised way, methodically**.

Economical means not wasteful or extravagant. It means getting the right amount of resources, of the right quality, delivered at the right time and place, at the lowest cost.
Effective refers to the accomplishment of objectives or to the extent to which the outcomes of an activity match the objective or the intended effects of that activity.

Efficient refers to the resources used to achieve the objectives. It means the minimum resource inputs to achieve a given quantity and quality of output, or a maximum output with a given quantity and quality of resource inputs.

Ethical relates to moral principles. The importance of ethical behavior and prevention and detection of fraud and corruption in the public sector has become more emphasized since the nineties. General expectations are that public servants should serve the public interest with fairness and manage public resources properly. Citizens should receive impartial treatment on the basis of legality and justice. Therefore, public ethics are a prerequisite to, and underpin public trust and are a keystone of good governance.

- **Safeguarding resources against loss due to waste abuse, mismanagement errors fraud and irregularities.**

Although the fourth objective can be viewed as a subcategory of the third one (orderly, ethical economical, efficient and effective operations), the significance of safeguarding the resources in the public sector needs to be stressed. This is due to the fact that budgetary accounting or accounting on a cash basis, which is still widespread in the public sector, does not provide sufficient assurance related to the maintenance of records of the resources. As a result, the organisations in the public sector do not always have a record of all their assets, which makes them more vulnerable. Therefore, controls should be embedded in each of the activities related to the management of resources of the entity, from the entry until the disposition.

Other resources such as information, source documents and accounting records are also in danger of being stolen, misused or accidentally destroyed. Safeguarding certain resources and records has become increasingly important since the arrival of computer systems. Sensitive information stored on computer media can be destroyed or copied, distributed and abused if care is not taken to protect it.

### 5.01.02 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. It can give the management information about the entity's progress, or lack of it, toward the achievement of the objectives. But internal control cannot change an inherently poor manager into a good one. Moreover, shifts in government policy or programs. demographic or economic conditions are typically beyond management's control.

An effective system of internal control reduces the probability of not achieving the objectives. However, there will always be the risk that internal controls fail to operate as designed.
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.

Another limiting factor is that the design or an internal control system faces resource constraints. The benefits of controls must consequently be considered in relation to their costs. Maintaining an internal control system that eliminates the risk of loss is not realistic and would probably cost more than is warranted by the benefit derived. In determining whether a particular control should be established, the likelihood of the risk occurring and the potential effect on the entity are considered along with the related costs of establishing a new control.
The limitations on internal control effectiveness need to be stressed to avoid exaggerated expectations due to a misunderstanding of its effective scope.

Organisational changes and management attitude can have a profound impact on the effectiveness of internal control and the personnel operating the system. Thus, management needs to continually review and update controls, communicate changes to personnel, and set an example by adhering to those controls.

## 5.02 Components of internal control

Internal control consists of five interrelated components

- control environment
- risk assessment
- control activities
- information and communication
- Monitoring

Internal control is designed to provide reasonable assurance that the entity's general objectives are being achieved. Therefore, clear objectives are a prerequisite for an effective internal control process.

The control environment is the foundation for the entire internal control system. It provides the discipline and structure as well as the climate which influences the overall quality of internal control. It has overall influences on how strategy and objectives are established and control activities are structured.

Having set clear objectives and established and effective control environment an assessment of the risks facing the entity as it seeks to achieve its objectives provides the basis for developing and appropriate response to risk.

The major strategy for mitigating risk is through internal control activities. Corrective actions are a necessary complement to internal control activities in order to achieve the objectives. Control activities and corrective actions should provide value for money. Their cost should not exceed the benefit resulting from them (cost effectiveness).

Effective information and communication is vital for an entity to run and control its operations. Entity management needs access to relevant, reliable, timely communication related to internal as well as external events. Information is needed throughout the entity to achieve its objectives.

Finally, since internal control is a dynamic process that has to be adapted continuously to the risks and changes an organisation faces. Monitoring of the internal control system is necessary to ensure that the internal control remains tuned to the changed objectives, environment, resources and risks.

These components define the recommended approach for internal control in government and provide a basis against which internal control can be evaluated. These components apply to all aspects of an organisation's operation.

These guidelines provide a general framework. When implementing them, management is responsible for developing the detailed policies, procedures, and practices to fit their organisation's operations and to ensure that they are built into and are an integral part of those operations.

### Relationship of objectives and components

There is a direct relationship between the objectives, which represent what an entity strives to achieve, and the internal control components, which represent what is needed to achieve them. The relationship is depicted in a three-dimensional matrix in shape of a cube.

The four objectives accountability(and reporting) compliance (with laws and regulations), (orderly, ethical, economical, efficient and effective) operations and safeguarding resources are represented by the vertical columns, the five components are represented by horizontal rows, and the organisation or entity and its departments are depicted by the third dimension of the matrix.

Each component row "cuts across" and applies to all four objectives. For example, financial and non financial data generated from internal and external sources, which belong to the information and communication component, are needed to manage operations, to report and fulfill accountability purpose, and to comply with applicable laws.

Similarly, looking at the objectives, all five components are relevant to each objective. Taking one objective e.g. effectiveness and efficiency of operations it is clear that all five components an applicable and important to its achievement.

Internal control is not only relevant to an entire organisation but also to an individual department. This relationship is depicted by the third dimension, which represents entire organization, entities and departments. Thus, one can focus on any of the matrix's cells.

While the internal control framework is relevant and applicable to all organisations, the manner in which management applies it will vary-widely with the nature of the entity and depends on a number of entity-specific factors. These factors include the organisational structure risk profile, operating environment, size, complexity, activities and degree of regulation, among others. As it considers the entity's specific situation, management will make a series of choices regarding the complexity of processes and methodologies deployed to apply the internal control framework components.

In the following text, each of the abovementioned components presented concisely with additional comments.

### 5.02.01 Control Environment

The control environment sets the tone of an organisation, influencing the control of its staff. It is the foundation for all other components of internal control. Providing discipline and structure. Elements to the control environment are.

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

(ii) competence;

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

(iv) organisational structure;

(v) human resource policies and practices.

### The personal and professional integrity and ethical Values of management and staff

The personal and professional integrity and ethical values of management and staff determine their preferences and tasks judgments, which are translated into standards of behavior. They should exhibit a supportive attitude toward internal control at all time throughout the organisation.

Every person involved in the organisation both managers and employees has to maintain and demonstrate personal and professional integrity and ethical value and has to comply with the applicable codes of conduct at all times. This can include for example the disclosure of personal financial interests outside positions and gifts (e.g. by elected officials and senior public servants), and reporting conflicts of interest.

Also public organisations have to maintain and demonstrate integrity and ethical values and they should make those visible to the public in their mission and core values.In addition, their operations have to be ethical, orderly, economical, efficient and effective. They have to be consistent with their mission.

### Competence

Competence includes the level of knowledge and skill needed to help ensure orderly, ethical, economical, efficient and effective performance as well as a good understanding of individual responsibilities with respect to internal control.

Managers and employees are to maintain a level of competence that allows them to understand the importance of developing, implementing, and maintaining good internal controls and to perform their duties in order to accomplish the general internal control objective and the entity's mission. Everyone in an organisation is involved in internal control with his own specific responsibilities.

Managers and their staffs must therefore maintain and demonstrate a level of skill necessary to help ensure effective and efficient performance, and an understanding of internal controls sufficient to effectively discharge their responsibilities.

Providing training for example, can raise the awareness of public servants on internal control and ethical issues, and helps develop public servants’ skills to handle ethical dilemmas and understand internal control.

### Tone at the top

The tone at the top (i.e. the management's philosophy and operating style) reflects:

- a supportive attitude toward internal control at all times, independence competence and leading by example.
- a code of conduct set out by the management and counseling and performance appraisals that support internal control and ethical behavior.

The attitude established by top management is reflected in all aspects of management's actions. The commitment the involvement and support of top government officials and legislators in setting "the tone at the top" foster a positive attitude and are critical to maintaining a positive and supportive attitude towards internal control in an organisation.

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. On the other hand if the members of the organisation feel that control is not an important concern to the top management and is given lip service rather than meaningful support, it is almost certain that management's control objectives will not be effectively achieved.

Consequently, demonstration and promotion of ethical conduct by the management is of vital importance to the objective 'ethical operations' In carrying out its role, management should set a good example through its own actions and its conduct should reflect what is proper rather than what is acceptable or expedient. However, ethics applies to all other objectives. Therefore, management policies, procedures and practices should promote orderly, ethical, economical, efficient and effective conduct.

The integrity of managers and their staff is however, influenced by many elements. Therefore, personnel should periodically be reminded of their obligations under an operative code of conduct issued by the top management. Counseling and performance appraisals are also important. Overall performance appraisals should be based on an assessment of many critical factors including the implementation and maintenance of effective internal controls.

**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. In exceptional circumstances, other lines of reporting have to be possible in addition to the normal ones. Organisational structure is also dealt with in chapter 3 on roles and responsibilities.

**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 counseling, promoting and compensating and remedial action.

An important aspect of internal control is personnel. Competent trustworthy personnel are responsible to provide effective control. Therefore, the methods by which persons are hired, evaluated, trained, promoted and compensated are an important part of the control environment Hiring and staffing decisions should therefore, include assurance that individuals have the proper education and experience to carry out their jobs and that the necessary formal, on-the-job, and ethics training is provided. Managers and employees who have a good understanding of internal controls and are willing to take responsibility, are vital to effective internal control.

Human resource management also has an essential role in promoting an ethical environment by developing professionalism and enforcing transparency in daily practice.

This becomes visible in recruitment, performance appraisal and promotion processes, which should be based on merits. Securing the openness of selection processes by publishing both the recruitment rules and vacant positions also helps to realise an ethical human resource management.

### 5.02.02 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 on the objectives of the entity:
include risks due to external and internal factorisation both the entity and the activity levels.

(2) Risk evaluation:-estimating the significance of a risk, assessing the likelihood of the risk occurrence.

(3) assessment of the risk appetite of the organisation.

(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 controls are the major mechanism to treat risk; the appropriate controls involved can be either detective or preventive.

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 controls to address changing risk.

As stressed in the definition internal control can provide only reasonable assurance that the objectives of the organisation are being achieved. Risk assessment as a component of internal control plays a key role in the selection of the appropriate control activities to undertake. It is the process of identifying and analysing relevant risks to the achievement of the entity's objectives and determining the appropriate response.

Consequently setting objectives is a precondition to risk assessment. Objectives must be defined before the management can identify the risks to their achievement and take the necessary actions to manage the risks. That means having in place and ongoing process for evaluating and addressing the impact of risks in a cost effective way and having staff with the appropriate skills to identity and assess the potential risks. Internal control activities are a response to risk in that they are designed to contain the uncertainty of outcome that has been identified.

Government entities have to manage the risks that are likely to have an impact on service delivery and the achievement of desired outcomes.

**Risk identification**

A strategic approach to risk assessment depends on identifying risks against key organisational objectives. Risks relevant to thoseobjectives are then considered and evaluated, resulting in a small number of key risks.

Identifying key risks is not only important in order to identify the most important areas to which resources in risk assessment should be allocated but also in order to allocate responsibility for management of these risks.

An entity's performance can be at risk due to internal or external factors at both the entity and activity levels. 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 relate it to the previous review. Such an approach facilitates the identification of changes in the risk profile of an organisation arising from changes in the economic and regulatory environments, internal and external operating conditions and from the introduction of new or modified objective. 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. 3

3.
Commissioning a risk review
This is a top down procedure. A team is established to consider all the operations and activities of the organisation in relation to its objectives and to identify the associated risks. The team conducts a series of interviews with key members of staff at all levels of the organization to build a risk profile for the whole range of activities thereby identifying the policy fields, activities and functions which may be particularly vulnerable to risk (including the risk of fraud corruption)
Risk self assessment
This is a bottom up approach. Each level and part of the organization is invited to review its activities and feed diagnosis of the risks faced upwards. This may be done through a documentation approach (with a framework).

**Risk evaluation**

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 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.

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. Generally, it is better to minimize the categories as over refinement may lead to separation off levels which in reality cannot be separated clearly.

By means of such evaluation, risks can be ranked in order to set management priorities and present information for management decisions about the risks that need to be addressed (for example those with a major potential impact and a high likelihood of the risks occurring.)

**Assessment of the risk “appetite” of the organisation**

An important issue in considering response to risk is the identification of the"risk appetite" of the entity. Risk appetite is the amount of risk to which the entity is prepared to be exposed before it judges action to be necessary. Decisions about responses to risk have to be taken in conjunction with an identification of the amount of risk that can be tolerated. 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 on the relevant budget, the source of the loss or associated other risk 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.

**Development of responses**

The result of the action outlined above will be at risk profile for the organisaiton. Having developed a risk profile, the organisaiton can then consider appropriate response.

Responses to risk can be divided into four categories. In some instances risk can be transferred, tolerated or terminated 4*. However, in most instances 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 purpose of treatment is not necessarily to obviate the risk, but more likely to contain it. The procedures that an organisation installs to treat risk are called internal control activities. Risk assessment should play a key role in the selection of appropriate control activities to undertake. Again, it is important to repeat that it is not possible to eliminate all risk and that internal controls can only provide reasonable assurance that the objectives of the organisation are being

4*
For some risks the best response may be to transfer them. This might be done by conventional insurance, by paying a third party to take the risk in another way, or it might be done by contractual stipulations.

The ability to do anything about some risks may be limited, or the cost of taking any action may be disproportionate to the potential benefit gained. In these cases the response may be to tolerate the risks.

Some risks will only be treatable or containable to acceptable levels, by terminating the activity. In the public sector, the option to terminate activities may be severely limited when compared to the private sector. A number of activities are conducted in the government sector because the associated risks are so great that there is no other way in which the output or outcome, which is required for the public benefit, can be achieved.

achieved. However entities that actively identify and manage risks are more likely to be better prepared to respond quickly when things go wrong and to respond to change in general. In designing an internal control system, it is important that the control activity installed is proportionate to the risk. Apart from the extreme undesirable outcome, it is normally sufficient to design a control to give 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 because governmental, economic, industry, regulatory and operating conditions continually change, the risk environment of any organization is constantly changing, and priorities of objectives and the consequent importance of risks will shift and change. Fundamental to risk assessment is an ongoing iterative process to identify changed conditions and take actions as necessary. Risk models and related controls have to be regularly revisited and reconsidered in order to have assurance that the risk profile continues to be valid, that responses to risk remain appropriately targeted and proportionate, and mitigating controls remain effective as risks change over time

### 5.02.03 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 must be appropriate, function consistently according to plan throughout the period and be cost effective, comprehensive, reasonable and integrated with the overall organisational objectives. Control activities occur throughout the organisation, at all levels and in all functions. They include a range of detective and preventive control activities control activities as diverse.
for example, as:

(1) authorization and approval procedures;
(2) segregation of duties (authorizing, processing, recording, reviewing).
(3) controls over access to resources and records;
(4) verifications;
(5) reconciliations;
(6) reviews of operating performance;
(7) reviews of operations, processes and activities;
(8) supervision(assigning, reviewing and approving guidance and training )

Control activities (1) -(7) are preventive, (4)- (6) are more detective while(7) and (8) are both preventive and detective Entities should reach an adequate balance between enforcementand prevention control activity.

Control activities are the policies and procedures established and executed 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 to the risk involved).
- function consistently according to plan throughout the period(that is be complied with

carefully by all employees involved and not bypassed when key personal are away or the workload is heavy).

- be cost effective(that is, the cost of implementing the control should not exceed the benefits derived);
- be comprehensive, reasonable and integrated into the overall organisational objectives.

Control activities include a range of policies and procedures as diverse as;

### 1- Authorization and approval procedures

Authorizing and executing transactions and events are only done by persons acting within the scope of their authority. Authorization is the principal means of ensuring that only valid transactions and events are initiated as intended by management. Authorization procedures.should be documented and clearly communicated to managers and employees, should include the specific conditions and terms under which authorisations are to be made. Conforming to the terms of and authorization means that employees act in accordance with directives and within the limitation established by management or legislation.

### 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 section should control all key stages of a transaction or event. Rather, 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. Collusion, however, can reduce or destroy the effectiveness of this internal control technique. A small organisation may have too few employees to fully implement this technique. In such cases, the management must be aware of the risks and compensate with other controls. 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. Also, encouraging or requiring annual holidays may help reduce risk by bringing about a temporary rotation of duties.

### 3 Controls over access to resources and records

Access to resources and records is limited to authorised individuals who are accountable for the custody and/or use of the resources. Restricting access to resources reduces the risk of unauthorised use or loss to the government and helps achieve management directives. The degree of restriction depends on the vulnerability of the resource and the perceived risk of loss or improper use, and should be periodically assessed. 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 in relation to bank accounts are reconciled with the corresponding bank statements.

### 6. Reviews of operating performance

Operating performances are reviewed against a set of standards on a regular basis, assessing effectiveness and efficiency.

### 7. Reviews of operations, processes and activities

Operations should be reviewed. This type of review of the actual operations of an organisation should be clearly distinguished form the monitoring of internal control.

### 8. Supervision (assigning, reviewing and approving, guidance and training)

Competent supervision ensures that internal control objectives are achieved. Assignment, review, and approval of an employee's work encompasses:clearly communicating the duties, responsibilities, and accountabilities assigned to each staff member:systematically reviewing each member's work to the extent necessary; approving work at critical points to ensure that it flows as intended.

A supervisor's delegations of work should not diminish the supervisor’s accountability for these responsibilities and duties. Supervisors also provide their employees with the necessary guidance and training to help ensure that errors, waste, and wrongful acts are minimized and that management directives are understood and achieved.

The abovementioned list is not exhaustive but enumerates the most common preventive and detective control activities. Control activities 1-3 are preventive, 4-6 are more detective while 7-8 are both preventive and detective. Entities should reach an adequate balance between enforcement and prevention control activities, where by often a mix of controls is used to compensate for the particular disadvantages of individual controls. Once a control activity is implemented, it is essential that assurance about its effectiveness is obtained. Moreover, it must be clear that control activities form only a component of internal control. They should be integrated with the other four components of internal control.

## 5.02.03.01 Information Technology Control Activities

Information system implies specific type of control activities. Therefore, information technology controls consist of two broad groupings;

1. General Controls

General controls are the structure policies and procedures that apply to all or a large segment of an entity's information system and help ensure their proper operation. They create the environment in which application systems and controls operate.

The major categories of general controls are (1) entity-wide security program planning and management. (2) access controls. (3) controls on the development maintenance and change of theapplication software. (4) system controls. (5) segregation of duties, and (6) service continuity.

2. Application Control

Application controls are the structure, policies, and procedures that apply to separate. Individual application systems and are directly related to separate, individual computerized applications. These controls are generally designed to prevent, detect and correct errors and irregularities as information flows through information systems. General and application controls are interrelated and both are needed to ensure complete and accurate information processing. Because information technology changes rapidly, the associated controls must evolve constantly to remain effective.

As information technology has advanced, organisations have become increasingly dependent on computerized information systems to carry out their operations and to process, maintain, and report essential information. As a result, the reliability and security of computerised data and of the systems that process, maintain, and report these data are a major concern to the management.

The use of automated systems to process information introduces several risks that need to be considered by the organisation .These risks stem from, among other things, uniform processing of transactions: information systems automatically initiating transactions; increased potential for undetected errors; existence, completeness, and volume of audit trails; the nature of hardware and software used; and recording of unusual or non-routine transactions. For example, an inherent risk from the uniform processing of transactions is that any error arising from computer programming problems will occur consistently in similar transactions. Effective information technology controls can provide management with reasonable assurance that information processed by its systems meets desired control objectives, such as ensuring the completeness, timeliness, and validity of data and preserving its integrity.

Information technology controls consist of two broad groupings, general controls and application controls.

**General controls**

General controls are the structure, policies and procedures that apply to all or a large segment of an entity's information system 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 :

**1.** Entity wide security program planning and management provide a framework and continuing cycle of activity for managing risk, developing security policies, assigning responsibilities, and monitoring the adequacy of the entity's computer related controls.

**2.** Access controls limit or detect access to computer resources (data. programs, equipment and facilities), thereby protecting these resources against unauthorized modification. loss, and disclosure. Access controls include both physical and logical controls.

**3.** Controls on the development, maintenance and change of application software prevent unauthorized programs or modifications to existing programs.

**4.** System software controls limit and monitor access to the powerful programs and sensitive files that control the computer hardware and secure applications supported by the system.

**5.** Segregation of duties implies that policies, procedures and an organisational structure are established to prevent one individual from controlling key aspects of computer- related operations and there by conducting unauthorised actions or gaining unauthorised, access to assets or records.

**6.** Service continuity controls ensure that when unexpected events occur, critical operations continue without interruption or are promptly resumed and critical and sensitive data are protected.

### 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 categorised into three phases of a processing cycle.

-inputs data are authorized, converted to an automated form and entered into the application in an accurate. complete. and timely manner;

-processing ;data are properly processed by the computer and files are updated correctly; and

-output: files and reports generated by the application reflect transactions or events that actually occurred and accurately reflect the results of processing, and reports are controlled and distributed to the authorized users.

Application controls may also be categorized by the kinds of control objectives they relate to, including whether transactions and information are authorized, complete, accurate and valid Authorization controls concern the validity of transactions and help ensure transactions represent events that actually occurred during a given period. Completeness controls relate to whether all valid transactions are recorded and properly classified. Accuracy controls address whether transactions are recorded correctly and all the data elements are accurate. Controls over the integrity of processing and data files, if deficient could nullify each of the above mentioned application controls and allow the occurrence of unauthorized transaction as well as contribute to incomplete and inaccurate data.

Application controls include programmed control techniques, such as automated edits, and manual follow-up of computer-generated output such as reviews of reports identifying rejected or unusual items.

### General and application controls over computer systems are interrelated

The effectiveness of general controls is a significant factor in determining the effectiveness of application controls. If general controls are weak, they severely diminish the reliability of controls associated with individual applications. Without effective general controls, application controls may be rendered ineffective by override, circumvention or modification. For example, edit checks designed to prevent users from entering unreasonably large amounts of money in a payment processing system can be an effective application control, However, this control can not be relied upon if the general controls permit unauthorized program modification that might allow some payments to be exempt from the edit. While the basic objectives of control do not change, rapid changes in information technology require that controls evolve to remain effective. Changes such as the increased reliance on networking, powerful computers that place responsibility for data processing in the hands of end users. Electronic commerce and the internet will affect the nature and implementation of specific control activities.

## 5.02.04 Information and Communication

Information and communication are essential to the realisation of all the internal control objectives.

### Information

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 time frame that enables staff to carry out their internal control and responsibilities (timely communication to the right people) Therefore, the internal control system and all transactions and significant events should be fully documented. Information systems produce reports that contain operations, financial and non-financial, and compliance related information and that make it possible to run and control the operation. They deal not only with internally generated data, but also information about external events, activities and conditions necessary to enable decision making and reporting.

Management’s ability to make appropriate decisions is affected by the quality of information, which implies that the information is appropriate, timely, current, accurate and accessible.

Information and communication are essential to the realisation of all the internal control objectives. For example, one of the objectives of internal control is fulfilling public accountability obligations. This can be achieved by developing and maintaining reliable and relevant financial and non-financial information and communicating this information by means of a fair disclosure in timely reports. Information and communication relating to the organisation's performance will create the possibility to evaluate the orderliness, ethicality, economy, efficiency and effectiveness of operations. In many cases, certain information or communications have to be provided in order to comply with laws and regulations.

Information is needed at all levels of an organisation in order to have effective internal control and achieve the entity's objectives. Therefore, an array of pertinent, reliable and relevant information should be identified, captured and communicated in a form and timeframe that enables people to carry out their internal control and other responsibilities. A precondition for reliable and relevant information is the prompt recording and proper classification of transactions and events.

Transactions and events must be recorded promptly when they occur if information is to remain relevant and valuable to the management in controlling operations and making decisions. This applies to the entire process or life cycle of a transaction or event including the initiation and authorization, all stages while in process, and its final classification in summary records. It also applies to promptly updating all documentation to keep it relevant. Proper classification of transactions and events is also required to ensure that reliable information is available to management. This means organizing, categorizing, and formatting information from which reports, schedules, and financial statements are prepared. Information systems produce reports that contain operational, financial and non-financial, and compliance-related information, and that make it possible to run and control the operation. The systems deal not only with quantitative and qualitative forms of internally-generated data, but also with information about external events, activities and conditions necessary for informed decision making and reporting. Management's ability to make appropriate decisions is affected by the quality of information, which implies that the information is:

- appropriate (Is the needed information there?)
- timely (Is it there when required?)
- current( Is it the latest available):
- accurate (Is it correct?)
- accessible (Can it be obtained easily by the relevant parties?)

In order to ensure the quality of information and reporting, to carry out the internal control activities and responsibilities.and to make monitoring more effective and efficient, the internal control system and all transactions and significant events should be fully and clearly documented (e.g. flow charts and narratives ). This documentation should be readily available for examination. Documentation of the internal control system should include identification of an organization's structure and policies and itsoperating categories and related objectives and control procedures. An organization must give written evidence of the components of the internal control process, including its objectives and control procedures. The extent of the documentation of an entity's internal control varies however with the entity's size, complexity and similar factors.

**Communication**

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. They should understand 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.

Information is a basis for communication, which must meet the expectations of groups and individuals, enabling them to carry out their responsibilities effectively. Effective communication should occur in all directions, flowing down, across and up the organization throughout all components and the entire structure. One of the most critical communications channels is that between the management and its staff. Management must be kept up to date on performance. developments, risks and the function of internal control and other relevant events and issues. By the same token, the management should communicate to its staff what information it needs and provide feedback and direction. Management should also provide specific and directed communication addressing behavioral expectations. This includes a clear statement of the entity’s internal control philosophy and approach and delegation of authority. Communication should raise awareness about the importance and relevance of effective internal control, communicate the entity's risk appetite and risk tolerances, and make personnel aware of their roles and responsibilities in effecting and supporting the components of internal control.

In addition to internal communications, management should ensure there are adequate means of communicating with, and obtaining information from external parties, as external communications can provide input that may have a highly significant impact on the organisation achieving its goals.

### 5.02.05 Monitoring

Internal control systems should be monitored to assess the quality of the system's performance over time. Monitoring is accomplished through routine activities, separate evaluations or a combination of both.

**(1) Ongoing monitoring**

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.

**(2) Separate evaluations**

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.

Monitoring should ensure that audit findings and recommendations are adequately and promptly resolved.

Monitoring internal control ensures 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, in order to ensure that internal control continues to be applied at all levels and across the entity, and that internal control achieves the desired results. Monitoring the internal control activities themselves should be clearly distinguished from monitoring an organisation's operations as an internal control activity.

Ongoing monitoring occurs in the course of normal, recurring operations of an organisation. It is performed continually and on a real-time basis, it reacts dynamically to changing conditions and is ingrained in the entity's operations. As a result, it is more effective than separate evaluations, Sinceseparate evaluations take place after the event.Problems will often be identified more quickly by ongoing monitoring routines.

The scope and frequency of separate evaluations should depend primarily on the assessment of risks and the effectiveness of ongoing monitoring procedures. When making that determination, the organisation should consider the nature and degree of changes, from both internal and external events, and their associated risks; the competence and experience of the personnel implementing risk responses and related controls; and the results of the ongoing monitoring. Separate evaluations of control can also be useful by focusing directly on the controls effectiveness at a specific time. Separate evaluations may take the form of self-assessments as well as a review of control design and direct testing of internal control. Separate evaluations also may be performed by the SAI's or by external auditors.

Usually, some combination of ongoing monitoring and separate evaluations will ensure that internal control maintains its effectiveness over time.All deficiencies found during ongoing monitoring or through separate evaluations should be communicated to those positioned to take necessary action. The term "deficiency" refers to a condition that affects and entity's ability to achieve its general objectives deficiency, therefore may represent a perceived, potential or real shortcoming or/ and opportunity to strengthen internal control to increase the likelihood that the entity's general objectives will be achieved.

Providing needed information on internal control deficiencies to the right party is critical. Protocols should be established to identify what information is needed at a particular level for effective decision making. Such protocols reflect the general rule that a manager should receive information that affects actions or behavior of personnel under his or her responsibility as well as information needed to achieve specific objectives.

Information generated in the course of operations is usually reported through normal channels, which relates to the individual responsible for the function and also to at least one level of management above that individual. However, alternative communications channels should also exist for reporting sensitive information such as illegal or improper acts.

Monitoring internal control should include policies and procedures that ensure that the findings of audits and other reviews are adequately and promptly resolved. Managers are to (1) promptlyevaluate 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 their attention.

The resolution process begins when audit or other review results are reported to management and is only completed after action has been taken that (1) corrects the identified deficiencies, (2) produces improvements, or (3) demonstrates that the findings and recommendations do not warrant management action.

## 5.03 Roles and Responsibilities

Everyone in an organisation has some responsibility for internal control:

**Managers** are directly responsible for all activities of organisation including the internal control system. Their responsibilities vary depending on their function in the organisation (e.g. board, financial officer, audit committee) and the organisation's characteristics.

**Internal auditors** examine the effectiveness of internal control and recommend improvements, but they don't have primary responsibility for establishing or maintaining it.

**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 establishment or operations of the organisation's internal control system.

**Supreme AuditInstitutions (SAI's**) encourage and support the establishment ofeffective internal control in the government. The assessment of internal control is essentialto the SAI's compliance, financial and performance audits. They communicate their findings and recommendations to interested stakeholders.

**External auditors** audit of 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 control. They should contribute to a common understanding of internal control.

**Other parties**interact with the organisations (beneficiaries, suppliers, etc) andprovide information regarding achievement of its objectives.

Internal control is primarily affected by an entity's internal stakeholders including management, internal auditors and other staff. However, the actions of external stakeholders also impact the internal control system.

All personnel in the organisation play important roles in making internal control work. However, management has the overall responsibility for the design, implementation and proper functioning of the internal control system. The organization structure may include boards and audit committees, which all have different roles and compositions and are subject to different legislation in different countries.

Management often establishes an internal audit unit as part of the internal control system and uses it to help monitor the effectiveness of internal control. Although internal auditors can be a valuable educational and advisory resource on internal control, the internal auditor should not be a substitute for a strong internal control system.

For an internal audit function to be effective, it is essential that the internal audit staff be independent from management, work in an unbiased, correct and honest way and that they report directly to a high level of authority within the organisation. This allows the internal auditors to present unbiased opinions on their assessments of internal control and objectively present proposals aimed at correcting the revealed shortcomings.

In addition to its role of monitoring and entity's internal controls, an adequate internal audit staff can contribute to the efficiency of the external audit efforts by providing direct assistance to the external auditor. The nature, scope or timing of the external auditor's procedures may be modified if the external auditor can rely upon the internal auditor's work.

Staff members and other personnel also effect internal control. It is often these frontline individuals who apply controls, review controls, correct for misapplied controls, and identify problems that may best be addressed through controls in conducting their daily assignments.

The second major group of internal control stakeholders are external parties such as external auditors (including SAI's) legislators and regulators, and other parties. 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 establishment or operation of the organisation's internal control system.

The tasks of external parties in particular external auditors and SAIs include assessing the functioning of the internal control system and informing management about its findings. SAIs may play a strategic role in the development of the internal control system, directly and indirectly, depending on their legal mandate and the management structure of the organisation.

*5For professional guidance, internal auditors can look to the Institute of Internal Auditors(IIA) and the INTOSAI code of ethics.*

Auditors assessing of internal control procedures 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 effectiveness or failure to fulfill accountability obligators and non compliance with laws and regulation;
- identifying and understanding the relevant internal 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 has a vested interest in ensuring that strong internal audit units exist where needed. Those audit units constitute an important element of internal control by providing a continuous means for improving an organisation's operations. In some countries, however the internal audit units may lack independence, be weak, or be non-existent. In those cases the SAI should, whenever possible offer assistance and guidance to establish and develop those capacities and to ensure the independence of the internal auditor's activities. This assistance might include secondment or lending of staff, conducting lectures, sharing training materials, and developing methodologies and work programs.

The Supreme audit Institution 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. Including internal audit observations and recognizing their contributions in the external audit report when appropriate can also foster this relationship. The SAI should develop procedures for assessing the internal audit unit's work to determine to which 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. The SAI should ensure that it has access to internal audit reports. related working papers, and audit resolution information.

Legislation can provide a common understanding of the internal control definition and objectives to be achieved. It can also prescribe the policies that internal and external stakeholders are to follow in carrying out their respective roles and responsibilities for internal control.