



USAID | **RULE OF LAW**
FROM THE AMERICAN PEOPLE PROGRAM IN ALBANIA

INTERNAL CONTROL

A Guide for Managers

INTERNAL CONTROL

A Guide for Managers

Prepared for publication by
Albania Rule of Law Program

Disclaimer

The views expressed in this publication do not necessarily reflect the views of the United States Agency for International Development (USAID) or the United States Government.

INTERNAL CONTROL

A Guide for Managers

Contents

INTRODUCTION.....	4
BACKGROUND	4
WHY DO WE NEED INTERNAL CONTROL?.....	5
INTERNAL CONTROL FRAMEWORK.....	7
WHAT IS INTERNAL CONTROL?	7
FOUR PURPOSES OF INTERNAL CONTROL	8
TYPES OF CONTROL.....	8
ORGANIZATIONAL ROLES.....	10
LIMITATIONS OF INTERNAL CONTROL.....	11
FIVE COMPONENTS OF INTERNAL CONTROL.....	13
1. CONTROL ENVIRONMENT.....	13
2. ASSESSING AND MANAGING RISK.....	17
3. CONTROL ACTIVITIES.....	20
4. INFORMATION AND COMMUNICATION	24
5. MONITORING.....	25
ANNEX 1: FIVE-STEPS IN EVALUATING INTERNAL CONTROL.....	28
STEP 1: CONTROL ENVIRONMENT ANALYSIS	28
STEP 2: ASSESSMENT OF RISK.....	30
STEP 3: REVIEW OF MANAGEMENT CONTROL ACTIVITIES.....	32
STEP 4: ASSESSMENT OF INFORMATION AND COMMUNICATION.....	33
STEP 5: EVALUATION OF MONITORING MECHANISMS	34
CONCLUSIONS ON INTERNAL CONTROL ASSESSMENT	35
PLAN TO ADDRESS INTERNAL CONTROL DEFICIENCIES	35
ANNEX 2: VULNERABILITY ASSESSMENT	37
VULNERABILITY ASSESSMENT WORKSHEET.....	40
ANNEX 3: INTERNAL CONTROL IN ALBANIA.....	41
MAIN ACTORS IN THE INTERNAL CONTROL ENVIRONMENT	41
ROLE OF THE GENERAL SECRETARY IN INTERNAL CONTROL.....	43
ROLE OF THE INSPECTOR GENERAL OF THE HIGH INSPECTORATE OF DECLARATION AND AUDIT OF ASSETS IN INTERNAL CONTROL	44
ROLE OF CENTRAL HARMONIZATION UNITS	44
PRESENT FLAWS IN INTERNAL CONTROL.....	46
ANNEX 4: CHU STRUCTURES.....	48
CHU-VERSION 1	48
CHU-VERSION 2	49
GLOSSARY OF CONTROL TERMS.....	50
GLOSSARY OF CORRUPTION TERMS	53
REFERENCES	57

INTRODUCTION

*"Management is doing things right; leadership is doing the right things."*¹

Planning, resourcing, directing, monitoring and controlling have been described as the five basic functions of management. Proper management control, which is synonymous with internal control, allows managers to delegate responsibilities to their staff and contractors with reasonable assurance that objectives will be achieved.

Internal control is an integral part of organization and management. It comprises the plans, methods, and procedures used to meet missions, goals, and objectives, and, in so doing, support performance-based management. Internal control also serves as the first line of defense in safeguarding assets and preventing and detecting errors and fraud. In short, internal control helps managers achieve desired results through the effective stewardship of public resources.

BACKGROUND

Internal control in Albania's public sector is generally considered to be weak because all of the components, elements and tools that enable effective internal control are not currently present. To start with, there is some confusion about the concept of "control". Historically, control in Albania and in other Eastern European countries implied "control revision". Internal control was synonymous with audit or inspection and was considered the responsibility of auditors or inspectors, and not management. Previous budget laws and other organic laws supported and confirmed this interpretation.

But, many of these laws have been changed over the years to reflect more modern management concepts in government. They set out concepts of accountability, authority and responsibility, delegation of authority, etc. and provide for better management mechanisms including internal control, internal audit, management responsibility, and so on.

Several policy papers on Public Financial Internal Control in Albania were drafted during 2005 and were approved by the Council of Ministers. These documents and action plans foresaw a series of developments in internal control with an ongoing need for update to keep them in line with new developments.

A series of laws, sub-regulatory acts and provisions that are elements of public internal financial control have now taken effect. The new organic budget law, "On Management of the Budgetary System" was passed in 2008. The law sets out rules and procedures in broad lines for drafting and implementing the state budget and every year, guidelines are to be provided for the application of this law.

¹ Peter F. Drucker

This law provides the rules of budgetary accounting in accordance with approved classification and sets forth sanctions for budgetary discipline. The law sets out authorities for budgetary actions into three categories: first authorizing officer; authorizing officer, and enforcing officer. The law also defines inspection, auditing, and reporting for the budgetary system. However, the law does not define rules and financial discipline for the use of funds which could be realized by regulations or by-laws.

The law “On Accounting”, which was originally approved in 1993, was amended by a new law passed in April 2004. This law sets out the standards of accounting for government and also provides for a group of other acts that are required to complete the framework for this law and for accounting, in general.

The law “On the Status of the Civil Servant”, approved in 1999, touches on several aspects of the administration of human resources. This law sets out some rules on the recruitment of civil servants, but does not extend to the analysis and use of these sources at the functional level. Neither does it stipulate organizational responsibilities for the development of human resources. In addition, while this law regulates the activity of human resources, it does so only for a small part of the entire public system.

The law “On Public Procurement,” its sub-regulatory acts, and a manual on public procurement comprise the framework for procurement. This framework will require monitoring and adjustment in the future as infractions and violations are identified during the implementation period of this law.

A new law has been drafted on internal audit, and positive developments have been noticed in the organization and functioning of the internal auditor profession in the public sector. However, a clearer division between the auditing activity and inspection will be required.

WHY DO WE NEED INTERNAL CONTROL?

Accountability. Public officials, legislators, and taxpayers are entitled to know whether government agencies are properly handling funds and complying with laws and regulations. They need to know whether government organizations, programs, and services are achieving the purposes for which they were authorized and funded. Officials and employees who manage programs must be accountable to the public. Public sector managers are responsible for managing the resources entrusted to them to carry out government programs. A major factor in fulfilling this responsibility is ensuring that adequate controls exist.

Encourage Sound Management Practices. Organizations exist to accomplish a goal. Managers are responsible for providing the leadership to reach this goal. That responsibility encompasses both identifying applicable laws and regulations and establishing internal control policies and procedures designed to provide reasonable assurance that the entity complies with those laws and regulations. Internal controls coordinates a department's policies and procedures to safeguard its assets, check the accuracy and reliability of its data, promote operational efficiency, and encourage adherence to prescribed managerial policies. Department managers must develop, implement, monitor, and update an effective plan of internal controls. The exact plan

developed will depend, in part, on management's estimation and judgment of the benefits and related costs of control procedures, as well as on available resources.

Fraud Prevention. Many opportunities for fraud exist when internal controls are missing or are inadequate. It is not sufficient to set up detection mechanisms alone, but prevention is also required. When reviews of internal controls do not take place, when there is poor supervision, when staff are unaware of the procedures to follow, when separation of duties is not established, when standard procedures for revenue collection and recording or issuance of contracts are not used, when there is little follow up of deficiencies, etc., the opportunity for fraud increases and the likelihood of detection decreases.

Facilitate Preparation for Audits. Each department is periodically subject to audits by independent auditors, federal auditors, the Internal Control Units of the Ministry of Finance and, in some cases, internal audit units. These audits are conducted to ensure the following:

- Public funds are administered and expended in compliance with applicable laws and regulations;
- Programs are achieving the purpose for which they were authorized and funded;
- Financial statements accurately represent the financial position of the government or entity;
- Programs are managed economically; and
- Internal controls exist and provide a basis for planning the audit and planning the timing, nature, and extent of testing.

Auditors' reports will nearly always include an opinion of the entity's internal controls. When it appears warranted, auditors will make recommendations for improvements. Managers are accountable for the adequacy of the internal control systems in their entities. Weak or insufficient internal controls will result in audit findings and, more importantly, could lead to theft, shortages, operational inefficiency, or a breakdown in the control structure.

INTERNAL CONTROL FRAMEWORK

WHAT IS INTERNAL CONTROL?

Internal Control helps an organization achieve its mission and objectives.

Many groups and organizations (e.g., Committee of Sponsoring Organizations (COSO), Canadian Institute of Chartered Accountants, INTOSAI, The US Government Accountability Office (GAO), etc.) have published standards and guidelines on internal control and defined it in various ways. Each of those definitions has captured the basic concept of internal control using different words. The definitions are similar in recognizing internal control's extensive scope, its relationship to an organization's mission, and its dependence on people in the organization.

Internal control is defined as follows:

Internal control is the integration of the activities, plans, attitudes, policies, and efforts of the people of an organization working together to provide reasonable assurance that the organization will achieve its objectives and mission.

This definition establishes that internal control:

- affects every aspect of an organization: all of its people, processes and infrastructure;
- is a basic element that permeates an organization, not a feature that is added on;
- incorporates the qualities of good management;
- is dependent upon people and will succeed or fail depending on the attention people give to it;
- is effective when all of the people and the surrounding environment work together;
- provides a level of comfort regarding the likelihood of achieving organizational objectives; and
- helps an organization achieve its mission.

Internal control is not an isolated action of a person or a group of people carried out at a given time, but a combination of actions, measures, and procedures performed by officers of an entity, as individuals and together, continually and throughout the entity's operations to achieve the objectives set by management. Internal control is:

- Carried out by people;
- Geared to the achievement of *objectives* in one or more separate but overlapping categories;
- A means to an end and not an end in itself;
- Expected to provide only *reasonable assurance*, not absolute assurance, to an entity's management and board;

- Not the sole responsibility of auditors but is the responsibility of managers at all levels; and
- Not one event or circumstance, but a series of actions that permeate an entity's activities;
- Not merely policy manuals and forms, but people at every level of an organization;

Internal control is focused on the achievement of the organization's mission. Therefore, it is essential that an organization has a clearly stated mission that is known and understood by everyone in the organization. It is also important to understand that, while good internal control will provide "reasonable assurance" that goals and objectives are met, good internal control cannot guarantee organizational success. However, goals and objectives are much less likely to be met if internal control is poor.

FOUR PURPOSES OF INTERNAL CONTROL

While the overall purpose of internal control is to help an organization achieve its mission, internal control also helps an organization to:

1. Promote orderly, economical, efficient and effective operations, and produce quality products and services consistent with the organization's mission;
2. Safeguard resources against loss due to waste, abuse, mismanagement, errors and fraud;
3. Promote adherence to laws, regulations, contracts and management directives; and
4. Develop and maintain reliable financial and management data, and accurately present that data in timely reports.

TYPES OF CONTROL

Classic forms of internal control that management undertakes to achieve its objectives are the following:

- Ex-ante control
- Ongoing control
- Ex-post control

Ex-ante controls are control activities undertaken by management to control activities before they are carried out. Usually ex-ante control is designed for activities that will have an important impact on the accomplishment of objectives. Such controls include the establishment of a signatory or authorization system. Through this control, senior management obtains information on the progress of the relevant activity and its expected results before this activity is undertaken. Examples include establishment of contracts, bank checks, and authorizations for transactions of considerable value.

Establishment of this control does not exclude other forms of control. In fact, it normally is also accompanied by both ongoing and ex-post controls because management simply undersigns or authorizes an action to provide the opportunity for that action to be completed. Yet management needs to know the concrete results of

that activity to check whether it has been carried out in compliance with predictions and authorizations.

Ongoing control – or control exercised during the accomplishment of an activity is an activity undertaken by management to monitor the accomplishment of projected activities and objectives. Monitoring includes supervision, reconciliation, comparison, implementation, evaluation, and reporting. To conduct effective monitoring, it is important to define indicators and the aspects of the activity or activities to be monitored. The ongoing control is very important because it can enable management to undertake corrective actions and construct supplementary controls when activities are not carried out in compliance with predictions.

Ex-post controls are activities projected by management to obtain information when activities to achieve the objectives have been conducted in accordance with the predictions, in compliance with the laws and regulations, and with effectiveness, efficiency, and economy. To achieve this, management develops several forms of controls, such as reporting and inspection. Another classification of internal controls is provided in accordance with the role they play during the accomplishment of an activity. They are:

- Preventive controls
- Detective controls
- Directive controls

Preventive controls are activities projected by management to prevent inefficient events, mistakes, irregularities, incorrect authorizations of payments or use of assets, etc. They are designed to minimize the occurrence of undesirable events or to lessen mistakes and irregularities. Examples of preventive controls include:

- Computer software controlling validation to prevent the entry of invalid account numbers and protect the accounting system from mistakes that lead to grave consequences in financial information
- Approval by managers of request for purchase of a necessary expense
- Limited access to data or assets only for authorized users
- Keeping dangerous things away from facilities where they could cause damage
- Running updated antivirus software on a PC and using a password for access
- Double-signatory system of transactions.

Detective controls aim to detect and repair undesirable events. They should be designed to detect a mistake or irregularity once it has occurred. Detective controls include subsequent confirmations of payments, verification of product stocks, and reconciliation of liquidities in the bank and cash box with the accounting records.

Directive controls are actions taken to cause or encourage a desirable event to occur. They are designed to assist in achieving established goals and objectives. Examples of directive controls include:

- Written and distributed policies and procedures
- Programs for the accomplishment of objectives
- Directives or orders at all management levels
- Clear elaboration of job descriptions
- Training workshops
- Rules on limited access to assets and information

ORGANIZATIONAL ROLES

Everyone in an organization has responsibility for internal control.

Internal control is people-dependent. It is developed by people; it guides people; it provides people with a means of accountability; and people carry it out. Individual roles in the system of internal control vary greatly throughout an organization. Very often, an individual's position in the organization determines the extent of that person's involvement in internal control.

Management's attitude, actions, and values set the tone of an organization, influencing the control consciousness of its people. Internal controls are likely to function well if management believes that those controls are important and communicates that view to employees at all levels. If management views internal controls as unrelated to achieving its objectives, or even worse, as an obstacle, this attitude will also be communicated.

Employees are aware of the practices followed by upper management including those that circumvent internal controls. Despite policies to the contrary, employees who note that their managers frequently override controls, will also view internal controls as "red tape" to be "cut through" or ignored, to get the job done.

Executive management needs to set the organization's "tone" regarding internal control. Management can show a positive attitude toward internal control by such actions as complying with their own policies and procedures, discussing internal controls at management and staff meetings, and rewarding employees for following good internal control practices. Although it is important to establish and implement policies and procedures, it is equally important to follow them.

Similarly, if individuals responsible for control activities are not attentive to their duties, internal control will not be effective. People can also deliberately defeat internal controls. For example, a manager can override a control activity because of time constraints, or two or more employees can act together in collusion to circumvent control and "beat the system." To avoid these kinds of situations, the organization

should continually monitor employee activity and emphasize the value of internal control.

While everyone in an organization has responsibility for ensuring the system of internal control is effective, the greatest amount of responsibility rests with the managers of the organization. Management has a role in making sure that the individuals performing the work have the skills and capacity to do so, and to provide employees with appropriate supervision, monitoring, and training to reasonably assure that the organization has the capability to carry out its work. The organization's top executive, as the lead manager, has the ultimate responsibility.

LIMITATIONS OF INTERNAL CONTROL

There is no perfect internal control system, because of inherent limitations that are typically uncontrollable.

Internal control, no matter how well conceived and operated, can provide only reasonable - *not absolute* - assurance that objectives will be achieved. Judgments in decision-making can be faulty. Breakdowns can occur because of simple error or mistake. Controls can be circumvented by the collusion of two or more people, and management may choose to override the system. There are also resource constraints, and the benefits of controls must be considered relative to their costs. Below are some limitations that affect internal control, and systems in support of good internal control.

Misunderstanding of instructions, regulations, and procedures. Internal control is the entirety of rules and procedures drafted by management to achieve objectives. Yet instructions implemented by people are prone to failure if their implementers do not understand them well. Misunderstanding of instructions may be the consequence of several factors. Unclear instructions are likely to be misunderstood; instructions may not be drafted in support of objectives or the organization's environment; or instructions may be related to the qualifications of the people who enforce them.

Costs versus benefits. Prohibitive cost can prevent management from installing the ideal internal control systems or mechanisms. Management will accept certain risks because the cost of preventing such risks cannot be justified. Furthermore, **more** control activities are not necessarily **better** for effective internal control.

Judgment. The effectiveness of internal controls is limited by the realities of human frailty in making decisions. Decisions often must be made under the pressure of time constraints, on the basis of limited information at hand, and rely on human judgment. Management may fail to anticipate certain risks and thus fail to design and implement appropriate controls.

Collusion. Collusion between two or more individuals can result in internal control failures. Individuals acting collectively to perpetrate and conceal an action from detection often can alter financial data or other management information in a manner that circumvents control activities and cannot be identified by the system of internal

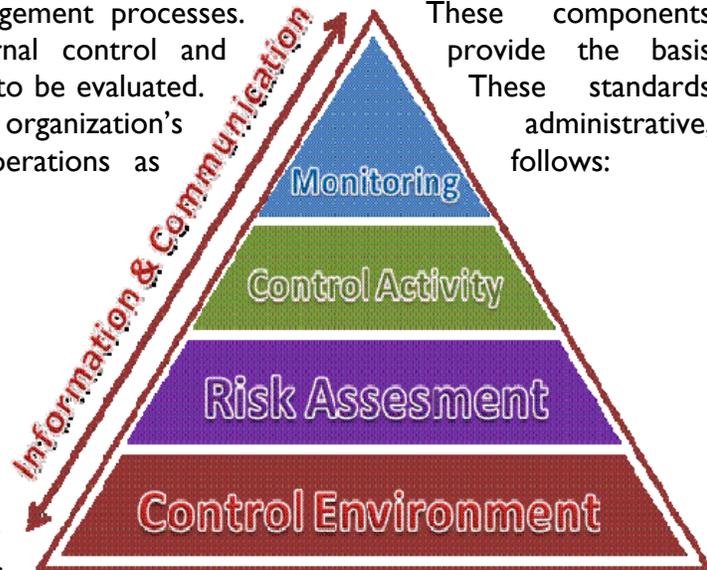
control. For example, a collusive activity between the cashier and the person in the organization assigned to register its accounting actions may lead to money theft and the disappearance of information on money transactions.

Management Override. No matter how sound systems of internal control are designed, management override will lessen, or even eliminate, their effectiveness. For example, a decision of a manager to select an inferior candidate despite a rigorous process having identified another better candidate, negates the effectiveness of the policies and procedures designed to identify and select the best candidate.

FIVE COMPONENTS OF INTERNAL CONTROL

The internal control process consists of five interrelated components that are derived from and integrated with management processes. These components define the standards for internal control and against which internal control is to be evaluated. These standards apply to all aspects of an organization's administrative, financial, and programmatic operations as follows:

1. Control environment;
2. Risk assessment;
3. Control activities;
4. Information and communication; and
5. Monitoring.



Managers are responsible for developing the detailed policies, procedures, and practices to fit their organization's operations and mission.

I. CONTROL ENVIRONMENT

Management and employees should establish and maintain an environment throughout the organization that sets a positive and supportive attitude toward internal control and conscientious management.

The control environment is the attitude toward internal control and control consciousness established and maintained by the management and employees of an organization. It is a product of management's governance, that is, its philosophy, style and supportive attitude, as well as the competence, ethical values, integrity and morale of the people of the organization. The control environment is further affected by the organization's structure and accountability relationships.

The control environment has a pervasive influence on the decisions and activities of an organization, and provides the foundation for the overall system of internal control. If this foundation is not strong or if the control environment is not positive, the overall system of internal control will not be as effective as it should be.

The following describes how management is responsible for creating a positive control environment and how employees are responsible for helping to maintain this environment.

Governance is the influence on an organization exercised by the executive body or the chief executive which/who governs it. The executive body may be a board of directors,

board of trustees, council, legislature or similar entity. The chief executive may be the president, chancellor, commissioner, chief judge or an individual elected or appointed as the highest ranking person in the organization. Their governance responsibilities are usually founded in a constitution, charter, laws, by-laws, regulations and other similar documents. The leadership, actions and tone established and practiced by the governing body/executive can have a profound impact on how the employees of the organization perform their responsibilities, which in turn affects the achievement of the organization's mission.

Among the critical areas influenced by the governing body/executive are:

- approving and monitoring the organization's mission and strategic plan;
- establishing, practicing, and monitoring the organization's values and ethical code;
- overseeing the decisions and actions of senior managers;
- establishing high-level policy and organization structure;
- ensuring and providing accountability to stakeholders;
- establishing the overall management style, philosophy and "tone"; and
- directing management oversight of key business processes.

Ethical Values and Integrity are key elements contributing to a good control environment. Ethical values are the standards of behavior that form the framework for employee conduct. An organization's culture evolves from the values of its members and the culture, in turn, exerts a strong influence on the actions, decisions, and behaviors of all employees.

Ethical values guide employees when they make decisions. Management addresses the issue of ethical values when it encourages:

- commitment to honesty and fairness;
- recognition of and adherence to laws and policies;
- respect for the organization;
- leadership by example;
- commitment to excellence;
- respect for authority;
- respect for employees' rights; and
- conformance with professional standards.

People in an organization have personal and professional integrity when they adhere to ethical values. While it is management's responsibility to establish and communicate the ethical values of the organization, it is everyone's responsibility to demonstrate integrity. Management encourages integrity by:

- establishing and publishing a code of conduct;
- complying with the organization's ethical values and code of conduct;
- rewarding employee commitment to the organization's ethical values;
- establishing methods for reporting ethical violations; and
- consistently enforcing disciplinary practices for all ethical violations.

An ethical culture requires engaged employees and managers who understand why doing the right thing is important for the organization's long-term viability; and they have the determination to see that in fact the right thing does get done.

Some of the key attributes needed for an organization to be fully integrity-based are as follows:

- Employees feeling a sense of responsibility and accountability for their actions and for the actions of others;
- Employees freely raising issues and concerns without fear of retaliation;
- Managers modeling the behaviors they demand of others;
- Managers communicating the importance of integrity when making difficult decisions;
- Leadership understanding the pressure points that drive unethical behavior; and
- Leadership developing processes to identify and remedy these areas where pressure points occur.

Management Operating Style and Philosophy reflects management's basic beliefs regarding how the people and activities of an organization should be managed. There are many styles and philosophies. Although none are inherently right or wrong, some may be more effective than others in helping a particular organization accomplish its mission. Management should practice the most effective style and philosophy for the organization, making sure that they reflect the ethical values of the organization, and positively affect staff morale. Management should practice and clearly communicate and demonstrate these beliefs to staff and periodically evaluate whether the style and philosophy are effective and are practiced consistently.

Management's philosophy and style can be demonstrated in such areas as: management's approach to recognizing and responding to risks (both internal and external); acceptance of regulatory control imposed by others; management's attitude toward internal and external reporting; the use of aggressive or conservative accounting principles; the attitude of management toward information technology and accounting functions; and management's support for and responsiveness to internal and external audits and evaluations.

Competence is a characteristic of people who have the skill, knowledge and ability to perform tasks. Management's responsibility for ensuring the competency of its employees should begin with establishing appropriate human resource policies and practices that reflect a commitment to:

- establishing levels of knowledge and skill required for every position;
- verifying the qualifications of job candidates;
- hiring and promoting only those with the required knowledge and skills; and
- establishing training programs that help employees increase their knowledge and skills.

Management should also ensure that employees have what they need to perform their jobs, such as equipment, software and policy and procedure manuals as well as the tools and support they need to perform their tasks.

Morale is the attitude people have about their work, as exhibited by their confidence, discipline and willingness to perform tasks. Management should recognize the importance of good morale in an effective control environment. People's attitude about their jobs, work environment and organization affects how well they do their jobs. Management should monitor the level of staff morale to ensure employees are committed to helping the organization accomplish its mission.

Management should also take actions to maintain high morale. Such actions should provide staff with a sense that:

- their opinions and contributions are welcomed, valued and recognized;
- the organization is willing to help improve their level of competency;
- there is opportunity for continuous improvement;
- they have a stake in the mission, goals and objectives of the organization;
- the organization's appraisal and reward systems are fair and consistent; and
- the lines of communication are open.

Supportive Attitude is a disposition that encourages desired outcomes. Since internal control provides management with reasonable assurance that the organization's mission is being accomplished, management should have a supportive attitude toward internal control that permeates the organization. Executive management should set a tone that emphasizes the importance of internal control. Such a tone is characterized by:

- minimal and guarded use of control overrides;
- support for conducting control self-assessments and internal and external audits;
- responsiveness to issues raised as the result of the evaluations and audits; and
- ongoing education to ensure everyone understands the system of internal control and their role in it.

Mission is the organization's reason for existing. It provides a sense of direction and purpose to all members of the organization, regardless of their position, and provides a guide when making critical decisions. During periods of change, it provides cohesion to the organization and helps keep it on its proper course. Without a clearly defined and communicated mission, an organization may drift aimlessly and accomplish little.

The mission of an organization should be a statement, approved by executive management and/or the governing board of the organization. Management should tell employees about the organization's mission and explain how their jobs contribute to accomplishing the mission. The mission statement will be most effective if all employees perceive they have a personal stake in it.

As time passes, both internal and external changes can affect the organization's mission. Therefore, management should periodically review the mission and update it, as necessary, for adequacy and relevancy.

Structure is the framework in which the organization's plans are carried out. It should define the functional sub-units of an organization and the relationships among them. An organization chart can provide a clear picture of the authority and accountability relationships among functions. The chart should be provided to all employees to help them understand the organization as a whole, the relationships among its various components and where they fit into the organization. Management should review this chart periodically to ensure it accurately reflects the organization's structure.

Management should delegate authority and responsibility throughout the organization. Management is responsible for organizing the entity's authority and accountability relationships among various functions to provide reasonable assurance that work activities are aligned with organizational objectives. With increased delegation of authority and responsibility, there is a need to provide qualified and continuous supervision, and to monitor results. Supervision throughout the organization helps ensure that employees are aware of their duties and responsibilities, and know the extent to which they are accountable for activities.

2. ASSESSING AND MANAGING RISK

Risk is the uncertainty that an event can occur that may have a negative impact on the accomplishment of objectives.

Risk should be assessed and managed through an organization-wide effort to identify, evaluate and monitor those events that threaten the accomplishment of the organization's mission. For each risk that is identified, management should decide whether to accept the risk, reduce the risk to an acceptable level, or avoid the risk.

Preparing to Assess Risk. Management should first ensure that it has identified all the operational and control objectives throughout the organization. Control objectives are generally derived from the four purposes of internal control and are stated in terms that reflect the responsibilities of the organization's sub-units. For example, the following two control objectives are derived from the first two purposes of internal control:

- *Ensure all applications are processed accurately* (from the first purpose of internal control: to promote orderly, economical, efficient and effective operations, and produce quality products and services consistent with the organization's mission).
- *Ensure access to electronic files is restricted to authorized personnel* (from the second purpose of internal control: to safeguard resources against loss due to waste, abuse, mismanagement, errors and fraud).

After identifying all the operational and control objectives, managers should identify all the risks associated with each objective (i.e., the events that would threaten the

accomplishment of each objective). These risks can be both internal (e.g., human error, fraud, system breakdowns) and external (e.g., changes in legislation, natural disasters). It is essential that managers within the organization identify the risks associated with their respective objectives.

Risk Assessment Process. *Internal control should provide for an assessment of the risks that an organization faces from both external and internal sources.*

Risk Matrix

LIKELIHOOD	High			
	Medium			
	Low			
		Low	Medium	High
		IMPACT (CONSEQUENCE)		
Overall risk evaluation:		Low	Medium	High

Management should evaluate each identified risk in terms of its likelihood of occurrence and its impact or consequence, as follows:

- **Likelihood** of occurrence is the probability that an unfavorable event would occur if there were no control activities (as described in the following section) to prevent or reduce the risk. A likelihood of occurrence should be estimated for each identified risk.
- **Impact** is the effect an unfavorable event would have on the organization if the event were to occur. This effect could be some type of harm or an opportunity that would be lost. If possible, this effect should be quantified. At the very least, this effect should be described in terms that are specific enough to indicate the significance of the impact.

The chart, above, depicts a reasonable approach to evaluating risks, with the lower left corner of the chart representing the lowest risk and upper right representing the highest priority risks. Management should use judgment to establish priorities for risks based on their likelihood of occurrence and their impact. Risks should be ranked in a logical manner, from the most significant (high impact) and most likely to occur (high likelihood) - as indicated in the far-right corner - to the least significant (low impact) and least likely to occur (low likelihood), as indicated in lower-left corner of the graph.

For example, a program manager has two cash accounts. One is the office petty cash fund and the other is for fees and fines from a program activity. Most people would consider the petty cash to be a lower risk assessment. When fees and fines, which are substantial in amount, are discovered to be stored in an open location and there is a six-month backlog in processing them, this would be a high risk assessment.

Management should use the information obtained from this assessment to help determine:

- how to manage risk;
- how to prevent or reduce risk; and
- how to manage risk during change.

Managing Risk. Executive management should provide guidance to managers throughout the organization to help them assess the level and the kinds of risk that are acceptable and not acceptable. Using this guidance and the risk assessment information, managers should determine whether to accept the risk in a given situation, prevent or reduce the risk, or avoid the risk entirely. For example, in deciding how to manage the risk that unauthorized persons could gain access to electronic files, managers should consider the following possibilities:

- *Accept the risk: Do not establish control activities* - Management can accept the risk of unauthorized access because the consequences of such access are not significant; for example, the files may contain data that is not sensitive. Management might also choose to accept the risk if the cost of the associated control activities is greater than the cost of the unfavorable event.
- *Prevent or reduce the risk: Establish control activities* - Management cannot accept the current level of risk of unauthorized access because the files contain confidential or otherwise inherently valuable data. Therefore, management establishes control activities that are intended to prevent the risk of unauthorized access, or at least reduce the risk to an acceptable level. However, the risk is prevented or reduced only as long as the control activities function as intended.
- *Avoid the risk: Do not carry out the function* - Management determines that it cannot tolerate any risk of unauthorized access to the files or that it cannot adequately control such access. For example, a file may contain extremely sensitive data, or access controls may not be feasible. In this case, management may decide that the impact of any unauthorized access to this file would be too risky or that access is too difficult or too costly to control. Therefore, management decides not to carry out this function (i.e., decides not to maintain the data electronically).

Preventing or Reducing Risk. *Risk management and internal control are two sides of the same coin.* When preventing risk or reducing it to an acceptable level, managers should use risk assessment information to help identify the most effective and efficient control

activities available for handling the risk. Specifically, manager should answer the following questions:

- *What is the cause of the risk?* Managers should consider the reason the risk exists to help identify all the possible control activities that could prevent or reduce the risk.
- *What is the cost of control vs. the cost of the unfavorable event?* Managers should compare the cost of the risk's effect with the cost of carrying out various control activities, and select the most cost-effective choice.
- *What is the priority of this risk?* Managers should use the prioritized list of risks to help decide how to allocate resources among the various control activities used to reduce the risks. The higher the priority, the greater the resources allocated to the control activities intended to reduce the risk.

Management should maintain its analysis and interpretation of the risk assessment information as part of its documentation of the rationale that supports its risk management decisions. Management should review these decisions periodically to determine whether changes in conditions warrant a different approach to managing, preventing and reducing risk.

3. CONTROL ACTIVITIES

Internal control activities help ensure that management's directives are carried out. The control activities should be effective and efficient in accomplishing the organization's control objectives.

Control activities are tools - both manual and automated - that help identify, prevent or reduce the risks that can impede accomplishment of the organization's objectives. Management should establish control activities that are effective and efficient. When designing and implementing control activities, management should try to obtain the maximum benefit at the lowest possible cost. A few simple rules follow:

- The cost of the control activity should not exceed the cost that would be incurred by the organization if the undesirable event occurred.
- Management should build control activities into business processes and systems as the processes and systems are being designed. Adding control activities after the development of a process or system is generally more costly.
- The allocation of resources among control activities should be based on the significance and likelihood of the risk they are preventing or reducing.

Many different control activities can be used to address the risks that threaten an organization's success. Most control activities, however, can be grouped into two categories: prevention and detection control activities.

- *Prevention activities* are designed to deter the occurrence of an undesirable event. The development of these controls involves predicting potential problems before they occur and implementing ways to avoid them.
- *Detection activities* are designed to identify undesirable events that do occur, and alert management about what has happened. This enables management to take corrective action promptly.

Prevention controls tend to be more expensive than detection controls. Costs and benefits should be assessed before control activities are implemented. Management should also remember that an excessive use of prevention controls can impede productivity. No one control activity provides all of the answers to risk management problems. In some situations, a combination of control activities should be used, and in others, one control activity could substitute for another.

The following are descriptions of some of the more commonly used control activities.

Documentation. Documentation involves preserving evidence to substantiate a decision, event, transaction or system. All documentation should be complete, accurate and recorded timely. Documentation should have a clear purpose and be in a usable format that will add to the efficiency and effectiveness of the organization. Examples of areas where documentation is important include critical decisions, significant events, transactions, policies, procedures and the system of internal control.

Critical decisions and significant events usually involve executive management. These decisions and events usually result in the use, commitment, exchange or transfer of resources such as in strategic plans, budgets and executive policies. By recording the information related to such events, management creates an organizational history that can serve as justification for subsequent actions and decisions and will be of value during self-evaluations and audits.

Documentation of transactions should enable managers to trace each transaction from its inception through its completion. This means the entire life cycle of the transaction should be recorded, including: (1) its initiation and authorization; (2) its progress through all stages of processing; and (3) its final classification in summary records. For example, the documentation for the purchase of equipment would start with the authorized purchase request, and continue with the purchase order, the vendor invoice and the final payment documentation.

Documentation of policies and procedures is critical to the daily operations of an organization. These documents set forth the fundamental framework and the underlying methods and processes all employees rely on to do their jobs. They provide specific direction to and help form the basis for decisions made every day by employees.

Without this framework of understanding by employees, conflict can occur, poor decisions can be made and serious harm can be done to the organization's reputation. Further, the efficiency and effectiveness of operations can be adversely affected.

The documentation of an organization's system of internal control should include the organization's structure, policies, assessable units, control objectives and control activities. The various aspects of a system of internal control can be represented in narrative form, such as in policy and procedure manuals, and/or in the form of flowcharts or matrices.

Approval and Authorization. Approval is the confirmation or sanction of employee decisions, events or transactions based on a review. Management should determine which items require approval based on the level of risk to the organization without such approval. Management should clearly document its approval requirements and ensure that employees obtain approvals in all situations where management has decided they are necessary. For example, a manager reviews a purchase request from an employee to determine whether the item is needed. Upon determining the need for the item, the manager signs the request indicating approval of the purchase.

Authorization (sometimes referred to as delegation of authority) is the power management grants employees to carry out certain duties, based on approval received from supervisors. Authorization is a control activity designed to ensure events or transactions are initiated and executed by those designated by management. Management should ensure that the conditions and terms of authorizations are clearly documented and communicated, and that significant transactions are approved and executed only by persons acting within the scope of their authority. For example, a manager may be authorized by his/her supervisors to approve purchase requests, but only those up to a specified dollar amount.

Verification. Verification is the determination of the completeness, accuracy, authenticity and/or validity of transactions, events or information. It is a control activity that enables management to ensure activities are being done in accordance with directives. Management should determine what needs to be verified, based on the risk to the organization if there were no verification.

Management should clearly communicate and document these decisions to those responsible for conducting the verifications. An example of verification is ensuring that a fair price has been obtained in a purchase and funds are available to pay for the purchase.

Supervision. Supervision is the ongoing oversight, management and guidance of an activity by designated employees to help ensure the results of the activity achieve the established objectives. Those with the responsibility for supervision should:

- monitor, review and approve, as appropriate, the work of those performing the activity to ensure the work is performed correctly;
- provide the necessary guidance and training to help minimize errors and waste and to ensure that employees understand and follow management directives; and
- clearly communicate the duties and responsibilities assigned to those performing the activities.

An example of supervision is when an assigned employee (supervisor) reviews the work of another employee processing a purchase order to determine whether it is prepared accurately and completely, and has been properly authorized. The supervisor then signs the order to signify his/her review and approval. However if there are any errors, the supervisor would return the order to the employee and explain how to complete the request properly.

Separation of Duties. Separation of duties is the division of key tasks and responsibilities among various employees and sub-units of an organization. By separating key tasks and responsibilities - such as receiving, recording, depositing, securing and reconciling assets - management can reduce the risk of error, waste, or wrongful acts. The purchasing cycle is an area where the separation of duties can minimize the risk of inappropriate, unauthorized or fraudulent activities. Specifically, the various activities related to a purchase (initiation, authorization, approval, ordering, receipt, payment and recordkeeping) should be done by different employees or sub-units of an organization. In cases where tasks cannot be effectively separated, management can substitute increased supervision as an alternative control activity that can help prevent or reduce these risks.

Safeguarding Assets. The safeguarding of assets involves restricting access to resources and information to help reduce the risk of unauthorized use or loss. Management should protect the organization's equipment, information, documents and other resources that could be wrongfully used, damaged or stolen. Management can protect these resources by limiting access only to authorized individuals. Access can be limited by various means such as locks, passwords, electronic firewalls and encryption. Management should decide which resources should be safeguarded and to what extent. Management should make this decision based on the vulnerability of the items being secured and the likelihood of loss.

Control Activities for Information Technology. While some of the control activities relating to information technology (IT) are the responsibility of specialized IT personnel, other IT control activities are the responsibility of all employees who use computers in their work. For example, any employee may use:

- encryption tools, protocols, or similar features of software applications that protect confidential or sensitive information from unauthorized individuals;
- back-up and restore features of software applications that reduce the risk of lost data;
- virus protection software; and
- passwords that restrict user access to networks, data and applications.

IT control activities can be categorized as either general or application controls. General controls apply to all computerized information systems - mainframe, minicomputer, network and end-user environments. Application controls apply to the processing of data within the application software.

General and application controls are interrelated. General controls support the functioning of application controls, and both types of controls are needed to ensure complete and accurate information processing.

4. INFORMATION AND COMMUNICATION

Information should be recorded and communicated to management and others within the organization who need it and in a form and within a time frame that enables them to carry out their internal control activities and other responsibilities.

For an organization to manage and control its operations, it must have relevant, valid, reliable, and timely communication relating to internal and external events. Managers must be able to obtain reliable information to determine their risks and communicate policies and other information to those who need it.

Reporting is a means of conveying information. It serves as a control when it provides information on issues such as timely achievement of goals, budget status and employee concerns. Reporting also helps to promote accountability for actions and decisions. An example of a report that serves as a control activity would be one that compares purchasing activities with the approved budget, indicating and explaining significant variances between the two.

Effective and accurate reporting serves as a control when it provides information on issues such as financial position, employee concerns, and the timely achievement of goals. Reporting also helps to promote accountability for actions and decisions. The list below offers some examples of effective and accurate reporting.

- Project status reports to alert management to potential cost or time overruns;
- Reports to monitor employee leave balances, position vacancies, and staff turnover to determine effectiveness of workplace and employment practices; and
- The Annual Financial Report issued for the public's review of financial performance and position.

Communication is the exchange of useful information between and among people and organizations to support decisions and coordinate activities. Information should be communicated to management and other employees who need it in a form and within a time frame that helps them to carry out their responsibilities. Communication with customers, suppliers, regulators and other outside parties is also essential to effective internal control.

Information can be communicated verbally, in writing and electronically. While verbal communication may be sufficient for many day-to-day activities, it is best to document important information. This provides a more permanent record and enables managers and others to review the information. Information should travel in all directions to ensure that all members of the organization are informed and that decisions and actions of different units are communicated and coordinated.

A good system of communication is essential for an organization to maintain an effective system of internal control. A communication system consists of methods and records established to identify, capture and exchange useful information. Information is useful when it is timely, sufficiently detailed and appropriate to the user.

Management should establish communication channels that:

- provide timely information;
- can be tailored to individual needs;
- inform employees of their duties and responsibilities;
- enable the reporting of sensitive matters;
- enable employees to provide suggestions for improvement;
- provide the information necessary for all employees to carry out their responsibilities effectively;
- convey top management's message that internal control responsibilities are important and should be taken seriously; and
- convey and enable communication with external parties.

Communication is not an isolated internal control component. It affects every aspect of an organization's operations and helps support its system of internal control. The feedback from this communication network can help management evaluate how well the various components of the system of internal control are working.

5. MONITORING

Monitoring is the review of the organization's activities and transactions to assess the quality of performance over time and to determine whether controls are effective.

Management should focus monitoring efforts on internal control and achievement of the organization's mission. For monitoring to be most effective, all employees need to understand the organization's mission, objectives, risk tolerance levels and their own responsibilities.

Everyone within an organization has some responsibility for monitoring. The position a person holds in the organization helps to determine the focus and extent of these responsibilities. Therefore, the monitoring performed by staff, supervisors, mid-level managers and executives will not have the same focus, as follows:

- **Staff** - The primary focus of staff should be on monitoring their own work to ensure it is being done properly. They should correct the errors they identify before work is referred to higher levels for review. Management should educate staff regarding control activities and encourage them to be alert to and report any irregularities. Because of their involvement with the details of the organization's daily operations, staff has the best vantage point for detecting any problems with existing control activities. Management should also remind staff to

note changes in their immediate internal and external environments, to identify any risks and to report opportunities for improvement.

- **Supervisors** - Supervision is a key element of monitoring. Supervisors should monitor all activities and transactions in their unit to ensure that staff are performing their assigned responsibilities, control activities are functioning properly, the unit is accomplishing its goals, the unit's control environment is appropriate, communication is open and sufficient, and risks and opportunities are identified and properly addressed.
- **Mid-Level Managers** - Mid-level managers should assess how well controls are functioning in multiple units within an organization, and how well supervisors are monitoring their respective units. The focus of these managers should be similar to that of supervisors, but extended to cover all the units for which they are responsible.
- **Executive Management** - Executive management should focus their monitoring activities on the major divisions of the organization. Because of this broader focus, executive managers should place even more emphasis on monitoring the achievement of the organization's goals. Executive managers should also monitor for the existence of risks and opportunities in either the internal or external environment that might indicate the need for a change in the organization's plans.

Management should ensure that it takes the proper actions to address the results of monitoring. For example, management may decide to establish new goals and objectives to take advantage of newly identified opportunities, may counsel and retrain staff to correct procedural errors, or may adjust control activities to minimize a change in risk.

The monitoring performed by staff, supervisors, mid-level managers and executives should focus on the following major areas:

- **Mission:** Monitoring activities should include the development and review of operational data that would allow management to determine whether the organization is achieving its mission. This can be achieved by periodic comparison of operational data to the organization's strategic plan.
- **Control Environment:** Executive management should monitor the control environment to ensure that managers at all levels are maintaining established ethical standards of behavior and that staff morale is at an appropriate level. Managers should also ensure that the staff is competent, that training is sufficient and that management styles and philosophies foster accomplishment of the organization's mission.
- **Risks and Opportunities:** Managers should also monitor the organization's internal and external environment to identify any changes in risks and the

development of opportunities for improvement. If changes are identified, managers should take appropriate action to address these new or changed risks and opportunities. Management should recognize that delays in responding to risks could result in damage to the organization and a missed opportunity may result in a loss of new revenue or savings.

- **Control Activities:** Control activities are established to prevent or reduce the risk of an unfavorable event from occurring. If these activities fail, the organization becomes exposed to risk. Control activities can fail when controls are overridden, or when there is collusion for fraudulent purposes. Therefore, management should establish procedures to monitor the functioning of control activities and the use of control overrides. Management should also be alert to signs of collusion. Effective monitoring gives management the opportunity to correct any control activity problems and to control the risk before an unfavorable event occurs.
- **Communication:** Managers should periodically verify that the employees they are responsible for are receiving and sharing information appropriately, and that this information is timely, sufficient and appropriate for the users. Management should ensure that there are open lines of communication, which fosters reporting of both positive and negative results.

ANNEX I: FIVE-STEPS IN EVALUATING INTERNAL CONTROL

An organization is a living entity which changes over time. As a result, the organization's mission, goals and objectives must regularly be evaluated and periodically revised. After an organization analyzes its goals and objectives to determine what might prevent it from achieving them (i.e., its risks), management must analyze these risks and evaluate the policies and procedures in place to minimize or mitigate them in the identified high-risk areas. Internal controls are those systems and practices that an organization uses to minimize risk to the achievement of objectives.

Part of the management process includes monitoring the progress made toward meeting goals and objectives. Monitoring also helps to ensure the effectiveness of the organization's internal controls and the effectiveness of the policies and procedures. Periodically, policies and procedures should be revised to mitigate risk and eliminate redundancy. These policies and procedures must also be communicated internally and externally, as necessary.

An evaluation of internal control is a detailed examination of the functions of a unit (e.g., ministry, department, agency, municipality, etc.), undertaken to determine whether internal control is functioning properly and is appropriate for the circumstances. The evaluation is then used to make any necessary improvements. Evaluation of internal controls is the responsibility of management and part of every manager's daily responsibilities.

There are many ways and methods to evaluate internal control. But, the five-step method ensures a quick and appropriate evaluation. The five steps correspond to the five components of internal control. Managers should apply this method to every unit for which they are responsible. They should start by reviewing the goals and objectives of the entity, and then identifying the specific risks to achieving these objectives. Managers should then decide which risks are highest and the policies, systems and procedures (i.e., control activities) necessary to mitigate those risks. The five steps are as follows:

STEP I: CONTROL ENVIRONMENT ANALYSIS

Internal controls are likely to function well if management believes that those controls are important and communicates that view to employees at all levels. If management views controls as unrelated to achieving its objectives, or even worse, as an obstacle, this attitude will also be communicated. Despite policies to the contrary, employees will then view internal controls as "red tape" to be "cut through" to get the job done. An effective internal control environment:

- Sets the tone of an organization influencing the control consciousness of its people.
- Is an intangible factor that is the foundation for all other components of internal control, providing discipline and structure.

- Describes "organizational culture".
- Includes a commitment to hire, train, and retain qualified staff.
- Encompasses both technical competence and ethical commitment.

The control environment sets the tone of an organization, influencing the control consciousness of its staff. It is the foundation for all other components of internal control, providing discipline and structure and providing the basis for whether internal controls are likely to be designed and managed properly. If, for example, management attitude toward internal control is not serious despite stated support for internal control; if there is little supervision, little trust, poor communication, little encouragement for innovation, lack of a sharing of ideas and work, and little motivation; and if goals and objectives are not clear and there is little shared vision among staff and management, then there is little chance of any internal control systems and procedures that have been developed to do their work – that is, to help the organization achieve its mission in an efficient and effective manner while safeguarding its assets and being accountable for the use of its resources.

Accordingly, Step 1 identifies the strengths and the weaknesses of the control environment and attempts to answer the following questions:

- (1) Are the personal and professional integrity and ethical values of management and staff evident?
- (2) Do managers and employees 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?
- (3) Do management's policies, procedures and practices provide a supportive attitude toward internal control at all times, independence, competence and leading by example and do they promote orderly, ethical, economical, efficient and effective conduct of operations?
- (4) Does the organizational structure of the entity provide assignment of authority and responsibility; empowerment and accountability; and appropriate lines of reporting?
- (5) Do human resource policies and practices by which persons are hired, trained, evaluated, compensated, and promoted support an ethical environment by developing professionalism and enforcing transparency?
- (6) Are the mission and objectives of the organization well understood, supported by management and staff, clear, complete, linked to the mandate, and measurable?

A generally strong control environment will provide some basis for assessing whether internal control systems and practices are likely to be functioning as intended. A weak one will caution the assessor to pay more attention to the identification of risks and the existence of management control activities to mitigate those risks.

STEP 2: ASSESSMENT OF RISK

A risk is anything that endangers the achievement of an objective. What could go wrong? What assets need to be protected?

- Risk assessment is the process used to identify, analyze, and manage the potential risks that could hinder or prevent an agency from achieving its objectives.
- Risk increases during a time of change, for example, turnover in personnel, rapid growth, or establishment of new services.
- Other potential high risk factors include complex programs or activities, cash receipts, direct third party beneficiaries, and prior problems.

Risk assessment, as the second component of internal control, plays a key role in the identification of critical areas and the selection of the appropriate control activities (policies, systems and procedures) to undertake in these areas. Risk analysis is the process of identifying and analyzing relevant risks to the achievement of the entity's objectives and determining the appropriate response.

A strategic approach to risk assessment depends on identifying risks against key organizational 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.

Two of the most commonly used tools are commissioning a risk review and, a risk self assessment. A risk review is a top down procedure. A team is established to consider all the operations and activities of the organization in relation to its objectives and to identify the associated risks. The team conducts a series of interviews with key members of staff at all levels of the organization to build a risk profile for the whole range of activities thereby identifying the policy fields, activities and functions which may be particularly vulnerable to risk (including the risk of fraud and corruption).

A risk self assessment is a bottom up approach. Each level and part of the organization is invited to review its activities and feed diagnosis of the risks faced upwards. This may be done through a documentation approach (with a framework 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 entity-wide and activity level risks.

Risk analysis is a two-step process:

- identifying possible events that, should they occur, would prevent the entity from attaining its objectives; and
- assessing the possible magnitude and likelihood of each event.

The resultant risks are classified according to their severity and those that are the highest, will point to the areas (e.g., activity, function, entity, system, practice, etc.) that need to be addressed through sound control activities or other mechanisms. An important issue in considering a 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.

Step 2 of the evaluation determines whether:

- (1) An appropriate assessment of risks has taken place?
- (2) Management has defined the “risk appetite” of the entity?
- (3) Those areas that have highest risk are identified and responses to these risks are developed (e.g., transferred, tolerated, terminated or treated)?

Below, are twelve characteristics of vulnerability (risk) which apply to any human endeavor – government or private sector, non-profit or commercial. A consideration of each characteristic can help determine if the management controls in place are proportionate to the risk, and appropriate to the environment.

- | | |
|---|-------------------------------------|
| 1. Operational Stability | 7. Physical Assets |
| 2. Organizational Structure | 8. Authorizations |
| 3. Policies & Procedures | 9. Frequency of Reviews |
| 4. Sensitivity/Complexity of Operations | 10. Reliance on Information Systems |
| 5. Personnel | 11. Influence |
| 6. Financial Assets | 12. Impact of Failure |

Each of these areas can be evaluated for the risks inherent in the organization, related to the specific function under review. **Annex 2** provides guidance and a worksheet to assist the determination of these risks but other mechanisms may also be used. An overall rating for each function or entity of High, Moderate or Low risk is derived from a combination of these twelve risk assessments.

Functions with HIGH vulnerability may be characterized by complex/sensitive operations, with high staff turnover, handling significant cash receipts. Failure to prevent or detect misuse of assets can seriously damage the agency's reputation and mission.

Functions with LOW vulnerability rely on qualified/trained staff, provide good documentation of policies & procedures and are subject to frequent outside review of operations. Potential for misuse of significant assets is low, or may not reflect directly on the agency's reputation and mission.

STEP 3: REVIEW OF MANAGEMENT CONTROL ACTIVITIES

Organizations establish policies and procedures so that identified risks do not prevent an organization from reaching its objectives.

- Clearly identified activities minimize risk and enhance effectiveness.
- Internal control activities are nothing more than policies, procedures, and the organizational structure of an organization.
- Control activities can be either preventive, for example, requiring supervisory sign off, or detective, for example reconciling reports.
- Need to avoid excessive controls, which are as harmful as excessive risk and result in increased bureaucracy and reduced productivity.

Risk assessment plays a key role in the selection of appropriate control activities to undertake. As indicated, it is not possible to eliminate all risk and internal control can only provide reasonable assurance that the objectives of the organization 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 organization. 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.

The assessment of this component will likely form the largest element of the evaluation of the entity's internal control. But, it remains only one component of internal control. In Step 3, an assessment is made of the management control activities as to their appropriateness, consistency according to plan throughout the period, cost effectiveness, comprehensiveness, reasonableness and relationship to the control objectives.

In evaluating whether control activities are effective, the assessor will need to answer the following questions:

- (1) Are control activities appropriate (that is, is the right control in the right place and commensurate to the risk involved)?

- (2) Do they function consistently according to plan throughout the period (that is, are they complied with carefully by all employees involved and not bypassed when key personnel are away or the workload is heavy)?
- (3) Are they cost effective (that is, does the cost of implementing the control exceed the benefits derived)?
- (4) Are they comprehensive, reasonable and directly related to the control objectives (i.e., provision of reliable financial and management reporting, effective and efficient operations, safeguard of resources and compliance with applicable laws and regulations)?

While not exhaustive, the evaluator should consider the following lines of inquiry in concluding on the four questions above:

- (1) Are authorizing and executing transactions and events done only by persons acting within the scope of their authority?
- (2) Are duties and responsibilities assigned systematically to a number of individuals to ensure that effective checks and balances exist?
- (3) Is access to resources and records limited to authorized individuals who are accountable for the custody and/or use of the resources?
- (4) Are transactions and significant events verified before and after processing?
- (5) Are records reconciled with the appropriate documents on a regular basis?
- (6) Is operating performance reviewed against a set of standards on a regular basis, assessing effectiveness and efficiency?
- (7) Are operations, processes and activities periodically reviewed to ensure that they are in compliance with current regulations, policies, procedures, or other requirements?
- (8) Is supervision (assigning, reviewing and approving, guidance and training) provided to 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?

STEP 4: ASSESSMENT OF INFORMATION AND COMMUNICATION

Information must be reliable to be of use and it must be communicated to those who need it. For example, supervisors must communicate duties and responsibilities to the employees that report to them and employees must be able to alert management to potential problems.

- Information must be communicated both within the organization and externally to those outside, for example, vendors, recipients, and other.
- Communication must be ongoing both within and between various levels and activities of the agency.

Information and communication are essential to realizing all internal control 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.

In Step 4, the assessor must address the following questions:

- (1) Does the entity maintain pertinent, reliable and relevant information, identified, captured and communicated in a form and timeframe that enables people to carry out their internal control and other responsibilities?
- (2) Do information systems produce reports that contain operational, financial and non-financial, and compliance-related information, that make it possible to run and control the operation?
- (3) Is the quality of information 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)?
- (4) Is the internal control system as such and all transactions and significant events fully and clearly documented (e.g. flow charts and narratives)?
- (5) Does documentation of the internal control system include identification of the organization's structure and policies and its operating categories and related objectives and control procedures?
- (6) Does communication flow down, across, and up the organization, throughout all components and the entire structure?
- (7) Do all personnel receive a clear message from top management that control responsibilities should be taken seriously; do they understand their own role in the internal control system, as well as how their individual activities relate to the work of others?

Negative or partially positive responses to these questions show that internal control is weak and that the other elements of internal control may also be deficient.

STEP 5: EVALUATION OF MONITORING MECHANISMS

After internal controls are put in place, their effectiveness needs to be periodically monitored to ensure that controls continue to be adequate and continue to function properly. Management must also monitor previously identified problems to ensure that they are corrected.

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.

In assessing whether the entity maintains adequate monitoring mechanisms as part of internal control, the assessor should consider the following questions:

- (1) Does ongoing monitoring of internal control occur in the course of normal, recurring operations of the organization? Ongoing monitoring activities cover each of the internal control components and involve action against irregular, unethical, uneconomical, inefficient and ineffective internal control systems.
- (2) Are specific separate evaluations carried out to cover the effectiveness of the internal control system and ensure that internal control achieves the desired results based on predefined methods and procedures?
- (3) Are internal control deficiencies reported to the appropriate level of management and adequately and promptly resolved?

CONCLUSIONS ON INTERNAL CONTROL ASSESSMENT

Internal control consists of all five components, not just the two components of risk analysis and management control activities design and functioning which usually are the major focus of an internal control review. If the control environment is not conducive and if information, communication and monitoring are inadequate, internal control is inadequate and the likelihood of not being able to achieve the entity's mission and objectives increases.

A determination of the soundness of each of the five components of internal control will provide the basis for strengthening areas that are weak or lacking and for a plan to address the findings.

PLAN TO ADDRESS INTERNAL CONTROL DEFICIENCIES

Having carried out an assessment (evaluation) of internal control in the entity, a final step is to address any deficiencies. Following, are a number of steps that can be considered:

1. Group deficiencies in terms of their significance. Identify those that will likely have the greatest impact on the achievement of the entity's objectives.
2. Confirm the risk appetite of the entity (i.e., what types of risks are accepted and/or what size of risks are accepted?).
3. Determine how best to address the internal control deficiencies (e.g., transferred, tolerated, terminated or treated).
4. For each option chosen, identify actions, timeframe, and responsibility for action. For a "tolerated" control deficiency, the implication of not addressing the deficiency should be clearly spelled out as well as the name of the responsible manager/s for making the decision. Actions will include developing appropriate policies and procedures, improving communication channels, issuing codes of

conduct, and so on, depending on the nature and significance of the deficiency. Where treatment is the preferred option, the mechanism used will need to be identified, the timeframe for implementation set forth and the responsible manager assigned.

5. For each activity plan, approval at the appropriate level is required and communication of the decisions made.
6. The plan needs to include a section on how actions will be monitored as well as when the next evaluation or series of evaluations or types of evaluation (e.g., on-going or periodic) will take place and who will be responsible.

In a small entity, the plan could include all the policies and procedures of the entity. In a big entity, the plan may include documents of policies and various procedures as referenced. As a component of the entity's plan, however, these policies and procedures will need review and renewal at least once a year.

ANNEX 2: VULNERABILITY ASSESSMENT

CHARACTERISTIC:

CONSIDERATIONS:

1. Operational Stability:

If the function or entity has existed for some time with the same fundamental mission, without major new responsibilities, legislative mandates or personnel changes, the risk is *Low*.
(Frequency of change increases the risk)

Does this function involve a long-term stable program, or a brand-new mandate/activity? Are staff well-seasoned in this operation, or has there been considerable turnover of veteran staff or acquisition of new personnel?

2. Organizational Structure:

If the organizational structure is well-documented & periodically reviewed, with clearly defined areas of authority, and direct and indirect lines of supervision are established understood, the risk is *Low*
(As the structure becomes more decentralized, the risk increases).

Are organization charts up-to-date? Are individual unit functions well-documented? Are staff clear as to lines of authority and in-house clearance mechanisms? Does the organization include field staff operating with limited supervision? Is individual employee productivity and attendance reviewed adequately?

3. Policies & Procedures:

If policies & procedures for the entity or function are documented, updated, and clearly define employee responsibility & limits of authority, the risk is *Low*.
(The better the documentation, the lower the risk)

Are policies & procedures clear and current? Is there potential for conflict or confusion with other policies or higher level authorities? Do employees have authority commensurate with responsibility, to ensure they can do their job in a timely, accountable manner? Are procedures keeping pace with organizational change or new mandates?

4. Sensitivity/Complexity of Operations:

If the function is important to the entity's primary responsibilities; and involves sensitive program, fiscal, or political considerations; or is highly technical or administratively complex, the risk is *High*.
(Greater complexity implies greater risk)

Is the function routine/repetitive, involving large numbers of small-value transactions, or does it involve a complex set of tasks, requiring individual initiative and/or involvement of other bureaus or other agencies? Is this function highly visible/vital to local political jurisdictions or the public?

5. Personnel:

If properly trained & technically proficient personnel are assigned to this function, assignments are clearly defined, employee performance is periodically reviewed, and additional staff development is provided as

Are staff adequately trained to conduct the variety, and complexity of functions? Are special credentials /training a prerequisite for employment? Is there a viable, ongoing staff development program to keep employee skills current with

CHARACTERISTIC:

CONSIDERATIONS:

necessary, the risk is *Low*.
(The more qualified & trained the staff, the lower the risk).

administrative systems, computer support or emerging new mandates?

6. Financial Resources:
If the function requires accurate & comprehensive financial records to handle significant cash receipts, disbursements, and negotiable instruments, or it has a large operating budget, the risk is *High*.
(More handling of funds means greater risk)

Does this function involve handling of cash or negotiable instruments? Is there adequate separation of duties to ensure accuracy/accountability? Is supervision/oversight commensurate with the value of assets received/dispensed (e.g. youth allowances, petty cash payments)?

7. Physical Resources:
If the function maintains an inventory of or utilizes expensive or transportable physical assets which could be lost, stolen, or damaged, the risk is *High*.
(Risk is also increased if comprehensive inventories are not maintained.)

What is the dollar value of assets used/accessed by this function? What potential is there for individuals to misuse such assets for personal gain (e.g., long distance phone calls, pilfering of office supplies/foodstuffs or theft of computers / electronics/ vehicles)?

8. Authorizations:
If the function involves approving applications, certifications or contracts; or requires on-site inspection of facilities, the risk is *High*.
(The greater the involvement, the higher the risk.)

Does this function involve approving service contracts, certification of building/construction safety, or vendor contracts? Does agency staff directly inspect facility or service provider sites? Would the consequences of staff action be significant enough to tempt desperate or unscrupulous parties to offer inducements for overlooking shortcomings?

9. Frequency of Reviews:
If the function is subject to frequent outside reviews of operations by agency internal auditors, outside auditors, accreditation groups or other oversight bodies, the risk is *Low*.
(Fewer reviews & less follow-up means greater the risk)

Is this function scrutinized on an annual basis, or could many years elapse before a potential problem is detected? Where errors are detected, is corrective action pursued in a timely manner? Are findings of auditors or oversight bodies made public (or disseminated beyond the individual unit affected)?

10. Reliance on Information Systems:
If the function relies on (or is responsible for) computer-generated information or

Could improper access to information damage individuals or the entity's reputation? If information systems were compromised, is there potential for

CHARACTERISTIC:

statistical data - either electronic or hard copy - which must be accurate, complete & protected from unauthorized use, the risk is *High*.

(More reliance on, & complexity of, statistical information means greater risk.)

11. Influence:

If the function is subject to external influence by interest groups and/or private interests with the potential for conflicts of interest by administrators/employees, or pressure for untimely action, the risk is *High*.

(More interest group contact means greater risk).

12. Impact of Failure:

If the function should fail to operate properly, with serious fiscal or human consequences, or if the internal controls should fail to detect the misuse or misappropriation of assets by employees or agency-funded programs, the risk is *High*.

(Greater significance means greater risk.)

CONSIDERATIONS:

personal financial gain, or sabotage of a vital agency function? Are there manual backup systems & procedures available to reconstruct files (disaster recovery)?

Is this function of interest to legislators, local elected officials, community organizations or special interest groups? Are steps taken to minimize potential for conflict of interest by the agency's own staff? Does the administrative organization screen line staff from undue pressure/influence?

If something goes wrong in this function or entity, is there serious risk of personal harm to staff or clients (e.g., client abuse, disease contagion, accident or fire), or significant misuse of agency assets by staff or agency-funded programs? What dollar value could be placed on such system failure? Is there potential for a lawsuit (involving a significant monetary award or damage to agency's reputation)?

VULNERABILITY ASSESSMENT WORKSHEET

Program/Function: _____

Bureau/Unit: _____

Instructions: For each characteristic below, rate vulnerability from 1 to 5 - with 1 being the lowest risk, and 5 being the highest degree of risk.

	Characteristic	1 -Low Risk	2 – Low to Moderate	3 - Moderate Risk	4 – Moderate to High	5 -High Risk
1.	Operational Stability	<input type="checkbox"/> 1	<input type="checkbox"/> 2	<input type="checkbox"/> 3	<input type="checkbox"/> 4	<input type="checkbox"/> 5
2.	Organizational Structure	<input type="checkbox"/> 1	<input type="checkbox"/> 2	<input type="checkbox"/> 3	<input type="checkbox"/> 4	<input type="checkbox"/> 5
3.	Policies & Procedures	<input type="checkbox"/> 1	<input type="checkbox"/> 2	<input type="checkbox"/> 3	<input type="checkbox"/> 4	<input type="checkbox"/> 5
4.	Sensitive/Complex Operations	<input type="checkbox"/> 1	<input type="checkbox"/> 2	<input type="checkbox"/> 3	<input type="checkbox"/> 4	<input type="checkbox"/> 5
5.	Personnel	<input type="checkbox"/> 1	<input type="checkbox"/> 2	<input type="checkbox"/> 3	<input type="checkbox"/> 4	<input type="checkbox"/> 5
6.	Financial Resources	<input type="checkbox"/> 1	<input type="checkbox"/> 2	<input type="checkbox"/> 3	<input type="checkbox"/> 4	<input type="checkbox"/> 5
7.	Physical Resources	<input type="checkbox"/> 1	<input type="checkbox"/> 2	<input type="checkbox"/> 3	<input type="checkbox"/> 4	<input type="checkbox"/> 5
8.	Authorizations	<input type="checkbox"/> 1	<input type="checkbox"/> 2	<input type="checkbox"/> 3	<input type="checkbox"/> 4	<input type="checkbox"/> 5
9.	Frequency of Reviews	<input type="checkbox"/> 1	<input type="checkbox"/> 2	<input type="checkbox"/> 3	<input type="checkbox"/> 4	<input type="checkbox"/> 5
10.	Reliance on Information Systems	<input type="checkbox"/> 1	<input type="checkbox"/> 2	<input type="checkbox"/> 3	<input type="checkbox"/> 4	<input type="checkbox"/> 5
11.	Influence	<input type="checkbox"/> 1	<input type="checkbox"/> 2	<input type="checkbox"/> 3	<input type="checkbox"/> 4	<input type="checkbox"/> 5
12.	Impact of Failure	<input type="checkbox"/> 1	<input type="checkbox"/> 2	<input type="checkbox"/> 3	<input type="checkbox"/> 4	<input type="checkbox"/> 5

TOTAL (Add ratings 1 thru 12) Score: _____

Total Score of 48+ indicates

HIGH Vulnerability

Total Score of 25-47 indicates

MODERATE Vulnerability

Total Score under 25 indicates

LOW Vulnerability

Completed By: _____ **Date:** _____

Reviewed By: _____ **Date:** _____

ANNEX 3: INTERNAL CONTROL IN ALBANIA

MAIN ACTORS IN THE INTERNAL CONTROL ENVIRONMENT

1. The Parliament of Albania approves the primary legislation in the Republic of Albania. Parliament structures include the Parliamentary Commission of Economy and Finance which has a particular role in the establishment and consolidation of the Public Internal Financial Control (PIFC) system, not only by passing laws, but also by providing recommendations to central government on the improvement of financial management.
2. The Council of Ministers (CoM) functions in accordance with a specific law and is chiefly responsible to the Parliament for drafting and enforcing financial and economic policies, managing public funds, and implementing state budgets. However, the law and the basic regulations for CoM functioning do not stipulate how it should operate within the framework of PIFC. The administrative control department, part of the CoM, inspects procedures, decision making, and their enforcement at the central and local level. It also monitors and coordinates the government's matrices for implementing policies and relevant decisions.
3. External audit in the public sector is carried out by the Supreme Audit Institution (SAI), whose activity is regulated by a specific law. Its mission is to "audit the administration of state assets and the application of the state budget in entities anticipated in the organic law on SAI by achieving the highest possible transparency in the use of public funds to the benefit of taxpayers." To accomplish its mission, the SAI has unlimited access to all public entities to assess the accuracy of transactions, but it does not have predefined obligations to conduct timely audits and to cover certain areas. The Supreme Audit Institution also assesses the activity of the internal audit units in terms of its entire system, taking heed of compliance with standards.

In concluding its audits, the Supreme Audit Institution recommends disciplinary measures and changes to the organization, including modifications to laws and legal provisions. Its recommendations are not mandatory for public entities, but they are generally esteemed and taken into consideration.

4. The Ministry of Finance is the main actor in the PIFC system in Albania. The Law on State Budget and the Law on Internal Audit in the Public Sector stipulate the specific role of the Ministry of Finance in financial management and the internal control system, in general. These laws do not set forth mechanisms, obligations, and responsibilities outside the MoF for the implementation of PIFC.
5. The General Department of Budget and the General Department of Treasury in the Ministry of Finance have the main role in preparing and applying annual and midterm budgets which are approved by the Parliament through specific laws. A Central Harmonization Unit is to be established in the General Department of Treasury. This department will also house the accounting directorate whose mission is to enforce application of a unique methodology in the accounting system and to provide financial reports in the public sector.

Application of the budget is organized and realized through the treasury system and its regional branches via a central service at the Ministry of Finance (Treasury Department). The Department identifies and provides final authorization on payments from the budget, but does not establish complete ex-ante control over budgetary spending entities.

6. Pursuant to the law “On Internal Audit in the Public Sector”, the General Internal Audit Department and its subordinate audit units were reorganized in 2000 to establish internal audit structures in all ministries, central institutions, and public entities. Internal audit units report to the General Department in the Ministry of Finance. The General Internal Audit Department monitors the operation of the internal audit units throughout the public sector and receives periodic reports from them.

The main function of internal audit is to assess the effectiveness and efficiency of the internal control system and to provide recommendations for its improvement.

7. All ministries have their own financial and budgetary services that are charged with the preparation of the ministry budget and its use. Line ministries, in collaboration with the Ministry of Finance, draft joint guidelines for the application of the state budget. The new law on the budget stipulates clear reporting channels among line ministries and the Budget and Treasury departments in the Ministry of Finance.
8. The Organic Budget Law provides that the top executive is responsible for establishing the organization’s system of internal control, and is also responsible for:
 - (1) establishing a system of internal control review,
 - (2) making management policies and guidelines available to all employees, and
 - (3) implementing education and training about internal control and internal control evaluations.

To the extent that the top executive authorizes other managers to perform certain activities, those managers become responsible for those portions of the organization’s system of internal control.

The law further requires the head of the organization to designate an internal control officer who reports to the head. Drawing on the knowledge and experience with internal control matters, the internal control officer is a critical member of the management team who assists the agency head and other management officials by evaluating and improving the effectiveness of internal controls. While the internal control officer has responsibility for both implementing and reviewing the organization’s internal control efforts, the organization’s managers are still responsible for the appropriateness of the internal control system in their areas of operation.

The internal control officer helps establish specific procedures and requirements and the effectiveness of these procedures and requirements must be audited by someone who was not involved in the process of putting them into place. Generally, this means that the organization’s internal auditor is responsible for evaluating the

effectiveness of the system of internal control. And, since the internal auditor must be independent of the activities that are audited, the internal auditor cannot properly perform the role of internal control officer.

9. The foundations for internal control in local government units have been laid out in the organic budget law, but the specificities of local governments will still need to be addressed and other laws will need to be amended to comply with the organic budget law.
10. A considerable number of public enterprises have been privatized, and other public institutions run business activities in compliance with their statutes. The legal basis for their activity is the law “On Commercial Companies” and other legal provisions which, however, do not provide specific regulations for their financial management. These enterprises are either completely owned by the state or the government owns the majority of shares; therefore, it is necessary to enact basic regulations regarding the financial management of these enterprises. Audit experience has shown that serious infractions, violations, and abuses have occurred in these enterprises to the detriment of public interests, as internal audit units have been either inexistent or established in contradiction of the standards. In general, these entities have internal audit structures established inside the organization, but their functional and organizational independence is weak. These structures have a direct relationship with the executive branch but not with their board, as efforts are being made to position the internal audit structures in reporting relationship with their boards.
11. The situation described above applies also to independent public institutions, but with the difference that the problems of infractions and the detriment to the public interests are greater. Because the government does not have the authority to audit these institutions, owing to the independence of their internal audit units and, in some cases, their lack of an audit function, the Supreme State Audit has proved a series of infractions and irregularities to the detriment of the state interests. These institutions’ internal audit regulations are very limited and evasive, providing vulnerabilities and enabling abuse and misuse. In these conditions, focused internal control regulations at the functional level are necessary to provide opportunities to independent institutions to make their own regulations at the operational level.

ROLE OF THE GENERAL SECRETARY IN INTERNAL CONTROL

In compliance with the law “On the Status of the Civil Servant” and the manuals prepared for its enforcement, each ministry and central institution has a function of General Secretary. According to the Act, the General Secretary is responsible for formulating policies and presenting them for approval of the Minister. The General Secretary is also responsible for implementing policy as well as managing the financial and human resources of his or her ministry. The Organic Budget Law clearly sets out the responsibilities of the General Secretary of line ministries as the “first authorizing officer” of the budget of the central government units, of special funds and of transfers of the central government units.

The first authorizing officer reports to the Minister of Finance for the management of the budgetary system and for PIFC of the annual budget law and its sub-regulatory acts. The first authorizing officer submits to the respective parliamentary commission periodic reports and financial information and the annual report on the implementation of the budget. Upon request of the responsible commission, this officer reports during the year on other issues that relate to the implementation of the budget and public internal financial control.

The Organic Budget law defines the First Authorizing Officer in central government units as an employee of the public administration of a senior level in the civil service equivalent to a General Secretary of a ministry or central institution.

According to this law, this function is responsible for the establishment, operation, and maintenance of the internal control system in the public sector in compliance with the standards and best practices of internal control with the aim of ensuring efficiency, effectiveness, and the rational use of public resources.

ROLE OF THE INSPECTOR GENERAL OF THE HIGH INSPECTORATE OF DECLARATION AND AUDIT OF ASSETS IN INTERNAL CONTROL

The High Inspectorate of Declaration and Audit of Assets (HIDAA) is an independent agency responsible for the administration of the Law on the Declaration and Audit of Assets established in 2003 and the Law on the Prevention of Conflicts of Interest in the Exercise of Public Functions, established in 2005. The High Inspectorate plays a key role in overall governance and internal control for the government as a whole by both providing audit and investigation of instances of inadequate or missing declarations of assets by senior public servants (including politicians) and instances of conflict of interest as well as guidance and direction for public servants on proper disclosure of assets and on how to refrain from carrying out activities where there may be conflicts of interest. The organization sets a moral tone as well as provides detective and preventive controls in government.

ROLE OF CENTRAL HARMONIZATION UNITS

The Central Harmonization Unit (CHU) is a key component of internal control in the Albanian public service. CHU is the responsible structure for the establishment of complete financial management control and an internal audit framework. Referring to the best practices recommended by the European Commission, CHU is made up of two functionally separate structures: one for financial management control and the other for the internal audit. Both structures are located in the Ministry of Finance and report to higher management.

The practices to date have formed two versions for the construction of CHU, which are presented in Annex 4. The first version includes the construction of a unique structure that reports to the highest management with two separate subdivisions: internal audit and financial management control. This unit establishes relations with its respective internal audit and financial services in the line ministries. These units report to their respective director and the director reports to the highest management level.

The second version creates two independent units: one for the internal audit, reporting to the highest management level, and a second for the financial management control established at the General Department of Budget or Treasury and reporting to its respective director. The director then reports to the highest management level. The relationship of these two units is similar to the first version: direct relationship with internal audit units and with offices of the financial services in the line ministries. The main responsibilities of CHU are as follows and apply to both versions of the organizational construction:

CHU's responsibilities for financial management:

- Assist the Ministry of Finance (MoF) in its proposals to the Government on the development of financial management control
- Implement a formal Policy Paper and Action Plan on the PIFC system
- Draft financial management and budget policies
- Draft strategy on PIFC
- Organize work on drafting primary and secondary legislation on internal audit
- Develop manuals on public internal control
- Draft and develop methodologies for evaluation and management of risk
- Draft and implement programs on training of officials for financial management control
- Coordinate work with financial service units on development of methodologies and procedures at functional and operational level
- Monitor PIFC systems and their corrective actions
- Assess reports of internal audit from the viewpoint of operation of internal control system
- Prepare reports on the status of PIFC

CHU's responsibilities for internal audit:

- Assist the Ministry of Finance to evaluate the economy and efficiency of public resources by making relevant recommendations
- Draft and develop primary and secondary legislation and methodology on internal audit in public sector
- Evaluate and develop capacities of internal audit in public sector and give relevant recommendations to the respective ministry
- Draft and develop audit procedures based on best international practices
- Prepare and develop programs for qualification and certification of internal auditors

PRESENT FLAWS IN INTERNAL CONTROL

Presently, public internal financial control (PIFC) in Albania can be considered as being deficient, flawed, or unable to ensure the effective use of public resources or accomplishment of objectives of public entities. Deficiencies and/or flaws of control allow for corruption, abuse of public funds, inefficient use of resources, and other activities that could harm public interests.

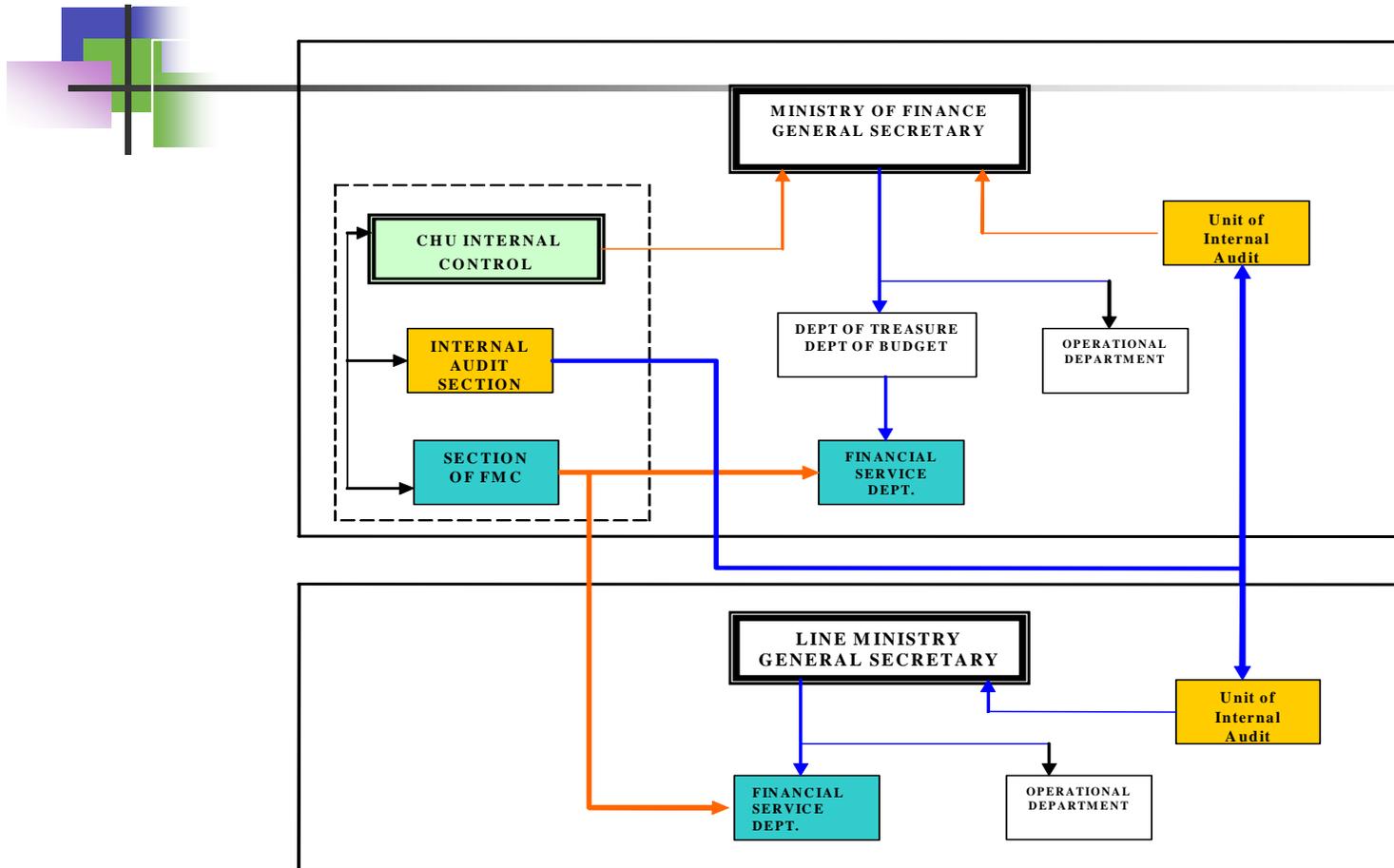
A detailed analysis of the internal control framework identifies several shortcomings the elimination of which could considerably improve the internal control system. Some of these are listed below:

1. There is no comprehensive legal framework with regard to internal control. Some laws such as that on budget and another on internal audit in the public sector, address responsibilities for internal control, but developments are in their early steps.
2. A lack of national professional standards on internal control is another obstacle for the harmonization and unification of practices and procedures on internal control.
3. Organization of specialized structures for methodological guidance for internal control is not complete. For example, the Central Harmonization Unit for internal auditing has been established, but there is no similar unit for financial management control.
4. Regulation of financial administration, in general, is deficient particularly in the areas dealing with cash flows, material and monetary values, documentation of work and salaries, inventories, and so forth.
5. There are inadequate rules and procedures for internal control in state-owned commercial companies and in those state-owned enterprises under privatization process.
6. Current internal control provisions do not ensure complete material and financial responsibility for officials in public entities and the recovery of improper or extra payments. Some regulations are provided under the Civil Code but they are incomplete and do not specify rules on assessment or other additional interests. In addition, procedures similar to those in the private sector are needed regarding the responsibilities of managers of state-owned entities.
7. Administrative procedures are needed for cases of fraud, abuse, and other offenses that endanger public funds. Several efforts have been made to include in the auditing procedures manual the administrative procedures for investigating criminal acts detected during audits, but the manual does not stipulate these procedures. The Criminal Procedures Code foresees the obligation of public officials to report to the prosecutor's office any criminal offenses they have detected during their work but there are no means for doing this. PIFC will need to define the administrative procedures and management responsibilities for cases in which internal audit or other inspection structures identify fraud or other misconduct within the organization that harms public funds. These cases must be reported in a timely manner to the prosecutor.

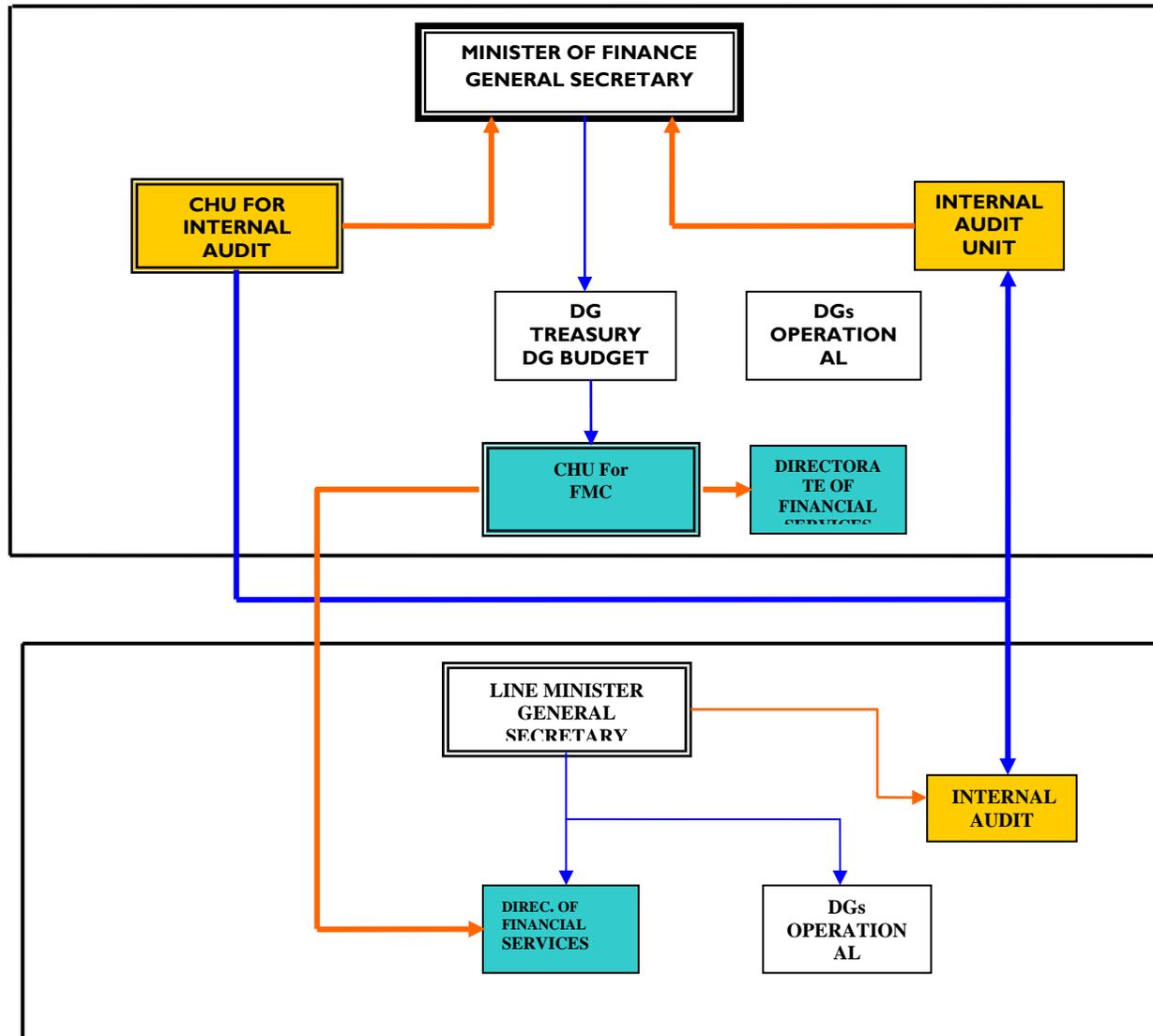
8. Certification of the public accounts is problematic and affects transparency and public trust. Accounting in the current PIFC system is weak because oversight and monitoring do not receive the full attention of management and other professional structures. In addition, financial declarations and balance sheets of public entities are not subject to certification by qualified professionals. Steps will need to be taken to establish a certification system for public accounts; and not only for budgetary spending entities. In addition, internal audits do not regularly examine complete financial statements but only certain parts. Finally, these statements are often not prepared in a timely basis.
9. An organic law to authorize the development of standards on internal control and the obligation of public agencies to enforce and develop them is required.

ANNEX 4: CHU STRUCTURES

CHU-VERSION I



CHU-VERSION 2



GLOSSARY OF CONTROL TERMS

Accountability	The recognition and acceptance that one is answerable for whatever happens within a particular area of activity of assigned responsibility regardless of the cause.
Components of internal control	The five internal control components are the control environment, risk assessment, control activities, communication and information, and monitoring.
Control activities	The third component of internal control: the structure, policies, and procedures that an organization establishes so that identified risks do not prevent the organization from reaching its objectives.
Control environment	The first component of internal control. It sets the tone of the organization, influencing the effectiveness of internal control. It is the foundation for all other components of internal control, providing discipline and structure and encompassing both technical competence and ethical commitment.
Control objectives	The objectives of an internal control system are reliable financial and management reporting, effective and efficient operations, safeguard of resources and compliance with applicable laws and regulations.
COSO	The Committee of Sponsoring Organizations of the Treadway Commission. It consists of the following organizations: the American Institute of Certified Public Accountants, the American Accounting Association, the Institute of Internal Auditors, the Institute of Management Accountants, and the Financial Executives Institute.
Effectiveness	The degree to which an organization or program succeeds in meeting goals, objectives, and statutory mandates.
Efficiency	The degree to which an organization or program succeeds in meeting goals and objectives with the least use of resources.
Goal	An elaboration of the mission statement, developed with greater specificity about the way an organization will carry out its mission. The goal may be of a programmatic, policy, or fiscal nature and is expressed in a manner that allows a future assessment to be made of whether the goal was or is being achieved.
Information and communication	The fourth component of internal control. An organization must have relevant, reliable, and timely communication relating to internal and external events.
Internal control	A process, effected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding

the achievement of objectives in the following categories:

- Effectiveness and efficiency of operations
- Reliability of financial reporting
- Compliance with applicable laws and regulations

Internal control system	A synonym of internal control.
Management intervention	Management's actions to override prescribed policies or procedures for legitimate purposes. Management intervention is usually necessary to deal with nonrecurring and nonstandard transactions or events that otherwise might be handled inappropriately by the system.
Management override	Management's overruling of prescribed policies or procedures for a number of possible reasons, including, illegitimate purposes with the intent of personal gain or an enhanced presentation of an organization's financial condition or compliance status.
Mission	The fundamental purpose for which an organization exists. A mission statement establishes the basis for the goals of the organization by describing in broad terms what the organization intends to accomplish.
Monitoring	The fifth component of internal control. It ensures that controls are adequate and function properly.
Objective	A subgoal that is identified in specific, well-defined, and measurable terms and that contributes to the achievement of an organization's goal, mission or mandate.
Organization	An entity of any size, established for a particular purpose. An organization may be, for example, an agency, a department, an office, a commission, a board, etc.
Policy	Management's directive of what is required to effect control. A policy serves as the basis for the implementation of management directives.
Preventive control	A control designed to avoid an unintended event or result.
Procedure	An action that implements a policy.
Process	A series of activities that are linked to achieve a specific objective.
Reasonable assurance	The concept that internal control, no matter how well designed and operated, cannot guarantee that an entity's objectives will be met.
Reliable	A high degree of certainty and predictability for a desired outcome.
Risk	The possibility that an event will occur and adversely affect the achievement of objectives.

Risk appetite	The amount of risk exposure or potential impact from an event that an organization is willing to accept or retain.
Risk assessment	The second internal control component. The process used to identify, analyze, and manage the potential risks that could hinder or prevent an organization from achieving its objectives.
Separation of duties	An internal control activity to detect and prevent errors and/or wrongful acts. It requires, for example, that different personnel perform the separate functions of initiation, authorization, record keeping, and custody.
Valid	Produces or relates to the intended results or goal.

GLOSSARY OF CORRUPTION TERMS

Access to information	The right of interested parties (the public, NGOs, the media, etc.) to receive information held by government. Access to information increases government accountability to its citizens and reduces opportunities for corruption.
Accountability	<p>Accountability is a relationship between a person or agency entrusted with a particular task or certain powers or resources, on the one hand, and the principal on whose behalf the task is undertaken, on the other.</p> <p>Accountability mechanisms operate according to three principles: transparency, answerability and controllability and refers to the idea that people entrusted with political power have a duty of accountability to their electorate, both directly through elections and indirectly through institutional controls.</p>
Blackmail	Any payment obtained by intimidation, threats of injurious revelations or accusations. The extortion of this payment.
Bribery	Any valuable consideration given or promised in return for corrupt behavior in the performance of official or public duty. Anything given or serving to persuade or induce.
Bureaucratic corruption	Takes place at the implementation end of politics, where the public meets public officials. Bureaucratic, administrative, or petty corruption is usually distinguished from grand and political corruption (to the extent to which administration can be distinguished from politics).
Collusion	Secret agreement for a fraudulent purpose; conspiracy. An arrangement between persons to do some act in order to injure a third person (e.g., government organization).
Competitive bidding	A selection process of a good or service based on the principle of openness and transparency, which increases the likelihood that the best bidder wins according to qualifications, value, and other objective criteria.
Conflict of interest	Occurs when public interest is compromised by the private interests of public officials. Often, activity such as a private business venture, primarily serves personal interests and can influence the objective exercise of an individual's official public duties.
Corruption	Corruption involves behavior on the part of officials in the public sector, whether politicians or civil servants, in which they improperly and unlawfully enrich themselves, or those close to them, by the misuse of the public power entrusted to them.

Cronyism	The favorable treatment of friends and associates in the distribution of resources and positions, regardless of their objective qualifications.
Discrimination	To make a distinction, as in favor of or against a person or thing.
Extortion	The unlawful demand or receipt of property or money through the use of force or threat.
Favoritism	The normal human inclination to prefer acquaintances, friends, and family over strangers. It is not always, then, a form of corruption. However, when public (and private sector) officials demonstrate favoritism to unfairly distribute positions and resources, they are culpable of cronyism or nepotism.
Fiduciary risk	<p>This is the risk that funds:</p> <ul style="list-style-type: none">• are not used for the intended purposes;• do not achieve value for money; or• are not properly accounted for. <p>One type of fiduciary risk is corruption. Because partner governments' public financial management systems are often relatively weak, fiduciary risk is of particular concern when donors provide direct budget support.</p>
Fraud	Economic crime involving deceit, trickery, or false pretenses, by which someone gains unlawfully. An actual fraud is motivated by the desire to cause harm by deceiving someone else, while a constructive fraud is a profit made from a relation of trust. Synonyms: swindle, deceit, double-dealing, cheat, and bluff.
Gift giving	Gift giving is a cultural practice in many societies, by which people offer presents and favors in various circumstances according to local customs. Problems arise when gift giving to and by public officials contradicts the principles of impartiality, professionalism, and meritocracy. In exchange for a gift, the official is expected to show preferential treatment to the giver. In such cases, gift giving can be regarded as bribery.
Graft	To obtain money dishonestly by exploiting one's position of power, especially political power. Graft is understood as political corruption with an element of greediness. As a noun, graft refers to the rewards of corruption.
Grand corruption	High level or grand corruption takes place at the policy formulation end of politics. It refers not so much to the amount of money involved as to the level at which it occurs – where policies and rules may be unjustly influenced. Transactions that attract grand corruption are usually large in scale and therefore involve more money than bureaucratic or petty corruption. Grand corruption is sometimes used synonymously with political corruption.

Incentive	An inducement that encourages someone to do something. An incentive might be a bribe, persuading officials to return undue favors to the briber. But an incentive might also be a legitimate management practice such as increased pay to discourage corruption.
Influence trading	The exchange of undue advantages between a public official and a member of the public. For example, a public official may promise to use his or her real or supposed influence for the benefit of another person in exchange for money or other favors.
Integrity pact	An agreement intended to prevent corruption in public contracting. One of the parties represents a central, local, or municipal government, a government's subdivision, or even a state-owned enterprise (the Authority). The other party is usually a private company interested in obtaining the contract or in charge of implementing it. In the processes related to the public project, such as bidding, contracting, and implementing, both the administration and the company pledge not to bribe or take bribes, and both agree to punishment if they break the pledge.
Integrity system	Integrity is adherence to a set of moral or ethical principles. An integrity system, therefore, is a political and administrative arrangement that encourages integrity.
Interest peddling	Occurs when a professional solicits benefits in exchange for using his or her influence to unfairly advance the interests of a particular person or party. Interest peddling is addressed through transparency and disclosure laws, which aim to expose suspect agreements.
Kickbacks	A bribe, the return of an undue favor or service rendered, or an illegal secret payment made as a return for a favor.
Kleptocracy	A political system dominated by those who steal from the state coffers and practice extortion as their modus operandi.
Money laundering	The process whereby the origin of dishonest and/or illegally obtained money is concealed so that it appears to come from a legitimate source. Money laundering is often used to disguise the proceeds of corruption and is widely practiced by drug traffickers, human traffickers, kleptocrats, and white-collar criminals.
Nepotism	The favorable treatment of family and relations in the distribution of resources and positions, regardless of their objective qualifications.
Patronage	The support or sponsorship of a patron (a wealthy or influential guardian) motivated by the desire to gain power, wealth, and status through their behavior. Patronage transgresses the boundaries of legitimate political influence and violates the principles of merit and competition.

Petty corruption	The everyday (also called administrative or bureaucratic) corruption that takes place where bureaucrats meet the public directly. Petty corruption has been described as corruption of need. Although petty corruption usually involves much smaller sums than those that change hands in acts of grand or political corruption, petty corruption disproportionately hurts the poorest members of society, who may receive requests for bribes regularly in their encounters with public administration and services like hospitals, schools, local licensing authorities, police, and taxing authorities.
Political corruption	This term is sometimes used synonymously with grand or high-level corruption, referring to the misuse of entrusted power by political leaders. It can also refer specifically to corruption within the political and electoral processes. In either case, political corruption both leads to the misallocation of resources and perverts the manner in which decisions are made.
Sporadic corruption	The opposite of systemic corruption. Sporadic corruption occurs irregularly and therefore does not threaten the mechanisms of control nor the economy. It is not crippling, but it can seriously undermine morale and sap the economy of resources.
State capture	Outside interests (often the private sector or mafia networks) bending state laws, policies, and regulations to their (mainly financial) benefit through corrupt transactions with public officers and politicians. The notion of state capture deviates from traditional concepts of corruption, in which a bureaucrat might extort bribes from powerless individuals or companies or politicians themselves might steal state assets (see kleptocracy). State capture is recognized as a most destructive and intractable corruption problem, especially in transition economies with incomplete or distorted processes of democratic consolidation and insecure property rights.
Systemic corruption	As opposed to exploiting occasional opportunities, systemic (or endemic) corruption occurs when corruption is an integrated and essential aspect of the economic, social, and political system. Systemic corruption is not a special category of corrupt practice, but rather a situation in which the major institutions and processes of the state are routinely dominated and used by corrupt individuals and groups, and in which most people have no alternatives to dealing with corrupt officials.
Transparency	The quality of being clear, honest, and open. As a principle, transparency implies that civil servants, managers, and trustees have a duty to act visibly, predictably, and understandably. Transparency is therefore an essential element of accountable governance, leading to improved resource allocation, enhanced efficiency, and better prospects for economic growth in general.

REFERENCES

1. Standards for Internal Control in the Federal Government. GAO. Washington 1999.
2. Internal control. Integrated framework (by COSO).
3. INTOSAI. Guidelines for Internal Control Standards for the Public Sector.
4. Internal Control. Guide for managers. Vermont, Department Finance Management.
5. A Guide to Internal Controls. Dianne Parkerson, Florida Atlantic University.
6. Jean-Pierre Garitte. What are the roles and responsibilities of management for establishing and maintaining internal controls and internal auditing systems?
7. Wikipedia: Internal Control Framework.
8. COSO-The Framework for Internal Control: Compiled by Mark Simmons.
9. Policy Paper, “On Internal Control,” Ministry of Finance, Tirana, June 2005.
10. European Guideline on Enforcement of INTOSAI Standards. A publication of Supreme State Audit.
11. Public Internal Audit: A Manual. Tirana, 2005.
12. Robert de Koning: PIFC Public Financial Control. (A European Commission initiative to build new structures of PIFC in applicant and third-party countries), 2007.