Guidelines for Internal Control Standards for the Public Sector

GUIDELINES FOR INTERNAL CONTROL STANDARDS FOR THE PUBLIC SECTOR

Internal Control Standards Committee

Fr. VANSTAPEL
Senior President
of the Belgian Court of Audit

Regentschapsstraat 2
B-1000 BRUSSELS
BELGIUM

Tel: ++32 (2) 551 81 11
Fax: ++32 (2) 551 86 22
E-mail: internalcontrol@ccrek.be

Guidelines for Internal Control Standards for the Public Sector

INTOSAI

INTOSAI General Secretariat - RECHNUNGSHOF
(Austrian Court of Audit)
DAMPFSCHIFFSTRASSE 2
A-1033 VIENNA
AUSTRIA
Tel: ++43 (1) 711 71 • Fax: ++43 (1) 718 09 69

E-mail: intosai@rechnungshof.gv.at
http://www.intosai.org

Contents

Preface 1

Introduction 3

1 Internal Control 6
1.1 Definition 6
1.2 Limitations on Internal Control Effectiveness 12

2 Components of Internal Control 13
2.1 Control Environment 17
2.2 Risk Assessment 22
2.3 Control Activities 28
2.4 Information and Communication 36
2.5 Monitoring 40

3 Roles and Responsibilities 43

Annex 1 Examples 49
Annex 2 Glossary 57

Guidelines for Internal Control Standards for the Public Sector

Preface

The 1992 INTOSAI guidelines for internal control standards were conceived as a living document reflecting the vision that standards should be promoted for the design, implementation, and evaluation of internal control. This vision involves a continuing effort to keep these guidelines up-to-date.

The 17th INCOSAI (Seoul, 2001) recognized a strong need for updating the 1992 guidelines and agreed that the Committee on Sponsoring Organisations of the Treadway Commission's (COSO) integrated framework for internal control should be relied upon. Subsequent outreach efforts resulted in additional recommendations that the guidelines address ethical values and provide more information on the general principles of control activities related to information processing. The revised guidelines take these recommendations into account and should facilitate the understanding of new concepts with respect to internal control.

These revised guidelines should also be viewed as a living document which over time will need to be further developed and refined to embrace the impact of new developments such as COSO's Enterprise Risk Management Framework[1].

This update is the result of the joint effort of the members of the INTOSAI Internal Control Standards Committee. This update has been coordinated by a task force set up among the committee members with representatives of the SAIs of Bolivia, France, Hungary, Lithuania, the Netherlands, Romania, the United Kingdom, the United States of America and Belgium (chair).

[1] COSO, Enterprise Risk Management - Integrated Framework, www.coso.org, 2004.

An action plan for updating the guidelines was submitted to and approved by the Governing Board at its 50th meeting (Vienna, October 2002). The Governing Board was informed of the progress of the work at its 51st meeting (Budapest, October 2003). The draft was discussed at and generally accepted by a committee meeting in Brussels in February 2004. After the committee meeting it was sent to all INTOSAI members for final comment.

The comments that were received, have been analyzed and subsequent changes have been made as deemed appropriate.

I would like to thank all the members of the INTOSAI Internal Control Standards Committee for their dedication and cooperation in completing this project. Special thanks is given to the members of the task force.

The *guidelines for internal control standards fot the public sector* are presented for approval by the XVIII INCOSAI in Budapest 2004.

Franki VANSTAPEL
Senior President of the Belgian Court of Audit
Chairman of the INTOSAI Internal Control Standards Committee

Introduction

In 2001, INCOSAI decided to update the 1992 INTOSAI guidelines on internal control standards to take into account all relevant and recent evolutions in internal control and to incorporate the concept of the COSO report titled Internal Control – Integrated Framework in the INTOSAI document.

By implementing the COSO model in the guidelines, the Committee not only aims at updating the concept of internal control, but also attempts to contribute to a common understanding of internal control among SAIs. It is self-evident that this document takes into account the characteristics of the public sector. This prompted the Committee to consider some additional topics and changes.

Compared to the COSO definition and the 1992 guidelines, the ethical aspect of operations has been added. Its inclusion in the internal control objectives is justified, as the importance of ethical behavior as well as prevention and detection of fraud and corruption in the public sector has become more emphasized since the nineties.[2] 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.

Since resources in the public sector generally embody public money and their use in the public interest generally requires special care, the significance of safeguarding resources in the public sector needs to be stressed. Moreover budgetary accounting on a cash basis is still a widespread practice in the public sector but it does not provide sufficient assurance related to the acquisition, use, and disposition of resources. As a result, organisations in the public sector do not always have an up-to-date record of all their assets, which makes them more vulnerable. Therefore, safeguarding resources was judged to be an important internal control objective.

Just as internal control in 1992 was not limited to the traditional view of financial and related administrative control and included the broader

[2] XVI INCOSAI, Montevideo, Uruguay, 1998.

concept of management control, this document also stresses the importance of non-financial information.

Because of the extensive use of information systems in all public organisations, information technology (IT) controls have become increasingly important, which justified a separate paragraph in these guidelines. Information technology controls relate to each of the components of an entity's internal control process including the control environment, risk assessment, control activities, information and communication, as well as monitoring. However, for presentation purposes, they are discussed under "Control Activities".

The goal of the Committee is to develop guidance for establishing and maintaining effective internal control in the public sector. Government management is therefore an important addressee of the guidelines. Government management can use these guidelines as a basis for the implementation and execution of internal control in their organisations.

Since evaluating internal control is a generally accepted field standard in government auditing[3], auditors can use the guidelines as an audit tool. The guidelines for internal control standards comprising the COSO model can therefore be used both by government management[4] as an example of a solid internal control framework for their organisation, and by auditors as a tool to assess internal control. However, these guidelines are not intended as a substitute for INTOSAI Auditing Standards or other relevant auditing standards.

This document defines a recommended framework for internal control in the public sector and provides a basis against which internal control can be evaluated. The approach applies to all aspects of an organisation's operation. However, it is not intended to limit or interfere with duly granted authority related to developing legislation, rule-making, or other discretionary policy-making in an organisation.

Internal control in public sector organisations should be understood within the context of the specific characteristics of these organisations,

---

[3] INTOSAI Auditing Standards

[4] Operative personnel are not specifically mentioned as a target group. Although they are affected by internal control and take actions that play an important role in effecting control, they, unlike management, are not ultimately responsible for all activities of an organisation, related to the internal control system. Chapter 3 of the guidelines describes individual roles and responsibilities.

i.e. their focus on meeting social or political objectives; their use of public funds; the importance of the budget cycle; the complexity of their performance (that calls for a balance between traditional values like legality, integrity and transparency and modern, managerial values like efficiency and effectiveness); and the correspondingly broad scope of their public accountability.

In conclusion, it should be clearly stated that this document includes guidelines for standards. These guidelines do not provide detailed policies, procedures and practices for implementing internal control, but rather provide a broad framework within which entities can develop such detailed controls. The Committee is obviously not in a position to enforce standards.

How is this document structured?

In the first chapter, the concept of internal control is defined and its scope is delineated. Attention is also given to the limitations of internal control. In the second chapter, the components of internal control are presented and discussed. The document ends with a third chapter on roles and responsibilities.

In every section, the main principles are first presented succinctly in a blue-shaded text box, followed by further background. Reference is also made to concrete examples, which can be found in the annexes. Also attached to the document is a glossary containing the most important technical terms.

1 Internal Control

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.

Internal control is a dynamic integral process that is continuously adapting to the changes an organisation is facing. 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.

An integral process

Internal control is not one 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 management runs the organisation. Internal control is therefore different from the perspective of some observers who view it 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 with the basic management processes of planning, executing and monitoring.

Built in internal control also has important implications for cost containment. Adding new control procedures that are separate from existing procedures adds costs. By focusing on 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. Because of the importance of this concept, a separate chapter (3) is devoted to it.

An organisation's people include management and other personnel. Although management primarily provides oversight, it also sets the entity's objectives and has 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. The implementation of internal control requires significant management initiative and intensive communication by management with other personnel. Therefore internal control is a tool used by management and directly related to the entity's objectives. As 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.

In pursuit of the entity's mission

Any organisation is primarily concerned with the achievement of its mission. Entities exist for a purpose – the public sector is generally concerned with the delivery of a service and a beneficial outcome in the public interest.

To address risks

Whatever the mission may be, its achievement will face all kinds of risks. The task of management is to identify and respond to these risks in order to maximize the likelihood of achieving the entity's mission. Internal control can help to address these risks, however it can only provide reasonable assurance about the achievement of the mission and the general objectives.

Provides reasonable assurance

No matter how well designed and operated, internal control cannot provide management absolute assurance regarding the achievement of the general objectives. Instead, the guidelines acknowledge that only a "reasonable" level of assurance is attainable.

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 its 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; or management can override the internal control system. In addition, compromises in the internal control system reflect the fact that controls have a cost. 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. Decisions on risk responses and establishing controls need to consider the relative costs and benefits. Cost refers to the financial measure of resources consumed in accomplishing a specified purpose and to the economic measure of a lost 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. Otherwise, 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.

However qualitative considerations should also be made.
For example, it may be important to have proper controls over high risk/low monetary unit transactions such as salaries, travel and hospitality expenses. The costs of appropriate controls might seem excessive for the amounts of money involved relative to overall government expenditures, but they may be critical to maintaining public confidence in governments and related organization.

Achievement of objectives

Internal control is geared to the achievement of a separate but interrelated series of general objectives. These general objectives are implemented through numerous specific sub-objectives, functions, processes, and activities.

The general objectives are:

- *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, methodical.

Ethical relates to moral principles. The importance of ethical behaviour 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.

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.

Efficient refers to the relationship between the resources used and the outputs produced 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.

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.

- *fulfilling accountability obligations*

Accountability is the process whereby public service organisations and individuals within them are held responsible for their decisions and actions, including their stewardship of public funds, fairness, and all aspects of performance.

This will be realized by developing, maintaining and making available 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. In public organisations laws and regulations mandate the collection and spending of public money and the way of operating. Examples include the Budget Act, international treaties, laws on proper administration,

accounting law/standards, environmental protection and civil rights law, income tax regulations and anti-fraud and corruption acts.

- *safeguarding resources against loss, misuse and damage due to waste, abuse, mismanagement, errors, fraud and irregularities*

Although the fourth general objective can be viewed as a subcategory of the first one (orderly, ethical, economical, efficient and effective operations), the significance of safeguarding resources in the public sector needs to be stressed. This is due to the fact that resources in the public sector generally embody public money and their use in the public interest generally requires special care. Moreover budgetary accounting on a cash basis, which is still widespread in the public sector, does not provide sufficient assurance related to the acquisition, use, and disposition of the resources. As a result, organisations in the public sector do not always have an up-to-date record of all their assets, which makes them more vulnerable. Therefore, controls should be embedded in each of the activities related to managing the entity's resources from acquisition to disposal.

Other resources such as information, source documents and accounting records are the key to achieving transparency and accountability of government operations, and should be preserved. However they are also in danger of being stolen, misused or destroyed.
Safeguarding certain resources and records has even 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.

1.2 Limitations on Internal Control Effectiveness[5]

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 management information about the entity's progress, or lack of it, toward 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 and may require managers to re-design controls or adjust the level of acceptable risk.

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

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 of 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.

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] The limitations on internal control effectiveness need to be stressed to avoid exaggerated expectations due to a misunderstanding of its effective scope.

2 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 an effective control environment, an *assessment of the risks* facing the entity as it seeks to achieve its mission and objectives provides the basis for developing an appropriate response to risk.

The major strategy for mitigating risk is through internal *control activities*. Control activities can be preventive and/or detective. 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, complete, reliable, correct and 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 help ensure that internal control remains tuned to the changed objectives, environment, resources and risks.

These components define a 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.

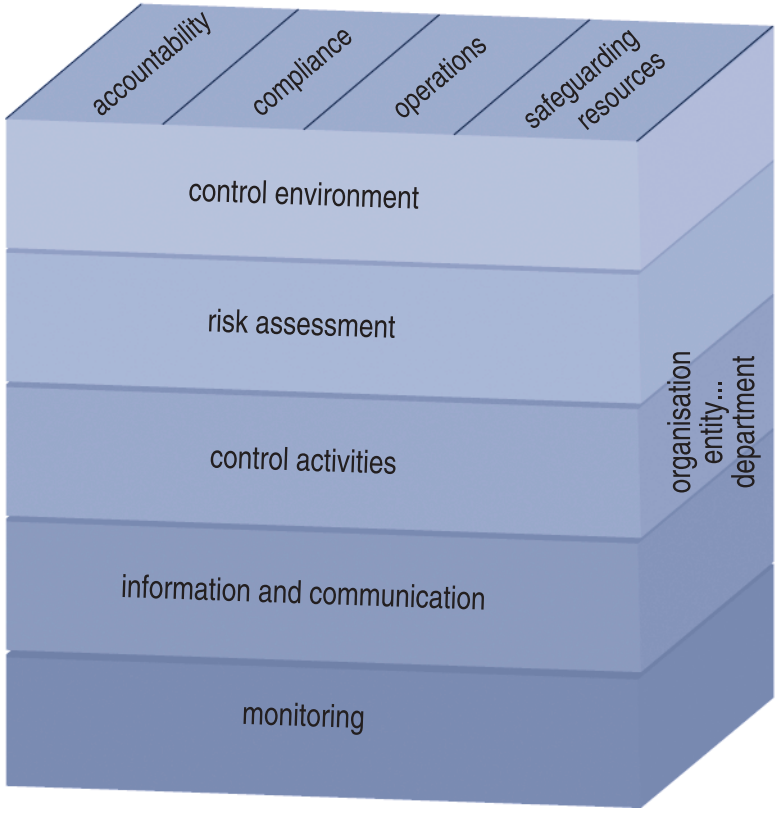
These guidelines provide a general framework. When implementing them, management is responsible for developing the detailed policies, procedures, and practices to fit their organisation's operations and to ensure that they are built into and are an integral part of those operations.

Relationship of objectives and components

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

The four general 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 general 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, report and fulfill accountability purposes, and comply with applicable laws.



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

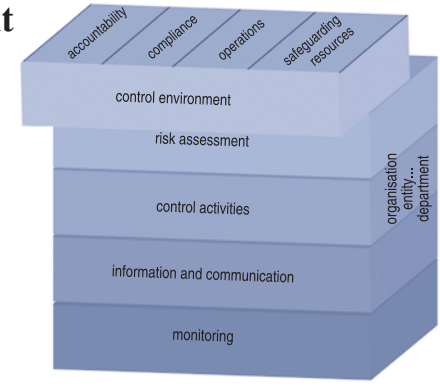
Internal control is not only relevant to an entire organisation but also to an individual department. This relationship is depicted by the third dimension, which represents entire organisations, entities and departments. Thus, one can focus on any of the matrix's cells.

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 is presented concisely with additional comments.

2.1 Control Environment



The control environment sets the tone of an organisation, influencing the control consciousness of its staff. It is the foundation for all other components of internal control, providing discipline 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 organisation;

(2) commitment to competence;

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

(4) organisational structure;

(5) 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 value judgments, which are translated into standards of behaviour. They should exhibit a supportive attitude toward internal control at all times throughout the organisation.

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. For example, this can include 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.

Commitment to competence

Commitment to 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 control and to perform their duties in order to accomplish the general internal control objectives 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 assess risk and help ensure effective and efficient performance, and an understanding of internal control sufficient to effectively discharge their responsibilities.

Providing training, for example, can raise the awareness of public servants of the internal control objectives and, in particular, the objective of ethical operations, and helps them to understand the internal control objectives and to develop skills to handle ethical dilemmas.

Tone at the top

The "tone at the top" (i.e. 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 management, and counselling and performance appraisals that support the internal control objectives and, in particular, that of ethical operations.

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. For example, the creation of an internal audit unit as part of the internal control system is a strong signal by management that internal control is important.

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

Consequently, demonstration of and insistence on ethical conduct by management is of vital importance to the internal control objectives and, in particular the objective of "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. In particular, management's policies, procedures and practices should promote orderly, ethical, economical, efficient and effective conduct.

The integrity of managers and their staffs 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. Counselling and performance appraisals are also important. Overall performance appraisals should be based on an assessment of many critical factors, including the employees's role in effecting internal control.

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, such as in cases where management is involved in irregularities.

The organisational structure can include an internal audit unit that should be independent from management, and reports directly to the highest level of authority within the organisation.

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 counselling, promoting and compensating, and remedial actions.

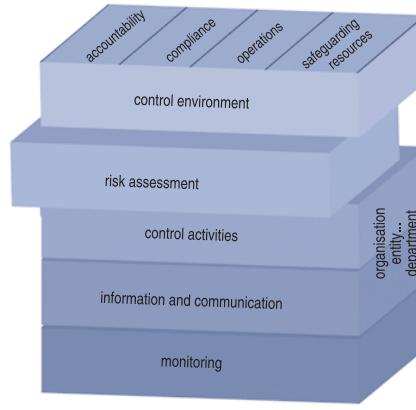
An important aspect of internal control is personnel. Competent, trustworthy personnel are necessary to provide effective control. Therefore, the methods by which persons are hired, trained, evaluated, compensated, and promoted, are an important part of the control environment. Hiring and staffing decisions should therefore include assurance that individuals have the integrity and 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 control 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 ethical human resource management.

Examples

We refer the reader to the annexes for integrated examples on each of the objectives and the components of internal control.

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;

(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 control is 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 control 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 management can identify the risks to their achievement and take the necessary actions to manage those risks. That means having in place an ongoing process for evaluating and addressing the impact of risks in a cost effective way and having staff with the appropriate skills to identify 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 those objectives 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[6] 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 objectives.

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.[7]

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 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 pri-

---

[6] An overview or matrix of the key risks facing an entity or sub-unit that includes the level of impact (e.g. high, medium, low) along with the probability or likelihood of the event occurring.

[7] *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 organisation 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 and corruption).

Risk self assessment
This is a bottom up approach. Each level and part of the organisation 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 for diagnosis set out through questionnaires) or through a facilitated workshop approach.

These two approaches are not mutually exclusive and a combination of top down and bottom up inputs to the risk assessment process is desirable to facilitate the identification of both entitywide and activity level risks.

ority. 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 spurious separation of 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.

Both inherent and residual risks need to be considered to determine the risk appetite. Inherent risk is the risk to an entity in the absence of any actions management might take to alter either the risk's likelihood or impact. Residual risk is the risk that remains after management responds to the risk.

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.

Development of responses

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.

Responses to risk can be divided into four categories. In some instances, risk can be *transferred, tolerated, or terminated*.[8] 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 establishes 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 control can only provide reasonable assurance that the objectives of the organisation are being 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 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.

Because governmental, economic, industry, regulatory and operating conditions continually change, the risk environment of any organisation is constantly changing, and priorities of objectives and the consequent importance of risks will shift and change. Fundamental to risk

---

[8] 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.

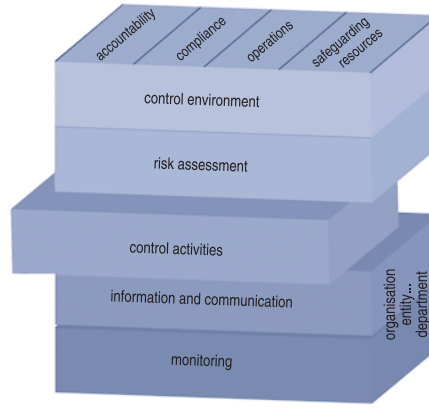
Some risks will only be treatable or containable to acceptable levels, by *terminating* the activity. In the public sector, the option to terminate activities may be severely limited when compared to the private sector. A number of activities are conducted in the government sector because the associated 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.

assessment is an ongoing, iterative process to identify changed conditions (risk assessment cycle) and take actions as necessary. Risk profiles 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.

Examples

We refer the reader to the annexes for integrated examples on each of the objectives and the components of internal control.

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 must be appropriate, function consistently according to plan throughout the period, and be cost effective, comprehensive, reasonable and directly relate to the control objectives.

Control activities occur throughout the organisation, at all levels and in all functions. They include a range of detective and preventive 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).

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.

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 personnel 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 directly relate to the control 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, 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. Conforming to the terms of an authorization means that employees act in accordance with directives and within the limitations 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 team 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 activity. A small organisation may have too few employees to fully implement this control. In such cases, 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 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. 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 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. If performance reviews determine that actual accomplishments do not meet established objectives or standards, the processes and activities established to achieve the objectives should be reviewed to determine if improvements are needed.

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. This type of review of the actual operations of an organisation should be clearly distinguished from the

monitoring of internal control which is discussed separately in section 2.5.

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 accountabilities assigned 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 delegation 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 detective and preventive control activities, whereby 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. Consequently corrective actions are a necessary complement to control activities. 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.

Examples
We refer the reader to the annexes for integrated examples on each of the objectives and the components of internal control.

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
General controls are the structure, policies and procedures that apply to all or a large segment of an entity's information systems 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 the application software, (4) system software controls, (5) 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, and are directly related to 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 help 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 computerized data and of the systems that process, maintain, and report these data are a major concern to both management and auditors of organisations. Although information systems imply specific types of control activities, information technology is not a "standalone" control issue. It is an integral part of most control activities.

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 the hardware and software used; and recording 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 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:

(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 all key aspects of computer-related operations and

thereby conducting unauthorized actions or gaining unauthorized access to assets or records.

(6) *Service continuity* controls help to 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 categorized into three phases of a processing cycle:

- input: 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 abovementioned application controls and allow the occurrence of unauthorized transactions, as well as contribute to incomplete and inaccurate data.

Application controls include programmed control activities, 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 unreasonable number of hours worked (e.g. more than 24 in a day) into a payroll system can be an effective application control. However, this control cannot be relied on if the general controls permit unauthorized program modifications that might allow some transactions to be exempt from the edit.

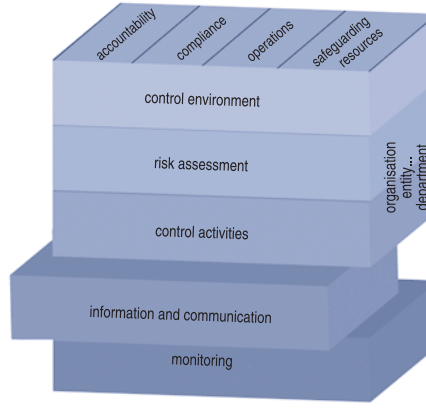
While the basic objectives of control do not change, rapid changes in information technology require that controls evolve to remain effective. Changes such as the increased reliance on networking, powerful computers that place responsibility for data processing in the hands of end users, electronic commerce, and the Internet will affect the nature and implementation of specific control activities.

Further guidance on information technology control activities can be obtained from the Information Systems Audit and Control Association (ISACA), in particular the ISACA Control Objectives for Information and Related Technology (COBIT) reference framework, and the proceedings of the INTOSAI IT-audit committee.

Examples

We refer the reader to the annexes for integrated examples on each of the objectives and the components of internal control.

2.4 Information and Communication



Information and communication are essential to realising all 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 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.

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. 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 should be 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 has to be provided or communication has to take place 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 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 help ensure the quality of information and reporting, carry out the internal control activities and responsibilities, and make monitoring more effective and efficient, the internal control system as such 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 organisation's structure and policies and its operating categories and related objectives and control procedures. An organisation must have written evidence of the components of the internal control process, including its objectives and control activities.

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 organisation, throughout all components and the entire structure.

One of the most critical communications channels is that between management and its staff. Management must be kept up to date on performance, developments, risks and the functioning of internal control, and other relevant events and issues. By the same token, management should communicate to its staff what information it needs and provide feedback and direction. Management should also provide specific and directed communication addressing behavioural expectations. This includes a clear statement of the entity's internal control philosophy and approach, and delegation of authority.

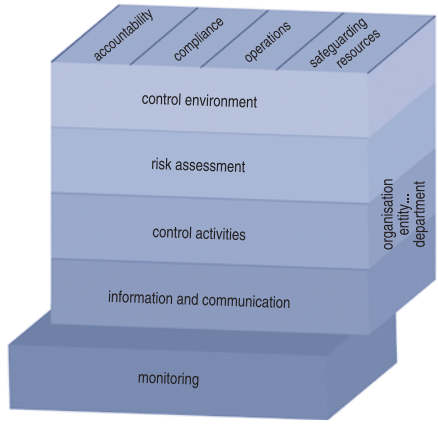
Communication should raise awareness about the importance and relevance of effective internal control, communicate the entity's risk appetite and risk tolerances, and make personnel aware of their roles and responsibilities in effecting and supporting the components of internal control.

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 extent to which the organisation achieves its goals.

Based on the input from internal and external communications, management has to take necessary action and perform timely follow up actions.

Examples
We refer the reader to the annexes for integrated examples on each of the objectives and the components of internal control.

2.5 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 is aimed at ensuring that controls are operating as intended and that they are modified appropriately for changes in conditions. Monitoring should also assess whether, in pursuit of the entity's mission, the general objectives set out in the definition of internal control are being achieved. This is accomplished through ongoing monitoring activities, separate evaluations or a combination of both, in order to help 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 reviewing an organisation's operations which is an internal control activity as previously described in section 2.3.

Ongoing monitoring of internal control occurs in the course of normal, recurring operations of an organisation. It is performed continually and on a real-time basis, reacts dynamically to changing conditions and is ingrained in the entity's operations. As a result, it is more effective than separate evaluations and corrective actions are potentially less costly. Since separate evaluations take place after the fact, 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 SAIs, by external or internal auditors.

Usually, some combination of ongoing monitoring and separate evaluations will help 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 an entity's ability to achieve its general objectives. A deficiency, therefore, may represent a perceived, potential or real shortcoming, or an 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 behaviour 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 means 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 aimed at ensuring the findings of audits and other reviews are adequately and 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 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.

Examples
We refer the reader to the annexes for integrated examples on each of the objectives and the components of internal control.

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.
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 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.

Internal control is primarily effected 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.

Managers

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

Internal auditors

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. Internal auditors regularly provide information about the functioning of internal control, focusing considerable attention on evaluating the design and operation of internal control. They communicate information about strengths and weaknesses and recommendations for improving internal control. However their independence and objectivity should be guaranteed.

Therefore internal auditing should be an independent, objective assurance and consulting activity that adds value and improves an organisation's operations. It helps an organisation accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control and governance processes.

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 the highest 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. For professional guidance, internal auditors should use the Professional Practices Framework (PPF) of The Institute of Internal Auditors (IIA) including the Definition, the Code of Ethics, the Standards and the Practice Advisories. Additionally, internal auditors should follow the INTOSAI Code of Ethics.

In addition to its role of monitoring an entity's internal control, 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

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.

External parties

The second major group of internal control stakeholders are external parties such as external auditors (including SAIs), 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 design, implementation, proper functioning, maintenance or documentation of the organisation's internal control system.

SAIs and external auditors

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. However, the external party's consideration of the internal control system is determined by his/her mandate.

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 effectivity, or failure to fulfil 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 Supreme Audit Institution 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? This should be done without threatening the independence of the SAI or external auditor.

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. 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 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. The SAI should ensure that it has access to internal audit reports, related working papers, and audit resolution information.

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.

Not only SAIs but also external auditors play an important role in contributing to the achievement of the internal control objectives, in particular "fulfilling accountability obligations" and "safeguarding resources". This is because external audits of financial reports and information are integral to accountability and good governance. External audits are still a primary mechanism that external stakeholders use to review performance, along with non-financial information.

Legislators and regulators

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.

Annex 1 Examples

Fulfilling accountability obligations example (1): A department that is responsible for the management of safe transport by water and sea has been organised by different service departments responsible for piloting, buoyage, inspection of the quality of the water, promotion of the use of waterways, investments in and maintenance of infrastructure (bridges, dikes, canals and locks).

Control Environment	Risk Assessment	Control Activities	Information & Communication	Monitoring
For each of the service departments an operational manager is appointed who has to report to the general manager of the department. The operational managers have the appropriate skills and have the authority to make certain decisions. All of them also sign a code of proper conduct.	Possible risks are collisions of ships, draining off toxic waste or fuel, and bursting of dikes. If mishaps are related to negligence of the government department, it could face a huge liability.	Control activities that can be organised are the pilotage of ships by competent pilots, placing buoys, beacons and markers; visual inspection by air, and taking water samples.	The information and communication related to this situation can be the reporting of collisions to warn other ships; informing ships of weather conditions, and publishing the names of polluters and the sanctions they are facing, and the remedial actions undertaken.	A follow-up of the number of collisions, environmental violations, results of the samples and a comparison with other countries and with historical data, can help to monitor the effectiveness and efficiency of the pilotage of ships, the placing of the beacons and markers, the inspections, and the water samples.

Fulfilling accountability obligations example (2): The manager of the department of sports stipulated last year the objective that the practice of sports would increase by 15% in the coming years.

Control Environment	Risk Assessment	Control Activities	Information & Communication	Monitoring
Because of the manager's good reputation, the executive committee trusted the manager and did not carry out the usual status meetings to check on the manager's progress. *(The abovementioned situation is not an example of good practice!)*	By not specifying the objectives, the risk arises of not achieving them. Also the danger exists that reporting will not be timely as the manager wants to wait with this report until he can say he realised the objective of 15% growth. Moreover, how to measure the 15% growth was not revealed, so he can say the number of people doing sports has increased or the number of hours people do sports, or even the number of sports centres or sports clubs has increased by 15%. This way the quality of the reported information decreases substantially.	This risk can be decreased by installing appropriate lines of reporting and a reporting model which defines the information that should be given.	This report should be delivered in time and according to the specified reporting model. It should specify the growth objectives, how they are measured and why they are measured this way. All the back up information should be available.	The verification of whether or not the report is satisfactory and what information is given and what information is still missing can be a form of monitoring.

Compliance with applicable laws and regulations example: The ministry of defence wants to buy new fighter planes via a public contract and publishes all stipulations and procedures for this government tender. All tenders received are left unopened until the end of the tender period. At that moment all tenders are opened in the presence of the responsible managers and some officials. Only these tenders will be investigated and compared to decide which tender is the best.

Control Environment	Risk Assessment	Control Activities	Information & Communication	Monitoring
The team that will execute this transaction is composed of competent people who signed a document that they have no financial or relational bond with any of the tenderers. The responsible managers and officials also signed this document.	One of the risks related to government tenders and public contract is insider dealing. One of the tenderers may have prior knowledge of the bids of the other tenderers and could make a winning tender with this information resulting in what may not be the best choice of all tenders. Another risk consists of choosing the wrong tender which may result in a new public contract because the other one did not meet the expectations. Also other tenderers who feel they were unfairly treated may make claims.	In order to mitigate risks, procedures should be developed and applied in accordance with all relevant laws and regulations concerning public contracts.	The procedures relating to the publication of all stipulations for this government tender, the assessment of the received tenders and the announcement of the selected tenderer, should be documented in writing and detail all actions to be taken. When assessing the tenders, all reasons why a tender was or was not chosen should be documented.	Internal audit can do file-reviews and follow-up on claims.

Orderly, ethical, economical, efficient and effective operations example (1): The department of culture wants to increase museum visits by the public. In order to accomplish this, it proposes to build new museums, give every citizen a cultural cheque and decrease ticket prices. To be economical, effective and efficient, management has to consider and evaluate whether or not the objectives as formulated can be achieved by its proposals and how much each of these proposals will cost.

Control Environment	Risk Assessment	Control Activities	Information & Communication	Monitoring
The department of culture needs to make sure that its organisation structure is suited to support overseeing design and construction of the proposed additions, as well as planning and operations of the new museums.	The fact that the number of museum visits does not increase is one of the possible risks. Also the risk that some of the proposals will backfire and exceed their budget is possible. For instance, if decreasing ticket prices does not increase museum visits, this decreases the government receipts. Further, building new museums without proper planning and consideration of requirements of lighting, temperature and security can result in expensive adjustments during or after construction.	The control activities related to the before mentioned risks can be a budgetary control that compares actual to budget, observations of the progress of the construction, and demanding justifications for overspending the budget.	The information and communication related to this example can consist of the documentation of meetings with architects, fire department (for safety regulations), artists and others. It can also contain different reports concerning following up on the budget and the progress of the construction work.	The analysis of the justifications for exceeding budget and related interest costs due to delayed work or payments are a part of monitoring.

Orderly, ethical, economical, efficient and effective operations example (2): The government wants to develop agriculture and increase the quality of life in the countryside. They provide funds to subsidize the construction of irrigation and the drilling of wells.

Control Environment	Risk Assessment	Control Activities	Information & Communication	Monitoring
The government must ensure that it has the appropriate department in place to implement and conduct the subsidy operation, and create the appropriate tone for the timely and efficient completion of this project.	The risks involved are that unscrupulous associations qualify for a grant but do not use the money for what it was intended.	Control activities can be: - Checking the qualifications of the associations applying for a grant. - Checking on site the progress of and reviewing progress reports on the construction works. - Checking the expenditures of the associations by reviewing their invoices, and delaying payment of (or part of) the subsidy until this review is completed.	- Progress reports detailing the costs and the number of wells that were drilled and the number of acres that were irrigated. - (Copies of) invoices are requested as justifications for the subsidised expenses.	Monitoring can consist of a follow-up of the drilling of wells and the construction of irrigation, and a comparison with other similar projects. Also a follow-up on the proceeds of the irrigated land can be considered.

Safeguarding resources example (1): The ministry of defence has some warehouses, military stores and fuel depots. The army command has the policy that these supplies are only for professional military use and not for personal use.

Control Environment	Risk Assessment	Control Activities	Information & Communication	Monitoring
Good human capital policies would be effective in recruiting and maintaining the appropriate personnel to staff and operate such warehouses.	The risk exists that people will want to try to steal weapons to use them inappropriately or sell them. Also other supplies like fuel can be vulnerable to theft.	Control activities that deal with these risks can be putting fences and walls around the warehouses and depots, or placing armed guards with dogs at the entrances. Regularly checking the stock records and a procedure which states that supplies can only be given with approval of a superior officer will also help to safeguard the assets.	Reports of damaged fences and differences noticed during stock takes. Supply approvals and procedures also provide information and communication related to this objective.	Monitoring can be an inspection of the fence, unannounced stock takes, follow-up of stock movements or even a secret test of security.

Safeguarding resources example (2): Large amounts of sensitive information are stored on computer media in an agency of the ministry of justice. However, the importance of IT controls is neglected and consequently the IT control has numerous deficiencies.

Control Environment	Risk Assessment	Control Activities	Information & Communication	Monitoring
Management must dedicate its commitment to competence and proper behaviour involving IT, and provide proper training in this area. Human capital policies also play a key role in establishing a positive control environment for IT issues.	At the general controls level, the agency has not: - limited user access to only that needed by users to perform their duties; - developed adequate system software controls to protect programs and sensitive data; - documented software changes; - segregated incompatible duties; - addressed service continuity; - protected its network from unauthorized traffic. At the application controls level, the agency has not maintained access authorizations. *(This is not an example of good practice!)*	The agency can: - implement logical (e.g. passwords) and physical access controls (e.g. locks, ID badges, alarms); - deny the ability to log in to the operating system for application users; - limit access to the production environment for the application development staff; - use audit logs to register all access (attempts) and commands to detect security violations; - have a contingency and disaster recovery plan to ensure the availability of critical resources and facilitate the continuity of operations; - have firewalls and monitor the web server activity to secure the network traffic.	Procedures on IT control should be available and software changes should be documented before the software is placed in operation. Policies and job descriptions supporting the principles of segregation of duties should be developed. Audit logs on access (attempts) and (unauthorized) commands should be periodically reported and reviewed.	Performing an IT audit, doing a disaster simulation exercise, and monitoring the web server activity, can be part of monitoring the IT environment.

Annex 2 Glossary

This glossary is intended to provide a common understanding of the main terms used in these guidelines in respect to internal control definitions and practices. In addition to some definitions we introduced in this document, we also used existing definitions from various sources as noted.

- Code of ethics and auditing standards, INTOSAI, 2001. (INTOSAI auditing standards)
- Internal Control – Integrated Framework, COSO, 1992. (COSO 1992)
- Glossarium, Office for official publications of the European communities, P. Everard and D. Wolter, 1989. (glossarium)
- Auditing and assurance services, an integrated approach, A. A. Arens, R. J. Elder and M. S. Beasley, Prentice Hall international edition, ninth edition, 2003. (Arens, Elder & Beasley)
- the COSO exposure draft "Enterprise Risk Management Framework", COSO, 2003. (COSO ERM)
- Handbook of international auditing, assurance, and ethics pronouncements, IFAC, 2003. (IFAC)
- Transparency International Source Book 2000, (Transparency International)
- XVI INCOSAI, Montevideo, Uruguay, 1998, Principal Paper Theme 1A (Preventing and Detecting Fraud and Corruption), February 1997, (XVI INCOSAI, Uruguay, 1998)
- Professional Practices Framework, The Institute of Internal Auditors. (IIA)

A

Access control
In information technology, controls designed to protect resources from unauthorized modification, loss, or disclosure.

Accountability
• The process whereby public service bodies and the individuals within them are held responsible for their decisions and actions, including their stewardship of public funds and all aspects of performance.
• Duty imposed on an audited person or entity to show that he/it has administered or controlled the funds entrusted to him/it in accordance with the terms on which the funds were provided. (glossarium)

Application
Computer program designed to help people perform a certain type of work, including specific functions, such as payroll, inventory control, accounting, and mission support. Depending on the work for which it is designed, an application can manipulate text, numbers, graphics, or a combination of these elements.

Application controls
• The structure, policies, and procedures that apply to separate, individual application systems and are designed to cover the processing of data within specific applications software.
• Programmed procedures in application software, and related manual procedures, designed to help ensure the completeness and accuracy of information processing. Examples include computerized edit checks of input data, numerical sequence checks and manual procedures to follow up on items listed in exception reports. (COSO 1992)

Audit
Review of a body's activities and operations to ensure that these are being performed or are functioning in accordance with objectives, budget, rules and standards. The aim of this review is to identify, at regular intervals, deviations which might require corrective action. (glossarium)

Audit committee
A committee of the Board of Directors whose role typically focuses on aspects of financial reporting and on the entity's processes to manage business and financial risk, and for compliance with significant applicable legal, ethical, and regulatory requirements. The Audit Committee typically assists the Board with the oversight of (a) the integrity of the entity's financial statements, (b) the entity's compliance with legal and regulatory requirements, (c) the independent auditors' qualifications and independence, (d) the performance of the entity's internal audit function and that of the independent auditors and (e) compensation of company executives (in absence of a remuneration committee).

Audit institution
Public body which, however it is appointed, composed or organised, carries out external audit duties in accordance with the law. (glossarium)

B

Budget
Quantitative, financial expression of a program of measures planned for a given period. The budget is drawn up with a view to planning future operations and to making ex post facto checks on the results obtained. (glossarium)

Budgetary control
Control by which an authority which has granted an entity a budget ensures that this budget has been implemented in accordance with the estimates, authorisations and regulations. (glossarium)

C

Collusion
A cooperative effort among employees to defraud a business of cash, inventory, or other assets. (Arens, Elder & Beasley)

Compliance
• Having to do with conforming with laws and regulations applicable to an entity. (COSO 1992)
• Conformity and adherence to policies, plans, procedures, laws, regulations, contracts, or other requirements. (IIA)

Component of internal control
One of five elements of internal control. The internal control components are the entity's internal control environment, risk assessment, control activities, information and communication, and monitoring. (COSO 1992)

Computer controls
1. Controls performed by computer, i.e., controls programmed into computer software (contrast with manual controls). 2. Controls over computer processing of information, consisting of general controls and application controls (both programmed and manual). (COSO 1992)

Computer information system
A computer information system (CIS) environment exists when a computer of any type or size is involved in the processing by the entity of (financial) information of significance to the audit, whether that computer is operated by the entity or by a third party. (IFAC)

Control
• 1. A noun, used as a subject, e.g. existence of a control – a policy or procedure that is part of internal control. A control can exist within any of the five components. 2. A noun, used as an object, e.g. to effect control – the result of policies and procedures designed to control; this result may or may not be effective internal control. 3. A verb, e.g. to control – to regulate; to establish or implement a policy that affects control. (COSO 1992)
• Any action taken by management, the board, and other parties to manage risk and increase the likelihood that established objectives and goals will be achieved. Management plans, organizes, and directs the performance of sufficient actions to provide reasonable assurance that objectives and goals will be achieved. (IIA)

Control activity
Control activities are the policies and procedures established to address risks and to achieve the entity's objectives. The procedures that an organisation puts in place to treat risk are called internal control activities. Internal control activities

are a response to risk in that they are designed to contain the uncertainty of outcome that has been identified.

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

Corruption
- Any form of unethical use of public authority for personal or private advantage. (XVI INCOSAI, Uruguay, 1998)
- The misuse of entrusted power for private benefit. (Transparency International)

COSO
Committee of Sponsoring Organisations of the Treadway Commission, a group of several accounting organisations. In 1992, it published a significant study on internal control titled Internal Control – Integrated Framework. The study is often referred to as the COSO Report.

D

Data
Facts and information that can be communicated and manipulated.

Deficiency
A perceived, potential or real internal control shortcoming, or an opportunity to strengthen internal control to provide a greater likelihood that the entity's objectives are achieved. (COSO 1992)

Design
1. Intent. As used in the definition, internal control is intended to provide reasonable assurance as to the achievement of objectives; when the intent is realized, the system can be deemed effective. 2. Plan; the way a system is supposed to work, contrasted with how it actually works. (COSO 1992)

Detective control
A control designed to discover an unintended event or result (contrast with preventive control) (COSO 1992)

Documentation
- Documentation of the internal control structure is the material and written evidence of the components of the internal control process, including the identification of an organisation's structure and policies and its operating categories, its related objectives and control activities. These should appear in documents such as management directives, administrative policies, procedures manuals, and accounting manuals.

E

Economical
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.

Economy
• Minimising the cost of resources used for an activity, having regard to the appropriate quality. (INTOSAI auditing standards)
• Acquisition at the right time and at the lowest cost of financial, human and material resources which are suitable in terms of both quality and quantity. (glossarium)

Edit checks
Programmed controls built into the early stages of the input process to identify erroneous data fields. For example, alphanumeric characters entered into numerical fields can be rejected by this control. Programmed edit controls can also be applied, for example, when transactions data enter the processing cycle from another application.

Effective
Refers to the accomplishment of objectives or the extent to which the outcomes of an activity match the objective or the intended effects of that activity.

Effectiveness
• The extent to which objectives are achieved and the relationship between the intended impact and the actual impact of an activity. (INTOSAI auditing standards)
• Extent to which the stated objectives have been attained in a cost-effective way. (glossarium)

Efficient
Refers to the relationship between the resources used and the outputs produced to achieve the objectives. It means that minimum resource inputs are used to achieve a given quantity and quality of output, or a maximum output with a given quantity and quality of resource inputs.

Efficiency
• The relationship between the output, in terms of goods, services or other results, and the resources used to produce them. (INTOSAI auditing standards)
• Use of financial, human and material resources in such a way as to maximize output for a given amount of resources, or to minimize input for a given quantity or quality of output. (glossarium)

End user computing
Refers to the use of non-centralized (i.e., non-IT department) data processing using automated procedures developed by end-users, generally with the aid of software packages (e.g., spreadsheet and database). End-user processes can be sophisticated and become an extremely important source of management information. Whether they are adequately tested and documented may be questionable.

Entity
An organization of any size established for a particular purpose. An entity, for example, may be a business enterprise, not-for-profit organization, government body or academic institution. Other terms used as synonyms include organization and department. (COSO 1992)

Ethical
Relates to moral principles.

Ethical values
Moral values that enable a decision maker to determine an appropriate course of behavior; these values should be based on what is "right," which may go beyond what is legally required. (COSO 1992)

External audit
Audit carried out by a body which is external to and independent of the auditee, the purpose being to give an opinion on and report on the accounts and the financial statements, the regularity and legality of operations, and/or the financial management. (glossarium)

F

Flowchart
A diagrammatic representation of the client's documents and records, and the sequence in which they are processed. (Arens, Elder & Beasley)

Flow-charting
Illustrates a flow of procedures, information or documents. This technique makes it possible to give a summary description of complex circuits or procedures. (glossarium)

Fraud
An unlawful interaction between two entities, where one party intentionally deceives the other through the means of false representation in order to gain illicit, unjust advantage. It involves acts of deceit, trickery, concealment, or breach of confidence that are used to gain some unfair or dishonest advantage. (XVI INCOSAI, Uruguay, 1998)

G

General controls
• General controls are the structure, policies and procedures that apply to all or a large segment of an entity's information systems and help ensure their proper operation. They create the environment in which application systems and controls operate.
• Policies and procedures that help ensure the continued, proper operation of computer information systems. They include controls over information technology management, information technology infrastructure, security management, and software acquisition, development and maintenance. General controls support the functioning of programmed application controls. Other terms sometimes used to describe general controls are general computer controls and information technology controls. (COSO ERM)

I

Independence
• Freedom given to an audit body and its auditors to act in accordance with the audit powers conferred on them without any outside interference. (glossarium)
• The freedom of the SAI in auditing matters to act in accordance with its audit mandate without external direction or interference of any kind. (INTOSAI auditing standards)
• The freedom from conditions that threaten objectivity or the appearance of objectivity. Such threats to objectivity must be managed at the individual auditor, engagement, functional and organizational levels.(IIA)
• The auditor's ability to maintain an unbiased viewpoint in the performance of professional services (independence in fact) (Arens, Elder & Beasley)
• The auditor's ability to maintain an unbiased viewpoint in the eyes of others (independence in appearance). (Arens, Elder & Beasley)

Inherent limitations
Those limitations of all internal control systems. The limitations relate to the limits of human judgment; resource constraints and the need to consider the cost of controls in relation to expected benefits; the reality that breakdowns can occur; and the possibility of management override and collusion. (COSO 1992)

Inherent risk
The risk to an entity in the absence of any actions management might take to alter either the risk's likelihood or impact. (COSO ERM)

Institute of Internal Auditors (IIA)
The IIA is an organisation that establishes ethical and practice standards, provides education, and encourages professionalism for its members.

Integrity
The quality or state of being of sound moral principle; uprightness, honesty and sincerity; the desire to do the right thing, to profess and live up to a set of values and expectations. (COSO 1992)

Internal audit
• The functional means by which the managers of an entity receive an assurance from internal sources that the processes for which they are accountable are operating in a manner which will minimise the probability of the occurrence of fraud, error or inefficient and uneconomic practices. It has many of the characteristics of external audit but may properly carry out the directions of the level of management to which it reports. (INTOSAI auditing standards)
• an independent, objective assurance and consulting activity designed to add value and improve an organisation's operations. It helps an organisation accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control and governance processes (IIA)
• Internal auditing is an appraisal activity established within an entity as a service to the entity. Its functions include, amongst other things, examining, evaluating and monitoring the adequacy and effectiveness of the accounting and internal control systems. (IFAC)

Internal auditor(s)
Examine and contribute to the ongoing effectiveness of the internal control system through their evaluations and recommendations, but they don't have primary responsibility for designing, implementing maintaining and documenting it.

Internal audit unit
• Department (or activity) within an entity, entrusted by its management with carrying out checks and assessing the entity's systems and procedures in order to minimize the likelihood of fraud, errors and inefficient practices. Internal audit must be independent within the organization and report directly to management. (glossarium)
• A department, division, team of consultants, or other practioner(s) that provides independent, objective assurance and consulting services designed to add value and improve an organisation's operations. The internal audit activity helps an organisation accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control and governance processes. (IIA)

Internal control
Internal control is an integral process that is effected by an entity's management and personnel and is designed to address risks and 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 and safeguarding resources against loss, misuse and damage.

Internal Control System (or Process, or Architecture)
A synonym for Internal Control, applied in an entity. (COSO 1992)

International Organisation of Supreme Audit Institutions (INTOSAI)
INTOSAI is the professional organisation of supreme audit institutions (SAI) in countries that belong to the United Nations or its specialised agencies. SAIs play a major role in auditing government accounts and operations and in promoting sound financial management and accountability in their governments. INTOSAI was founded in 1953 and has grown from the original 34 countries to a membership of over 170 SAIs.

Input
Any data entered into a computer or the process of entering data into the computer.

L

Legislature
The law-making authority of a country, for example a Parliament. (INTOSAI auditing standards)

Logical access
The act of gaining access to computer data. Access may be limited to "read only", but more extensive access rights include the ability to amend data, create new records, and delete existing records. (see also physical access)

M

Mainframe
A high-level computer designed for the most intensive computational tasks. Mainframe computers are often shared by multiple users connected to the computer by terminals.

Management
Comprises officers and others who also perform senior managerial functions. Management includes directors and the audit committee only in those instances when they perform such functions. (IFAC)

Management intervention
Management's actions to overrule prescribed policies or procedures for legitimate purposes; management intervention is usually necessary to deal with

non-recurring and non-standard transactions or events that otherwise might be handled inappropriately by the system (contrast this term with Management Override). (COSO 1992)

Management override
Management's overruling of prescribed policies or procedures for illegitimate purposes with the intent of personal gain or an enhanced presentation of an entity's financial condition or compliance status (contrast this term with Management Intervention). (COSO 1992)

Management process
The series of actions taken by management to run an entity. Internal control is a part of and integrated with the management process. (COSO 1992)

Manual controls
Controls performed manually, not by computer (contrast with Computer Controls). (COSO 1992)

Monitoring
Monitoring is a component of internal control and it is the process that assesses the quality of the internal control system's performance over time.

N

Network
In information technology, a group of computers and associated devices that are connected by communications facilities. A network can involve permanent connections, such as cables, or temporary connections made through telephone or other communications links. A network can be as small as a local area network consisting of a few computers, printers, and other devices, or it can consist of many small and large computers distributed over a vast geographic area.

O

Objectivity
An unbiased mental attitude that allows SAI's, internal and external auditors to perform engagements in such a manner that they have an honest belief in their work product and that no significant quality compromises are made. Objectivity requires the auditors not to subordinate their judgment on audit matters to that of others.

Operations
• Used with "objectives" or "controls": having to do with the effectiveness and efficiency of an entity's activities, including performance and profitability goals, and safeguarding resources. (COSO 1992)

• The functions, processes, and activities by which an entity's objectives are achieved.

Orderly
Means in a well-organised way, or methodically.

Output
In information technology, data/information produced by computer processing, such as graphic display on a terminal or hard copy.

P

Physical access
In access control, gaining access to physical areas and entities. (see logical access)

Policy
Management's dictate of what should be done to effect control. A policy serves as the basis for procedures for its implementation. (COSO 1992)

Preventive control
A control designed to avoid unintended events or results (contrast with detective control). (COSO 1992)

Procedure
An action that implements a policy. (COSO 1992)

Processing
In information technology, the execution of program instructions by the computer's central processing unit.

Public accountability
The obligations of persons or entities, including public enterprises and corporations, entrusted with public resources to be answerable for the fiscal, managerial and program responsibilities that have been conferred on them, and to report to those that have conferred these responsibilities on them. (INTOSAI auditing standards)

Public sector
The term 'public sector' refers to national governments, regional (for example, state, provincial, territorial) governments, local (for example, city, town) governments and related governmental entities (for example, agencies, boards, commissions and enterprises). (IFAC)

R

Reasonable assurance
• Equates to a satisfactory level of confidence under given considerations of costs, benefits, and risks.
• The concept that internal control, no matter how well designed and operated, cannot guarantee that an entity's objectives will be met. This is because of inherent limitations in all internal control systems. (COSO 1992)

Residual risk
The risk that remains after management responds to the risk.

Risk
The possibility that an event will occur and adversely affect the achievement of objectives. (COSO ERM)

Risk appetite
• The amount of risk to which the entity is prepared to be exposed before it judges action to be necessary.
• The broad-based amount of risk a company or other entity is willing to accept in pursuit of its mission or vision. (COSO ERM)

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.

Risk assessment cycle
An ongoing, iterative process to identify and analyse altered conditions, opportunities and risks and to take actions as necessary, in particular modifying internal control to address changing risk. Risk profiles 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.

Risk evaluation
Means estimating the significance of a risk and assessing the likelihood of the risk occurrence.

Risk profile
An overview or matrix of the key risks facing an entity or sub-unit that includes the level of impact (e.g., high, medium, low) along with the probability or likelihood of the event occurring.

Risk tolerance
The acceptable variation relative to the achievement of objectives. (COSO ERM)

S

Security program
An organization-wide program for security planning and management that forms the foundation of an organization's security control structure and reflects senior management's commitment to addressing security risks. The program should establish a framework and continuing cycle of activity for assessing risk, developing and implementing effective security procedures, and monitoring the effectiveness of these procedures.

Segregation (or separation) of duties
To reduce the risk of error, waste, or wrongful acts and the risk of not detecting such problems, no singular individual or team should control all key stages (authorizing, processing, recording, reviewing) of a transaction or event.

Service continuity control
This type of control involves ensuring that when unexpected events occur, critical operations continue without interruption or are promptly resumed and critical and sensitive data are protected.

Stakeholders
Parties that are affected by the entity, such as shareholders, the communities in which the entity operates, employees, customers and suppliers. (COSO ERM)

Supreme Audit Institution (SAI)
The public body of a State which, however designated, constituted or organised, exercises by virtue of law the highest public auditing function of that State. (INTOSAI auditing standards & IFAC)

System software
Software primarily concerned with coordinating and controlling hardware and communication resources, access to files and records, and the control and scheduling of applications.

System software controls
Controls over the set of computer programs and related routines designed to operate and control the processing activities of computer equipment.

U

Uncertainty
Inability to know in advance the exact likelihood or impact of future events. (COSO ERM)

V

Value for money
See Economy, Effectiveness and Efficiency