MINISTRY OF FINANCE OF MONTENEGRO

Financial Management and Control Manual

Podgorica, July 2011

The document has been produced with the assistance of EU

This document – Financial Management and Control Manual – was produced by the Ministry of Finance – Central Harmonisation Unit, with the assistance of the EU. The document does not constitute a formal comunication and does not necessarily represent the official position of the European Union.

With the aim of improvement of the financial management and control system, this Manual will be the subject of continuous review and will be updated by the CHU of the Ministry of Finance.

IPA 2009 project „Strengthening the management and control systems for EU financial assitance in Montenegro“, EUROPEAID 129081/C/SER/ME, 09ME01.9.1 implemented by consortium of East West Consulting, Eurecna and Sofreco.

Table of Contents

Purpose of the FMC Manual

The purpose of the *Financial Management and Control Manual* is to assist all Managers and their staff in their role in establishing a framework for financial management and internal control in the public entities.

Additionally, it aims at providing guidance for the existence of basic and consistent internal controls throughout the public sector and to define the roles and responsibilities for the sound management of national and foreign funds.

In this way, the Financial Management and Control Manual address five interrelated components of the control system, notably:

- The control and operating environment.
- Organisational goals and objectives and related risk assessment and management.
- The controls and related policies and procedures that will contribute for managing and minimising risks and achieving goals and objectives.
- The information systems and communication.
- The activities to monitor the performance of the public entity.

It focuses on the following:

- Emphasising that management is responsible for ensuring that internal controls are established, properly documented, maintained and adhered to in each unit, department, and division.
- Emphasising that all public sector employees are responsible for compliance with internal controls.
- Emphasising that the internal audit capabilities are responsible for giving reasonable assurance that the system of internal control is adequate and effective and is functioning as designed by management with a view to achieve the organisations objectives.

The FMC Manual defines the framework for internal control in the public entities. It further provides a basis against which internal control can be evaluated. The approach applies to all aspects of a public entities activity and operation, not just the financial aspects. However, the need for sound financial management is a key objective of the FMC Manual.

Finally, it should be clearly stated that the *FMC Manual* includes only guidelines for implementing internal control. These guidelines do not provide detailed policies, procedures and practices for implementing internal control, but rather provide a broad framework within which public entities can develop their own internal controls aligned to their financial management.

Milorad Katnic

Minister of Finance

1. Introduction to Public Internal Financial Control

Public Internal Financial Control (PIFC) is a term and concept developed by the European Commission to assist the understanding and implementation of a well developed and effective internal control system during the EU Accession process.

P - Public Sector;

I – Internal to the organisation;

F – Financial systems mainly but not exclusively;

C – Control based on internationally accepted and recognised standards

Its aim is to ensure that public funds (both national and EU) are well managed and cost effectively controlled and it should provide value for money to the taxpayer.
It covers all internal control systems and procedures in public institutions and helps provide reasonable assurance that public funds are spent properly and achieve value for money.

The EU requires that candidate countries demonstrate that their financial control systems comply with best international practice and standards. These financial control systems should be effective in achieving the objectives of the organisation, making best use of resources and provide value for money. This goes beyond compliance with the legal framework and fundamentally this is where the 'new' control arrangements differ from traditional public sector internal control systems. The status quo is not an option for potential member states.

PIFC is the overall financial control system performed internally by a Government or by its delegated organisations, aiming to ensure that the financial management and control of its national budget spending centres (including foreign funds) complies with the relevant legislation, budget descriptions, and the principles of sound financial management, transparency, efficiency, effectiveness and economy.

PIFC comprises all measures to control all government income, expenditure, assets and liabilities. It represents the wide sense of internal control. It includes but is not limited to financial control and internal audit.

The PIFC Model = FMC + IA +CHU

There are 3 pillars of the PIFC framework which work together to achieve reasonable assurance that internal controls are performing adequately and efficiently:

Financial Management and Control (FMC) - and the need for managerial responsibility of the internal control process;

Internal Audit (IA) - A functionally independent and decentralised Internal Audit that reviews the effectiveness of Internal controls;

Central Harmonisation Unit (CHU) - a separate section that develops and directs the process of PIFC.

The EU requires that candidate countries have financial control systems in line with best international practice and standards. These financial control systems should be effective to achieve the objectives of the organisation, to make best use of resources and to provide value for money.

It is not just about compliance with the law and legal framework but about organisations providing good public services and the best use of resources. So this is where the ‘new’ concept differs from what exists in the old style public sector control systems. It is about organisations (line ministries, agencies, municipalities) being responsible and accountable for budget execution and the use the public monies. There has to be a change from centralised control to decentralised control whereby line ministries approve and authorise all payments but are also held accountable for fiscal decision making. The Ministry of Finance has to allow line ministries to have greater control of their financial affairs. This means that the financial units in the line ministries are managed by suitably qualified financial experts to plan, budget, monitor and report on its financial affairs.

To achieve this will take time as the process must be properly controlled at a pace that is suitable for both line ministries and for the Ministry of Finance. Change needs to be managed and controls moved from the Ministry of Finance to the line ministries to ensure that there is no deterioration in FMC. This will require a transition period when ‘testing’ of new controls will take place.

Managers must be given delegated authority and allowed to manage using ‘on-going’ controls and this means that each line ministry must take full responsibility for spending and controlling its own budget and for ensuring that appropriate checks and safeguards are in place.

It should be emphasised that FMC relates to all operational systems, financial and non financial ones of the entity. FMC is carried out in all organisational units and at all levels of the entity, and covers all resources of the entity, including EU funds.

There are many financial controls already functioning adequately in the Public Sector of Montenegro and the introduction of a formalised FMC system is more about adopting a common approach based on managerial responsibility and accountability and the use of an Internal Audit Service to review and report on the effectiveness of internal controls.

The legal framework in Montenegro already covers many aspects of FMC in terms of the Budget Law, Accounting Rulebooks and Treasury Directions to name but three. It is in the concept of management, the need for change, the decentralisation of control and the use of Internal Audit which is new to the public sector in Montenegro.

To achieve this requires the development of good management practices and sound financial control. This along with a staff training programme for PIFC for both central and local government will provide better services and the best use of limited resources.

This in turn will result in continuous improvement as public bodies identify and introduce best practice that will ensure the sustainability of public services in Montenegro.

2. Legal Framework

Introduction

It is important that Montenegro continually develops a legal and policy framework for PIFC. These reforms affect the whole Public Sector which must be committed to implementing not only these rules but also the culture of change required to sustain the spirit of PIFC.

The PIFC Law (73/08) was adopted in November 2008 and a FMC Rulebook (37/10) adopted in July 2010.

The PIFC Law is like an umbrella and should be linked to all main laws related to finance and accounting controls such as the Organic Budget Law- latest version was published 53/09.

The current version of the Organic Budget Law (53/09)

Financial Management and Control (FMC) is described and defined in the Law on Public Internal Financial Control System (73/08) passed in November 2008.

FMC is described by the Law in Article 4 as "the comprehensive internal control system that is established by and is the responsibility of the head of the entity, and which, together with risk management provides reasonable assurance that the Budget and other public funds will be used properly, economically, efficiently and effectively in the accomplishment of the relevant objectives of the entity".

In other words, FMC is a part of PIFC and is the prime responsibility of the head of each public entity for the purpose of improving financial management and decision making in achieving objectives of the public entity and in particular as mentioned in Article 5 of the PIFC Law:

- Compliance of operations with legislation, regulations, internal policies, contracts and procedures,
- The provision of reliable, complete and timely financial reporting,
- Economic, efficient and effective use of funds,
- Safeguarding of assets against loss or waste caused by mismanagement, unjustified spending, theft and fraud.

There is also the Rulebook for Public Financial Management and Control (37/10) published in July 2010. This provides a brief guide for establishing and implementing financial management and control.

PIFC is about **Managerial Accountability** for the use of budget funds and the provision of best value services to meet the needs of the public.

Senior management in each Ministry are accountable for the way an organisation is run and perceived by its staff and other stakeholders.

Based on the model above all managers need to take responsibility for their staff and their span of control as well as support the overall organisation policies.

Managers should realise that a strong internal control structure is fundamental to control of an organisation and its purpose, operations, and resources.

Responsibility for providing an adequate and effective internal control structure rests with an organisation's management. The head of each governmental organisation must ensure that a proper internal control structure is instituted, reviewed, and updated to keep it effective.

A positive and supportive attitude on the part of all managers is critical. All managers must be individuals of personal and professional integrity. They are to maintain a level of competence that allows them to understand the importance of developing, implementing, and maintaining effective internal controls.

The change required is built on a system first adopted by the Public Sector in the 1990's namely, the COSO Model which is explained later. It is complemented by the INTOSAI 'Guidelines for Internal Control Standards for the Public Sector' which expands the theories from the COSO Model. These guidelines were first published in 1992 but were updated in 2004 based on the framework of the COSO Model. See the quote below

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

The EU recognised that these documents and their methodology would serve as a framework for the FMC pillar of PIFC and therefore the contents of this FMC Manual are based on these two documents:

INTOSAI Internal Control Standards

More detailed information and a full copy of the document can be found at the link below:

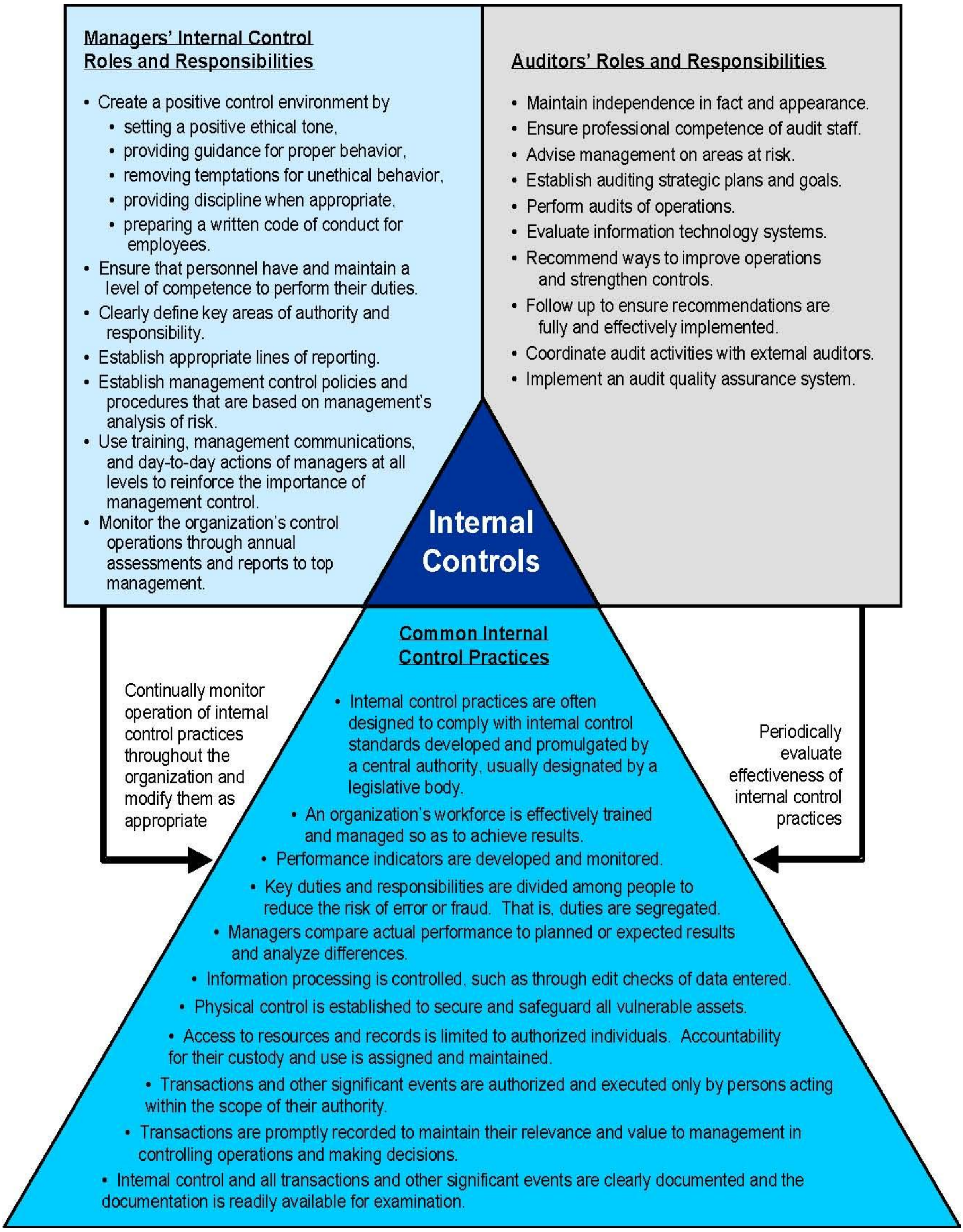
http://intosai.connexcc-hosting.net/blueline/upload/1guicspubsece.pdf

INTOSAI is the International Organisation of Supreme Audit Institutions.

INTOSAI have prepared a framework for establishing and maintaining effective internal control which highlights the roles of both managers and internal audit in the internal control process.

The following diagram lists the respective roles and responsibilities of managers and auditors as well as their focus of attention for ensuring effective internal control.

This provides guidance on the roles of Managers and Internal Auditors and what is expected of them in relation to the Internal Control System.



COSO Framework

Below is a brief explanation of the COSO Model which will be explained in more detail in Chapter Six

COSO Framework - Five Control Components

The fundamental principles of internal control are rooted in well established organisational techniques and practices. These are derived from the way management runs an activity, programme and project, and are integrated within the management process. The application of internal control is dynamic, and practices that fit past circumstances may need to be adjusted as those circumstances change. There are various methodologies and approaches to internal control but the most widely used is the COSO Framework.

In 1992, the **Committee of Sponsoring Organisations (COSO)**[1] of the National Commission on Fraudulent Financial Reporting (also known as the Treadway Commission) published a document called: *Internal Control – Integrated Framework,*[2] which defined internal control as "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 4 categories mentioned here above, notably:

- Compliance with applicable laws and regulations.
- Reliability of financial and managerial reporting.
- Effectiveness and efficiency of operations.
- Safeguarding of assets.

Internal control can be judged as effective in each of these categories if the Head of the Entity and management have reasonable assurance that:

- They understand the extent to which the entity's operations objectives are being achieved.
- Published financial statements are being prepared reliably.
- Applicable laws and regulations are being complied with.
- The entity is providing a service to the public that delivers value for money

The COSO Framework went on to say that internal control consists of five interrelated components.

The five basic components and their grouping provide a combination of "soft" controls such as establishing an environment in which control can survive and flourish alongside stricter more traditional types of "hard" controls over accounting and financial transactions.

---

[1] The Committee of Sponsoring Organisations consists of the American Institute of CPAs (AICPA), the Institute of Management Accountants (IMA), the Institute of Internal Auditors (IIA), Financial Executives International (FEI), and the American Accounting Association (AAA).
[2] The COSO publication *Internal Control—Integrated Framework* (Product Code Number 990012), may be purchased through the AICPA store at www.cpa2biz.com. The proceeds from the sale of the Framework are used to support the continuing work of COSO.

The five components for establishing internal control system based on the COSO Framework are:

1. Control environment – must be positive and senior management must set the tone and lead by example for staff to respect and perform their duties to the best of their ability;

2. Risk assessment - a strategy must be adopted that supports the mission and key objectives of the organisation by minimising the risk of things going wrong;

3. Control activities – suitable controls must be established and reviewed regularly to ensure that the system of internal control is functioning properly;

4. Information and Communication – relevant information must be issued to staff and the public and a good two communication system introduced; and

5. Monitoring of controls - the organisation must assess and monitor the risks and controls of the organisation regularly and improve when and where necessary.

These are the 5 key areas that should be reviewed and developed for all internal control systems to be in line with EU best practice.

These documents should be read in conjunction with the relevant national legislation covering elements on Financial Management and Control

- Law on Public Internal Financial Control System (OG No. 73/08) and
- Rulebook on the manner and procedure for the establishing and implementing Public Financial Management and Control (OG No. 37/10).

These are included for ease of reference as annexes to this document. Also included in the annexes is the Glossary of Definitions used by the European Commission in the Framework of PIFC.

3. Financial Management and Control - FMC

Introduction

Sound financial management is essential to improving the quality of public service outcomes. It affects how funding is used to address national and local priorities, the availability of resources for investment and the cost-effectiveness of public services.

Sound financial management depends upon the achievement of a number of objectives:

• Giving a reliable account of the money spent and the income received.

• Ensuring that there is probity and sound financial administration, including proper stewardship of public resources and compliance with regulatory standards.

• Ensuring the achievement of value for money, that is economy, efficiency, effectiveness in how funds are used.

• Identifying, evaluating and managing risk.

• Supporting good decision making and assisting managers to properly assess the financial consequences of policy and other choices.

• Enabling the organisation to plan for the future and to align its resource allocation with its policy objectives.

• Maximising income sources.

• Making it possible, from a financial management point of view for organisational change to occur, to meet new circumstances.

Also, it is more than likely that the general public will have greater trust in public sector organisations if there is strong financial stewardship, accountability and transparency in the use of public funds.

It is important for governments to get it right because it impacts on a broad range of areas including:

- financial management – fiscal sustainability, resource mobilisation and allocation
- operational management – performance, value-for- money and budget management
- governance – transparency and accountability
- risk management – controls and compliance

In addition, effective public financial management is important for decision making. Accurate financial information is often used as the mechanism to support decisions and ensure effective resource allocations.

There is a general expectation that those responsible for the conduct of public business and the handling of public money are held fully accountable for the conduct of that business in accordance with the law and proper standards, and that public money is safeguarded and properly accounted for, and used economically, efficiently and effectively.

Managerial responsibility and the accompanying accountability should help each organisation to achieve their specific and general objectives. Managers have to consider the following in the process of decision making

- to use time and resources sparingly and dedicate their precious time to most important things,
- to best allocate scarce resources and to act in the economic, efficient and effective way,
- to react to change in a positive manner and
- to be ready to avail themselves of the opportunities and comparative advantages.

Financial Management and Control (FMC) is one of the three pillars of Public Internal Financial Control and it is founded on the principles of modern public governance and managerial accountability

Managers must be given delegated authority and allowed to manage. In practice this means that each line ministry must take full responsibility and accountability for spending and controlling its own budget and ensuring that appropriate checks and safeguards are in place.

The traditional centralised control systems are based on physical control via checking and authorising every transaction. Typically, the Ministry of Finance controls the budget process, the allocation of funds to line ministries and controls all payments usually via a single treasury system.

Decentralised management is a new concept to many administrations. This change process needs time and support to develop. However, changes in culture; changes to management styles; changes to encourage continuous improvement; changes in public consultation arrangements and changes to transparency and public accountability are all required to provide better quality public service provision. Each entity should have a financial officer who is responsible for the budget preparation and execution and all financial matters.

The PIFC system has to empower public service managers to respond quickly to these new and changing demands. A good PIFC system has to be able to respond and react to these opportunities and risks.

In general financial control is the most important area of internal control as it covers almost every activity of the organisation. In the public sector emphasis is directed to the principles and activities supporting financial control. All managers have a duty and responsibility for financial control. They must ensure the best use of resources, minimise losses, waste, minimise the misuse of assets and prevent and detect fraud and corruption.

Public financial management is the effective management of the income and expenditure of government/public sector funds.

As financial demands will exceed available supply then it is important that public monies should be used as efficiently as possible.

Efficient public financial management is important in creating trust, transparency and a shared consensus between government and citizens.

To achieve effective financial management and control in the public sector it is essential that organisations concentrate on developing the following key areas of financial management:

1 Financial Regulations;

2 Financial Planning;

3 Financial Monitoring and Review;

4 Financial Control

5 Financial Information;

6 Financial Awareness

To achieve these, organisations must have good management information systems and in particular key financial systems that are:

- Modern
- Reliable
- Integrated (both with each other and with related management information systems operated by the Public Sector)
- Effectively support financial administration and management requirements.

It is necessary, therefore, to commit the financial and human resources to ensure that these systems:

- Are continuously developed to meet emerging needs;
- Make full use of new technology to improve their financial processes
- Are available to users and managers with the minimum downtime;
- Are decentralised to the budget users so that they are responsible and in control;
- Are integrated wherever possible to minimise data processing and maximise systems integrity.

1. Financial Regulations

To operate efficiently, a public sector organisation must ensure that the accepted principles of financial management are in place and, are adhered to.

Part of this process is the development and implementation of Financial Regulations or rulebooks which include the policies and procedures for all financial transactions involving payment of invoices and payment of staff; collection of revenues; budget preparation and execution; financial monitoring and reporting. These provide the framework and guiding principles for day-to-day routines for managing the organisation's financial affairs and for financial reporting and monitoring.

In Montenegro, apart from the Organic Budget Law (53/09), the Treasury Directions (latest version is 45/10) issued by the Ministry of Finance provides guidance and instructions on how line ministries should apply best practice financial management. This is a good starting point in that they provide all public sector organisations with the basic guidelines and instructions for the main financial processes.

The Treasury Directions provide guidance on the following financial matters:

1. Budget Execution;
2. Financial Control- Payments, Receipt of Goods and Commitments
3. Accounting and Expenditure Control;
4. Collection of Public Revenue;
5. Cash Security;
6. Irregularities;
7. Banking;
8. Salaries;
9. Borrowing- Debt and Loans
10. Financial Records;
11. Advances;
12. Donor Funded Programs.

The above list covers all the main financial processes that a line ministry must address for applying internal controls to minimise the risk of loss, waste and mismanagement. These systems/processes should be the basis for conducting the Internal Control Review in each organisation.

If the process is to be decentralised further an independent review should take place to record the process step by step from the beginning in the line ministry to the end in the Ministry of Finance. A report will follow which will provide recommendations and actions that can be presented to the Ministry of Finance for consideration.

It is expected that there will be internal procedures for each of these 12 areas so that line ministry staff are aware and understand how to administer each of these financial processes.

In reaction to changes, a modern public sector organisation should be committed to continuous review and changes to the regulatory framework.

Many organisations that have a quality control system will already have internal procedures and with their experience in this matter they can provide valuable support and guidance to others in the preparation of these procedures.

2. Financial Planning

The Ministry of Finance has overall responsibility for budget preparation and execution but it is important that all line ministries manage their financial affairs. The line ministries should prepare their draft financial budgets in conjunction with a plan of activities (service plan) that details the operational objectives for the forthcoming year. These objectives should support and be consistent with the Government objectives. Senior management should work together in the preparation of the budget and the service plan for their ministry.

Each year a Budget Circular is prepared for Budget Users that provides guidance and instructions for the preparation and submission of the annual budget. The budget users will then prepare their budget submissions to the Ministry of Finance in the required format and by the required deadline.

How does the Budget User prepare their budget? This will probably vary from ministry to ministry but it is important that all key staff that are responsible for programs are involved in the budget preparation and not just the financial staff. This process should be planned and not left to the last minute. Also, before submission of the budget each organisation should have considered their key objectives and priorities for the coming year. This may result in various budget proposals and scenarios being considered before a final decision is made.

It should be noted that the Government has adopted a Medium Term Expenditure Framework document that represents the basis for budgetary planning for the following three years.

Sound financial planning and budgetary control must be undertaken within an integrated Corporate and Business Planning framework and is fundamental to:

- Ensuring delivery of the Public Sector's objectives
- Effective resource utilisation and allocation
- Effective financial control throughout the organisations' activities

3. Financial Monitoring and Review

The key components of financial monitoring and review processes are:

- Regular financial reporting to management supplemented by effective budgetary control procedures; and
- Continuous, independent review of financial and internal controls and operational performance. Usually carried out by internal audit.
- Ad hoc investigations into costs, overspends or reduced revenue.

- Comparison of performance and costs by internal units; this can be to compare the cost for current year to the cost for previous year and/or comparison to budget and/or other organisations.

- Outsourcing of services to other organisations; is it cheaper to use an external agency?

4. Financial Control

In some countries the focus of financial control is on ex ante and ex post controls. Financial management and control is integral to all activities and functions of an organisation and should exist for all financial and non financial processes.

Decentralised control by the line ministries is the objective of PIFC. The internal audit section work with the managers of the main financial processes to ensure that there is reasonable assurance that the controls for the main financial processes are working adequately.

As financial control covers the whole organisation it requires that every head of department (manager) must ensure that controls exist and are working effectively within his/her area of control. Financial Managers in the line ministries are responsible for internal control not the Ministry of Finance.

Managers are therefore responsible and accountable for ensuring that they have performed adequate reviews as well as checked and monitored the internal control arrangements to provide evidence that these are effective or not. If there is a problem or a weakness in the internal control system then the manager of the process must address this and decide on how to fix the problem to improve the control and reduce the risk of this event occurring again.

The main financial systems such as Accounting, Budgeting, Treasury, Payroll, and Revenue Collection should be regularly reviewed, assessed and reported on by Internal Audit. These reviews should include checking the effectiveness of the IT system as a control tool.

5. Financial Information

Good quality financial information is essential to ensure that managers can be effective in:

- Policy formulation

- Decision making

- Service planning

- Financial planning

- Financial monitoring and control.

The quality standard will only be met where it can be clearly demonstrated that financial information is:

- Complete, accurate and timely

- Available to managers when they need it
- Accessible and understandable to all whom use it.

Core financial information is provided by systems such as:

- Income and Revenue Management - which records every income transaction.
- Commitment Accounting - which provides facilities to order goods and services and match these to available budgets.
- Financial Information System (FIS) – this provides general ledger, debtors and creditors accounting and budget execution information.
- Payroll - this provides data for salaries and wages for all employees.

Note the key systems terminology may differ from country to country and may exist in one Single Treasury System - what is important is that there must be a system(s) available capable of providing this core financial information.

6. Financial Awareness

Effective administration of an organisation's financial affairs can only be achieved if the systems and procedures referred to earlier are implemented operated and reviewed by employees who have the appropriate skills. Ideally professionally qualified accountants will be in charge of financial units but this may take many years to be implemented.

Employee training needs will be identified and continuously reviewed to identify new training needs. Once identified, training gaps should be addressed in a coordinated manner through a mix of in-house and external training courses.

For budgetary control, all budget holders will require mandatory training in:

- Using the organisations Financial Information System and, where appropriate, Commitment Accounting System; and
- Budgetary control techniques.

The Ministry of Finance should take the lead in the provision of training for example in regard to preparation of the Budget based on the Budget Circular so that all public sector organisations are proficient in the preparation of their Budget and in general financial management.

Management Framework

The concept of management may be new to Montenegro but it is essential that managers fully understand their responsibilities and those they are pro-actively involved in the decision making process.

It is only by being responsible and accountable that managers will take ownership to control their area of responsibility for inputs, processes and outputs.

Every manager has an on-going responsibility to ensure that staff makes every effort to achieve their specific outputs as their contribution to meeting the overall objectives of the organisation. For example: -

- Provide central direction for general, financial and administration policies in line with government requirements;

- Ensure essential processes are integrated components of management and financial administration systems;

- Define the framework of accountability, organisational principles and functional relationships for management and financial functions; and

- Ensure financial management processes and control systems are adequately documented, communicated and understood by all.

The following general public management principles apply to all administrations:

- Resource allocation decisions made during the budget process must clearly communicate the government's service delivery and political priorities;

- Government and ministry goals and objectives must be communicated clearly to the public and staff ensure that all partners are working to achieve the same goal;

- A clear assignment of responsibilities to minimise duplication of tasks and to ensure that someone is responsible for completing each function;

- All managers' who have been assigned responsibilities are delegated the authority to carry them out. Statutes grant authority to ministers and deputy ministers, and the authority is delegated throughout the organisation; and

- All mangers' are accountable for their actions and decisions both financial and non-financial.

All administrations must have the following components for a cohesive financial management framework:

- Legislation, regulations, policies and procedures;

- Financial planning and budgetary control procedures;

- Processes, systems and internal controls;

- Schemes of delegation of authority and responsibility;

- Processes and procedures to monitor and report on adherence to control standards; and

- A transparent and fair process for holding individuals and organisations accountable for non-performance.

Public sector approaches to control have evolved as new demands for governance have emerged. This has involved moving beyond traditional financial and general management control expectations. In all organisations, the components of internal control are purpose, commitment, capability and monitoring. Government resources, structures, systems, processes and culture must support management and staff in achieving organisational objectives.

Internal control can assist by monitoring performance and providing reliable information on the effectiveness or otherwise of the current arrangements. This in turn, may lead to further management decisions or actions designed to improve the control environment.

However the process of taking decisions is recognised as being inherently flawed and no amount of control can prevent this. Therefore, to minimise this, it will be necessary to carry out risk assessments to ensure that those areas that are most susceptible to risk are clearly identified and protected.

Checklist for Establishing Managerial Control

The assessment of the four main objectives of internal control should be the focal point for establishing whether your organisation has adequate controls in place.

1. **The economical, efficient and effective use of resources;**
2. **The reliability and integrity of information;**
3. **Compliance with policies, plan, procedures, laws and regulations;**
4. **The safeguarding of assets against loss, misuse and damage due to waste, abuse, mismanagement, errors, fraud and irregularities**

The starting point is to ask yourself what documented evidence do I have to support each of these objectives of internal control?

Then you should prepare a check list and a file of all relevant documents used in your organisation that will support each objective.

For example under the objective - **The economical, efficient and effective use of resources**

- What does your organisation do to monitor performance?

- Do you have a comprehensive performance management system for each of your key operational and functional services

- Do you have monthly financial performance monitoring reports?

- Do you produce key performance indicators that are benchmarked?

- Do you produce annual statistics about your outputs?

- Do you have target setting for each operational and functional service?

For example under the objective – **The reliability and integrity of information;**

- Are all transactions recorded promptly when they occur?
- Do you have a management information system for decision making?
- What information do you provide to the public on a regular basis about your organisation?
- Do you have documented procedures and timetables for the production of management reports?
- Do your senior management have access to information relevant to their position and responsibilities?
- Do you monitor the use and requirements for information from both staff and the public?
- Do you provide the public with answers to their questions and complaints?
- Do you communicate effectively between staff and management on key personnel issues?
- Do you hold public meetings to discuss your performance and strategy?

For example under the objective - **Compliance with policies, plan, procedures, laws and regulations;**

- What does your organisation do to provide compliance?
- What internal procedures and laws regulate your organisation?
- Do you operate a Code of Ethics?
- Do you operate a Whistle Blowing Policy?
- Do you have a Corporate Complaints Procedure for both the public and staff?
- Do you have a risk management strategy?
- Who monitors compliance?
- Do you have Audit Committees, Scrutiny Committees

For example under the objective - **The safeguarding of assets against loss, misuse and damage due to waste, abuse, mismanagement, errors, fraud and irregularities.**

- Do you have security and controls for the various computer based systems?
- Do you have procedures for each computer system?
- Do you have daily back up of computer data?

- Do you have a disaster recovery plan?
- Do you monitor the use and performance of assets
- Do you have procedures for recording of fixed assets?
- Do you have physical stock taking of fixed assets?
- Do you have reports on the value and use of fixed assets?
- Do you assess the productivity of assets?
- Do you have regular information on the level of waste, fraud etc?

The above examples are a guide to some of the issues that should be considered when deciding whether internal control is functioning effectively in your organisation.

Key Points

For financial management to operate effectively in the Public Sector will require changes to the cultural and public administration operating environments that will bring about the empowerment of professional financial managers.

To achieve good sound financial management and control organisations must focus control activities on those areas of financial expenditure that are expected to provide the best use of public funds and services.

Part of this will be the development of Financial Regulations that set the framework and principles for managing the organisation's financial affairs. They apply to everyone in the organisation.

The FMC reforms will take time to understand the new concepts as well as bring about effective implementation. These FMC reforms must compliment other public administration reform programmes, which might be changing managerial and institutional arrangements across the public sector. Significant resources will often be needed to complete a FMC reform programme. This is most clearly demonstrated in the need to provide extensive training programmes and recruit new internal audit staff.

4. Responsibility and Accountability

Introduction

The need for Managerial Responsibility is an essential factor for sound financial management and control; however the Government, Ministers and all Senior Political Officials need to ensure that there is real commitment for Public Internal Financial Control. The setting of budget priorities to ensure the best use of public money is crucial to ensure that the best public services are provided.

By setting a good example in proper use of public funds and implementing the PIFC framework then the Government of Montenegro will satisfy the EU requirements for the closing of Chapter 32 – Financial Control.

This will require genuine support from the top and setting the tone for all the public sector to proceed in implementing sound financial management and control supported by an independent and decentralised Internal Audit Service.

Everyone (all staff) has a role to play in achieving Financial Management and Control, some greater than others. It is important to inform all staff about the need for better internal control and the expectation of improved and efficient public services. There are certain key players that are crucial for the success of PIFC in each organisation. These are as follows:

- Government
- Central Harmonisation Unit
- Head of Public Entity
- Chief Finance Officer
- Financial Management and Control Manager
- Heads of Departments
- Financial Staff
- All other staff
- Internal Audit Unit

Government

Appropriate financial control is firstly the responsibility of central and local government organisations which are accountable to the parliament and all national and foreign stakeholders, citizens and organisations, regarding the preparation and execution of the central and local budget.

As part of this responsibility the government provides guidance with strategies and policy papers and operationally with regulations and decisions that supports the implementation and continuous improvement of internal control.

Government acceptance of the need for a sound system of internal control is recognition that the public sector must deliver value for money and the best use of public money.

This will act as a means for the assurance of the orderly, ethical, economical, efficient and effective operations and the prevention of fraud and corruption in the public sector.

The adherence to the necessary corrective and preventive measures including administrative and judicial sanctions is the ultimate “setting the tone from the top” and a precondition for the implementation and performance of the effective internal control in the public sector.

Central Harmonisation Unit – Ministry of Finance

The Central Harmonisation Unit (CHU) is responsible for the development, guidance and co-ordination of the system of Public Internal Financial Control and is a Unit of the Ministry of Finance.

The CHU issues guidelines and makes proposals to public entities to make internal financial control more efficient by developing and updating methodology. It also evaluates on the basis of annual reports the entity of internal financial control in public entities and makes proposals for the improvement thereof.

The CHU in particular performs the following tasks:

- prepares methodologies for the implementation of financial management and controls in public entities,
- provides training programmes and training of persons responsible for and involved in financial management and control and internal audit;
- coordinates the establishment and development of internal financial management and control including internal audit;
- monitors the implementation of laws, regulations and standards for financial management and control and internal audit, ethical code of internal auditors, instructions and methodologies for financial management and control and internal audit;
- reviews the quality of the financial management and control system and internal audit within entities, with the objective of monitoring over implementation of recommendations for the purpose of collecting information for the improvement of work methodologies and standards;
- cooperates with national and international professional bodies and institutions in the area of financial management and control and internal audit.
- prepares annual consolidated report on the system of internal control for the Government with recommendations for improvement.

Head of the Public Entity

The Head of each Public Entity is responsible and accountable to the Government for the setting up and the continuous improvement of the FMC system in their entity. He/she needs to assess the risks to the entity so that internal controls are adequate to provide reasonable assurance that the specific and general objectives of the entity will be achieved. With this regard in particular he/ she must:

- ✓ have a clear understanding of the organisation's mission and ensures that the long and short term objectives of the organisation are effectively communicated to all employees and stakeholders;
- ✓ appoint a suitably qualified person as the FMC Manager to deliver a strategy for the organisation as a whole;
- ✓ review, understand and approve the risk management strategy;
- ✓ regularly discuss and update the risk register that reflects the actual objectives and risks
- ✓ defines acceptable risks;
- ✓ undertake appropriate measures to control risks, appoint the risk owner and monitor the implementation;
- ✓ undertake appropriate corrective measures in case of fraud, corruption and other irregularities;
- ✓ promote the use and need for Internal Audit to review the system of internal control and to make recommendations for improvement,
- ✓ submit the annual report on the progress of the system of internal control to the Central Harmonisation Unit.

The Head of the Public Entity adopts a plan that includes

- ✓ the necessary activities for establishing FMC,
- ✓ persons in charge of conducting the necessary activities, and
- ✓ timetable for the implementation of activities.

Chief Finance Officer

Although the Head of each Public Entity is responsible for establishing an adequate financial control system it is normal to have a responsible person at a senior level to be in charge of financial affairs and provide financial leadership and guidance to the organisation in all matters relating to finance.

The title of this position varies from country to country and even within countries e.g. - Director of Finance, **Chief Finance Officer**; Principal Accountable Officer; Accounting Officer, State Secretary- what is important is that the responsibilities of this position are clearly defined and explained.

It is likely that in a public sector based on professional managers that this management role would be probably second in order of importance, behind only the Minister or Head of the organisation.

In each organisation there must be a responsible person for managing and administration of the financial affairs. Using for example, the title Chief Finance Officer, their role is important and critical – not only in assessing risk and ensuring probity in the use of public money, but also in securing sound financial management and effective controls. In these areas the Chief Finance Officer can make an important contribution to the effectiveness of the organisation and help to demonstrate openness and transparency in the way it operates and conducts its business.

To be able to fulfil their responsibilities effectively and to facilitate robust corporate governance, the Chief Finance Officer needs to be at the heart of the organisation's decision making process and play a key role in the organisation – not only to ensure that finance views carry appropriate weight in policy and decision making but also so that he or she is able to intervene with authority if proper standards are not being met at any time.

There are five key roles that are critical to the achievement of the Chief Finance Officer statutory responsibilities:-

- maintaining strong financial management underpinned by effective financial controls;
- contributing to corporate management and leadership;
- supporting and advising politicians;
- supporting and advising managers and staff in their operational roles;
- leading and managing an effective and responsive financial service.

FMC Manager – Person Responsible for Financial Management and Control

The Head of the Public Entity must appoint a suitably qualified person responsible for the co-ordination of the FMC. This should probably be the Chief Finance Officer The key tasks are to:

- prepare a plan for the establishing of FMC and monitor the implementation,
- co-ordinate activities on establishing and developing FMC,
- assist the head of entity in establishing the FMC strategy,
- prepare and monitor the implementation of the plan for rectifying deficiencies of FMC
- prepare annual reports on FMC,
- report to the head of the entity on the current status and development of FMC,
- co-operate with the Central Harmonisation Unit of the Ministry of Finance.

Head of Department

One of the changes needed for the implementation of FMC is the introduction of the concept of delegation of authority and responsibility. This will mean that the Heads of Department (HoD) will have budgets to prepare, manage, execute, monitor and report for the staff and resources under their control.

The implementation of this change process will take time and involve the need for training of staff and changes in budgetary control, financial monitoring and reporting. This will need to be part of public administration reform that will impact on all staff.

Financial Staff

The staff involved in the various financial processes such as accounting and budgeting, payments to suppliers, payroll, debt management, treasury etc should all be aware of the implementation of PIFC and the role of FMC and Internal Audit Service.

Other Staff

As FMC covers the whole organisation it is important that all staff are aware and understand the need for financial management and control. They will be involved and will need to implement the various procedures and controls to ensure that the various financial processes are working properly.

Internal Audit Unit

Internal Audit (IA) is an independent, objective and consulting activity designed to improve an organisation's operations. It helps the organisation accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, internal control and governance processes.

The IA ubit reports directly to the Head of the Entity but IA must consult and co-operate with the FMC Manager to ensure that the PIFC process is moving in the same direction.

The IA unit is not responsible for the implementation of the financial management and control systems and risk management but it can provide advice.

It is the responsibility of the head of each entity to undertake measures to implement recommendations arising from internal audit service reports.

Key Points

FMC is an integral and interacting process undertaken by the Government, the Central Harmonisation Unit, the Head of the Entity, the FMC Manager, Internal Audit Service and requires all staff pursuing the specific objectives of each entity and general objectives which are as follows:

- Compliance of operations with legislation, regulations, internal policies, contracts and procedures,
- The provision of reliable, complete and timely financial reporting,
- Economic, efficient and effective use of funds,
- Safeguarding of assets against loss or waste caused by mismanagement, unjustified spending, theft and fraud.

The responsibility of public sector staff regarding these general objectives must be clearly expressed in the laws, regulations, codes, internal instructions and supported by the management at all levels of the entity. In order to be able to respond to their responsibility civil servants must have the access to necessary training and must have at their disposal the appropriate tools e.g. information’s, methodologies, material and human resources.

In case of suspected fraud, corruption or other irregularity and illegal acts civil servant must have the opportunity to report bona fide such cases and be protected against any repercussions.

5. Risk Management

Introduction

Risk Management is an important aspect of all our lives. We are all exposed to risk daily, at work and in our private lives, and often manage it subconsciously. We need to ensure that we think about it actively in the way we undertake our work. Current arrangements for corporate governance place significant emphasis on risk management and its methodologies have developed in recent times partly as a result. However, the reality is that risk management is not a separate activity but part of normal management responsibility – in the way that managers are also responsible for many aspects of financial and human resources management.

Risk can take various forms, e.g. financial risk, risk to projects, risk to the services we deliver, risk to the public or specific stakeholders, risks from missed opportunities or from policy failures, and risks to our reputation. They can affect our performance, our stakeholders, our customers and members of the public. We need a clear understanding of how such risks should be managed. Doing this properly is central to planning to succeed and avoiding failure; to meeting our key objectives and targets; to creating confidence in a watchful public; and to meeting the demands of good corporate governance. It will also make us better able to learn the value of appropriate risk-taking and benefit from innovation, promoted through a 'no blame' culture.

Risk can be defined as "Any event or issue that could occur and adversely impact the achievement of the political, strategic and operational objectives of the Government of Montenegro. Lost opportunities are also considered as risk".

Purpose

In recent years all sectors of the economy have focused on a strategy for managing risk as the key to making organisations successful in delivering their objectives whilst protecting the interests of their stakeholders. Risk is uncertainty of outcome, and good Risk Management Strategy (RMS) allows an organisation to:

- have increased confidence in achieving its desired outcomes;
- effectively constrain threats to acceptable levels; and
- take informed decisions about exploiting opportunities.

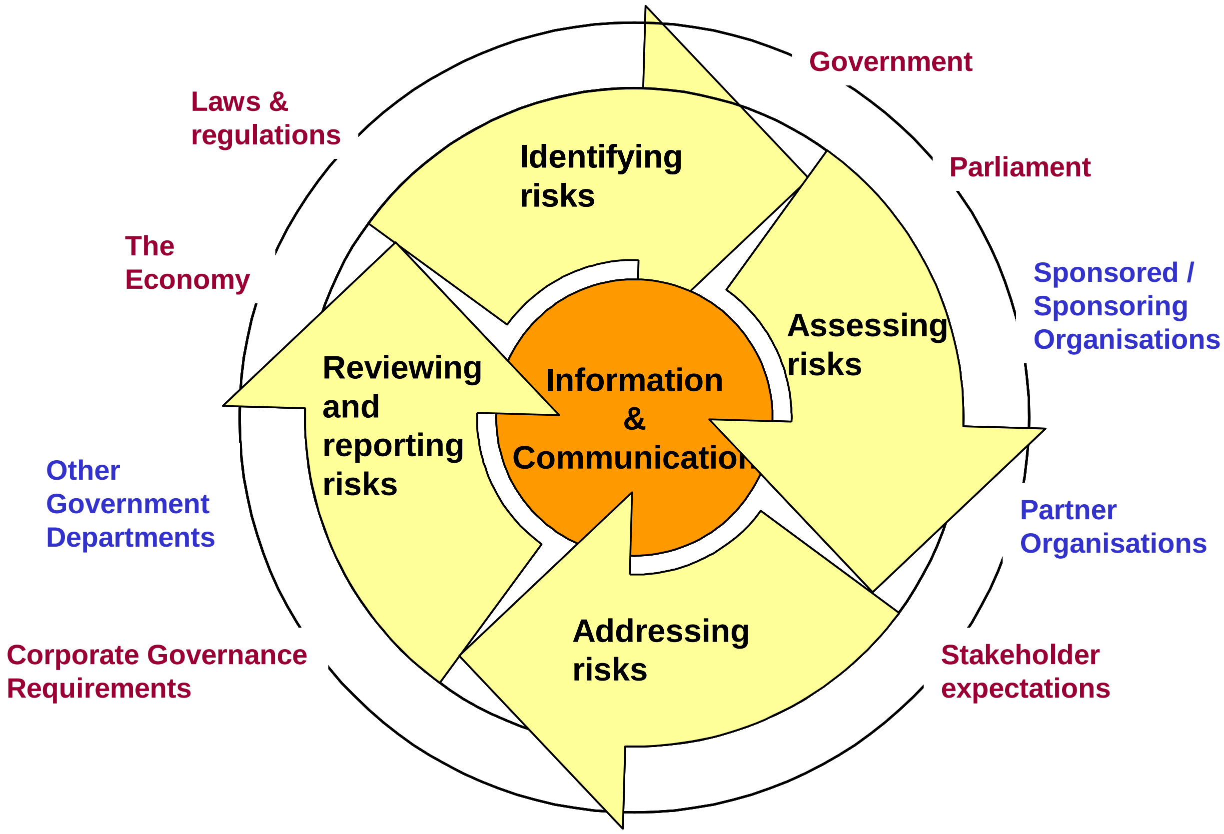
Good RMS also allows stakeholders to have increased confidence in the organisation's corporate governance and ability to deliver.

The management of risk is not a linear process; rather it is the balancing of a number of interwoven elements which interact with each other and which have to be in balance with each other if risk management is to be effective. Furthermore, specific risks cannot be addressed in isolation from others; the management of one risk may have an impact on another, or management actions which are effective in controlling more than one risk simultaneously may be achievable.

The ultimate intention of risk management is not to eliminate all risk but to reduce the level of risk to an acceptable level. That level will vary from organisation to organisation depending upon its appetite for risk which in turn is determined by its ability to manage risk situations as they develop and deal with the consequences of them occurring. Thus risks are taken but in a managed way.

Key Stages of Risk Management

1. **Identifying Risks**
2. **Assessing Risks - Risk Analysis and Evaluation**
3. **Addressing Risks**
4. **Reviewing and Reporting Risks**



Objectives

The objective of the RMS is to **identify and assess** risks so that the organisation can decide the best solution for **addressing** the risks. The most common solution is to introduce suitable internal controls to minimise the occurrence of risk. The steps involved are:

- to develop a risk register related to objectives which will **identify** and **assess** all significant risks facing the entity and so assist achievement of the entity's mission and objectives;
- to rank all risks in terms of likelihood of occurrence and expected impact upon the entity;
- to allocate clear roles, responsibilities and accountabilities for **addressing** the risk;
- to **review** compliance with laws and regulations, including the regular **reporting** on the effectiveness of the internal control system to minimise risks;
- to raise awareness of the principles and benefits involved in the risk management process and to obtain staff commitment to the principles of risk control.

Risk Register

The Risk Register will involve consideration of all potential risks facing the entity in pursuing its mission and achieving its objectives with risks broken down into appropriate headings (e.g. staffing, budgeting, information security, etc.) and identified with management at all levels.

All risks should be clearly defined together with measures for their control. Considering the adequacy of the control system will avoid duplication of resources as several of the identified risks may already prove to be effectively controlled.

It is important that the internal systems have in place adequate controls to minimise the identified risks. Where control weaknesses are identified by internal auditing or other, these should be noted and addressed.

Internal Audit will undertake the assessment of the internal controls to evaluate if the financial systems are functioning effectively to ensure with reasonable assurance that risks are being minimised

Risks can be categorised as external (political, financial, legislative, environmental) and internal (in respect of deadlines, qualitative, technological and operational). As not all risks represent equal significance to the entity, each area shall be ranked as e.g. insignificant, significant, very significant and disastrous in terms both of likely occurrence and impact.

Risks, having been identified and analysed and the risk acceptance determined the next step is to take measures to control them. This will involve the consideration of cost-effective action, which will be judged against risk ranking. The proposed action to be taken will then be mapped against the specified risk together with an implementation date reflected by the perceived urgency and the named person designated as responsible for managing the risk.

Benefits of Risk Management

Provided the risk management approach is effectively planned and executed the benefits derived are:

- Awareness of significant risks with priority ranking assisting the efficient planning of resources.
- Enhancement of focus for internal audit needs assessment and planning.

- Recognition of responsibility and accountability.
- As an aid to strategic and business planning.
- Identification of new opportunities.
- Action plan for the effective management of significant risks.

Stage 1 - Identifying Risks

In order to manage risk, an organisation needs to know what risks it faces, and to evaluate them. Identifying risks is the first step in building the organisation's risk profile. There is no single right way to document an organisation's risk profile, but documentation is critical to effective management of risk. There can be no exhaustive list of the risks that may affect the achievement of an organisation's objectives but, based on the definition of risk given in the previous topic, the following are categories that may be encountered:

- Anything that poses a threat to the achievement of a department's objectives, programs or service delivery for citizens;
- Anything that could damage the reputation of a department and undermine the public's confidence in it;
- Failure to guard against impropriety, malpractice, waste or poor value for money;
- Failure to comply with regulations such as those covering health and safety and the environment;
- An inability to respond to or to manage changed circumstances in a way that prevents or minimises adverse effects on the delivery of public services

The identification of risk can be separated into two distinct phases. There is:

- Initial risk identification (for an organisation which has not previously identified its risks in a structured way, or for a new organisation, or perhaps for a new project or activity within an organisation), and there is;
- Continuous risk identification which is necessary to identify new risks which did not previously arise, changes in existing risks, or risks which did exist ceasing to be relevant to the organisation (this should be a routine element of the conduct of business).

Risk identification methods

There are lots of methods to identify risks; none is perfect in giving you the picture you're looking for.

Some will provide you with quantities of items, areas at risks and will leave you confused about what doing next?

Conversely others will issue a few areas or activities at risk but with no precise information about risks.

The first tip could be: consider the time you have to identify the risks threatening your activities, it's quite different to identify the risks you face when driving your car compared to building a new bridge across a wide river.

The second tip is: Watch Behind, Think Ahead. Good risk analysis entails driving forward while looking in the rear view mirror. Information about the past is useful, but the primary concern is what could happen.

It's important to look for problems rather than waiting for them to find the organisation; proactive rather than reactive.

For example, if an organisation experiences unusual success or growth compared to its peers that may not be good news—it may be a warning. Just because it appears things are going well doesn't mean they actually are.

How to begin to identify Risks

Many methods exist, from a simple approach i.e. a list written on a “post-it”; to a more professional approach i.e. an organisation-wide approach driven by a team of specialists.

“Brain Storming”

This is the common tool when using a participative approach through organising workshops across the organisation. Generally, brain storming is the first step of risk assessment which is a very effective method to grasp information and opinions from all the levels of an organisation.

To organise the creativity of participants to the workshop, the workshop should use headings such as:

Strategic Level: Reputation, Financial, Service Provision, Political

Operational Level: Commercial, Human resource, Operational, Financial, Information technology, Asset management;

Alternative: - Assets, People, Reputation, Information, Continuity of Operations, Targets

A standard brain storming session is oral and no limit should be given to the attendee’s creativity, all opinions should add something to others.

But don’t say “*I don’t agree, It is like this or that”* but *“yes it is and I add this and that”.*

In some situations, people may be shy and unwilling to give their opinion, especially when several levels of staff in the same workshop. In that case, the “paper-storm” method may encourage people to give their opinion.

Opinions are written on a paper which is then folded and put in a basket. The facilitator takes the papers, writes them on a board and asks participants to start a new “paper storm round”.

Alternatively, opinions are written on "post-it" notepads and are sorted by the facilitator and stuck on the wall in logical groups.

Both, brain storming and paper storming, provide the organisation with a big quantity of items, it means that the process to analyse, sort and evaluate the risks may be quite long.

Use of check lists

This is the typical method for self assessment and to conduct interviews of executives.

Each risk is considered against a pre-agreed checklist. It is generally difficult to draw up a list that will provide parameters that can be used widely. They should be reviewed regularly to make sure that they remain relevant to the areas of operation being considered

The use of check lists is particularly relevant to review the risks; the previous analysis performed before give enough information to build check lists leaving nothing apart of the process while focusing on a precise scope.

Past experience

Historic records maintained by the organisation, or available to it from other sources, are valuable for identifying incidents, their frequency and impact. The information must be reliable and as comprehensive as possible, ideally identifying 'near misses' as well as actual incidents. If data is available for a three- or five-year period, this will reduce the possibility of short-term problems distorting the trends indicated.

These methods are used by experts who have access to databases and specific information sources to support thorough analysis. The use of experts may be quite expensive and long and it is normally devoted to high risks.

It is necessary to adopt an appropriate approach or tool for the identification of risk. Two of the most commonly used approaches are:

Commissioning a risk review: A designated team is established (either in-house or contracted in) to consider all the operations and activities of the organisation in relation to its objectives and to identify the associated risks. The team should work by conducting a series of interviews with key staff at all levels of the organisation to build a risk profile for the whole range of activities (but it is important that the use of this approach should not undermine line management's understanding of their responsibility for managing the risks which are relevant to their objectives);

Risk self-assessment: Each level and part of the organisation is invited to review its activities and to contribute its diagnosis of the risks it faces. This may be done through a documentation approach (with a framework for diagnosis set out through questionnaires), but is often more effectively conducted through a facilitated workshop approach (with facilitators with appropriate skills helping groups of staff to work out the risks affecting their objectives). A particular strength of this approach is that better ownership of risk tends to be established when the owners themselves identify the risks.

Stage 2 - Assessing Risks

In order to decide how to handle risk, it is essential not only to identify in principle that a certain type of risk exists, but also to evaluate its impact and assess the probability of the risk event occurring.

The methodology for analysing risks can vary, largely because many risks are difficult to quantify (e.g. reputation risks) while others lend themselves to a numerical diagnosis (particularly financial risks). For the former, a much more subjective view is the only possibility. In this sense, risk evaluation is more of an art than a science. However, the use of systematic risk rating criteria will mitigate the subjectivity of the process by providing a framework for judgments to be made in a consistent manner.

Risk assessment is an objective evaluation of risk in which assumptions and uncertainties are clearly considered and presented. Part of the difficulty of risk management is that measurement of both of the quantities in which risk assessment is concerned – Impact (potential loss) and Probability (of an event occurring) - can be very difficult to measure. The chance of error in the measurement of these two concepts is large. A risk with a large potential loss and a low probability of occurring is often treated differently from one with a low potential loss and a high likelihood of occurring. In theory, both are of nearly equal priority in dealing with first, but in practice it can be very difficult to manage when faced with the scarcity of resources, especially time, in which to conduct the risk management process. Financial decisions, such as insurance, express loss in terms of euro amounts.
Risk evaluation is concerned with assessing probability and impact of individual risks, taking into account any interdependencies or other factors outside the immediate scope under investigation:

- Probability is the evaluated likelihood of a particular outcome actually happening (including a consideration of the frequency with which the outcome may arise). For example, major damage to a building is relatively unlikely to happen, but would have enormous impact on business continuity. Conversely, occasional personal computer system failure is fairly likely to happen, but would not usually have a major impact on the business.

- Impact is the evaluated effect or result of a particular outcome actually happening

- Impact should ideally be considered under the elements of:
    - time
    - quality
    - benefit
    - people/resource

Risk measurement

The risk measuring is derived from the identification of the risks. It is considered in terms of *Impact* and *Probability*.

An example of measuring a risk Impact is delivered here below.

Rating	Ranking Impact	Description
3	High	Disruption of all essential programs/services Loss of major assets Serious environmental damage Death Significant loss of public trust Public outcry for removal of Minister and/or departmental official
2	Medium	Disruption of some essential programs/services Loss of assets Some environmental damage Serious injury Some loss of public trust Negative media attention
1	Low	Schedule delays to minor projects/services Loss of assets (low value) Temporary environmental effect First aid treatment Setback in building public trust Some unfavourable media attention

An example of measuring a risk Probability is below.

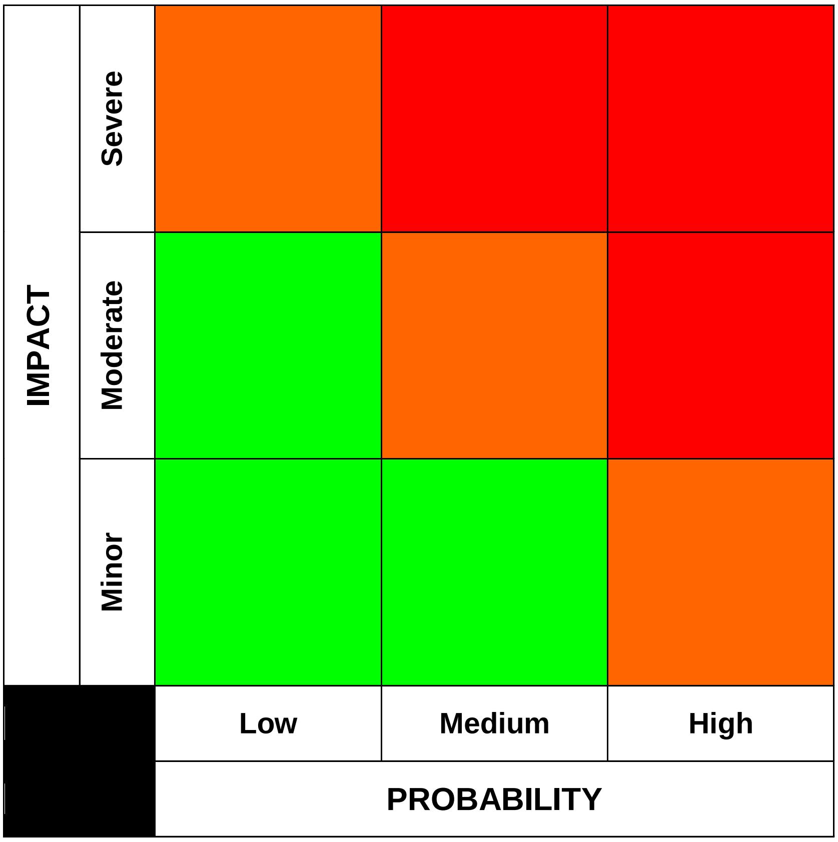
Rating	Probability	Description
3	High	The event is expected to occur in most circumstances
2	Medium	The event should occur at sometime
1	Low	The event occurring is unlikely

Risk Ranking

The overall risk ranking is derived from consideration of the conclusions reached in the analysis of the general control environment, the inherent risk and the measurement in terms of impact and likelihood.

The risk ranking will be identified following the intersection of the impact and likelihood. Overall risk is the combination of impact and likelihood, according the chosen method. Assessment and proposed action must be made according to individual judgement of circumstances. A purely mathematical calculation would be dangerously simplistic.

The categorization of high/medium/low level of risk results in a *“3*3” risk matrix* that is shown below.



Several variants exist, however, the most common practice is to use the “3*3” matrix that gives enough information in a simple way.
Worth mentioning is that management may consider some risks as <u>unacceptable</u> (human death, corruption…), even though impact and/or likelihood are medium or low, such risks must be rated as a decision rather than calculation to be pointed out all along the risk assessment process.
The “3*3” risk matrix will derive the risk rating. Or at this stage, the questions that should be answered are:

How to sort and rank risks coming from several processes?
In other words, how to prioritise the top risks that can cause the most damage?
The presentation of the result may be the list of process associated to the most important risks.

Stage 3 - Addressing Risks

The purpose of addressing risks is to turn uncertainty to the organisation's benefit by constraining threats and taking advantage of opportunities. Any action that is taken by the organisation to address a risk forms part of what is known as "internal control". There are five key aspects of addressing risk; tolerate the risk, treat the risk, transfer the risk, take the opportunity the risk presents, or terminate the risk. Each is explained in more detail below.

- **Tolerate the risk**

The exposure may be tolerable without any further action being taken. Even if it is not tolerable, ability to do anything about some risks may be limited, or the cost of taking any action may be disproportionate to the potential benefit gained. In these cases the response may be to tolerate the existing level of risk. This option, of course, may be supplemented by contingency planning for handling the impacts that will arise if the risk is realised.

- **Treat the risk**

By far the greater number of risks will be addressed in this way. The purpose of treatment is that whilst continuing within the organisation with the activity giving rise to the risk, action (control) is taken constrain the risk to an acceptable level. Such controls can be further sub-divided according to their particular purpose.

- **Transfer the risk**

For some risks the best response may be to transfer them. This might be done by conventional insurance, or it might be done by paying a third party to take the risk in another way. This option is particularly good for mitigating financial risks or risks to assets. The transfer of risks may be considered to either reduce the exposure of the organisation or because another organisation (which may be another government organisation) is more capable of effectively managing the risk. It is important to note that some risks are not (fully) transferable – in particular it is generally not possible to transfer reputation risk even if the delivery of a service is contracted out. The relationship with the third party to which the risk is transferred needs to be carefully managed to ensure successful transfer of risk.

- **Take the opportunity the risk presents**

This option is not an alternative to those above; rather it is an option which should be considered whenever tolerating, transferring or treating a risk. There are two aspects to this. The first is whether or not at the same time as mitigating threats, an opportunity arises to exploit positive impact. For example, if a large sum of capital funding is to be put at risk in a major project, are the relevant controls judged to be good enough to justify increasing the sum of money at stake to gain even greater advantages? The second is whether or not circumstances arise which, whilst not generating threats, offer positive opportunities. For example, a drop in the cost of goods or services frees up resources which can be re-deployed.

- **Terminate the risk**

Some risks will only be treatable, or containable to acceptable levels, by terminating the activity. It should be noted that the option of termination of activities may be severely limited in government when compared to the private sector; a number of activities are conducted in the government sector because the associated risks are so great that there is no other way in which the output or outcome, which is required for the public benefit, can be achieved. This option can be particularly important in project management if it becomes clear that the projected cost / benefit relationship is in jeopardy.

Residual risk – Inherent risk

Thinking about risk frequently focuses on residual risk (i.e.- the risk after control has been applied which, assuming control is effective, will be the actual exposure of the organisation). Residual risk, of course, will often have to be re-assessed – for example, if control is adjusted. Assessment of the anticipated residual risk is necessary for the evaluation of proposed control actions.

Care should also be taken to capture information about the inherent risk. If this is not done the organisation will not know what its exposure will be if control should fail. Knowledge about the inherent risk also allows better consideration of whether there is over-control in place – if the inherent risk is within the risk appetite, resources may not need to be expended on controlling that risk. This need to have knowledge about both inherent and residual risk means that the assessment of risk is a stage in the risk management process which cannot be separated from addressing risk; the extent to which the risk needs to be addressed is informed by the inherent risk whereas the adequacy of the means chosen to address the risk can only be considered when the residual risk has been assessed.

Risk appetite

The concept of a “risk appetite” is important to understanding and achieving effective risk management and it is essential to consider it before moving on to consideration of how risks can be addressed. The concept may be looked at in different ways depending on whether the risk (the uncertainty) being considered is a threat or an opportunity:
When considering threats the concept of risk appetite embraces the level of exposure which is considered tolerable and justifiable should it be realised. In this sense it is about comparing the cost (financial or otherwise) of constraining the risk with the cost of the exposure should the exposure become a reality and finding an acceptable balance
When considering opportunities the concept embraces consideration of how much one is prepared to actively put at risk in order to obtain the benefits of the opportunity. In this sense it is about comparing the value (financial or otherwise) of potential benefits with the losses which might be incurred (some losses may be incurred with or without realising the benefits).
It should be noted that some risk is unavoidable and it is not within the ability of the organisation to completely manage it to a tolerable level – for example many organisations have to accept that there is a risk arising from terrorist activity which they cannot control. In these cases the organisation needs to make contingency plans

Unacceptable risk

Management may consider some risks as unacceptable, (human death, corruption…) even though impact and/or likelihood are medium or low, such risks must be rated as a decision rather than calculation to be pointed out all along the risk management process.
An unacceptable risk generally provides only unfavourable consequences, its mitigation most commonly relies on contingency plans.

Stating that some events represent unacceptable risks is a strong signal sent by management to keep vigilance against them and strengthen controls.
In that case, the risk appetite is nil!
In either case the risk appetite will best be expressed as a series of boundaries, appropriately authorised by management, which give each level of the organisation clear guidance on the limits of risk which they can take, whether their consideration is of a threat and the cost of control, or of an opportunity and the costs of trying to exploit it. This means that risk appetite will be expressed in the same terms as those used in assessing risk. An organisation's risk appetite is not necessarily static; in particular the Board will have freedom to vary the amount of risk which it is prepared to take depending on the circumstances at the time.

Further applications of the concept of risk appetite include:

Resource allocation: Once the risk appetite level is set, it is possible to review if resources are targeted appropriately. If a risk does not correspond to the agreed risk appetite, resources could be focused on bringing it to within the tolerance level. Risks, which are already within the agreed tolerance level, could be reviewed to see if resources could be moved to more risky areas without negative effects. Customs, Inland Revenue, the Police and Fire Service all use risk-based resource allocations to prioritise allocation of resources;
Project initiation: When taking the decision whether to initiate a new project, and when undertaking subsequent Office of Government Commerce Gateway reviews, risk appetite can be used as a guide on whether to proceed with the project and also to help identify and manage risks which may impede the success of the project.

Stage 4 - Review and reporting of Risks

The Risk Management process should be subject to periodic review. This will ensure that the risk register is updated, taking into account the constantly changing environment, amended objectives, recognising that new risks arise whilst others either disappear or become less significant in terms of priority.

Monitoring the effectiveness of the process is vital and the entity should ensure that:

- Clear responsibility exists for the management of a particular risk or risk area.
- Reporting arrangements should be in place, which will highlight changes in risk priority and any instances where risks are not being effectively managed.
- Procedures are in place, which will ensure the review of the effectiveness of the overall risk process.
- Methods are established for the appraisal of the performance of the risk management process and that suitable performance standards are implemented by which the process may be reviewed.

The management of risk has to be reviewed and reported on for three reasons:

- To monitor whether or not the risk profile is changing;
- To gain assurance that risk management is effective,
- And to identify when further action is necessary.

Processes should be put in place to review whether risks still exist, whether new risks have arisen, whether the likelihood and impact of risks has changed, and report significant changes which adjust risk priorities, and deliver assurance on the effectiveness of control. In addition, the overall risk management process should be subjected to regular review to deliver assurance that it remains appropriate and effective. Review of risks and review of the risk management process are distinct from each other and neither is a substitute for the other.

The review processes should:

- ensure that all aspects of the risk management process are reviewed at least once a year;
- ensure that risks themselves are subjected to review with appropriate frequency (with appropriate provision for management's own review of risks and for independent review/audit);
- make provision for alerting the appropriate level of management to new risks or to changes in already identified risks so that the change can be appropriately addressed.

A number of tools and techniques are available to help with achieving the review process:

- Risk Self Assessment (RSA) is a technique which has already been referred to in the identification of risk. The RSA process also contributes to the review process. The results of RSA are reported into the process for maintaining the organisation-wide risk profile. (This process is also sometimes referred to as CRSA – "Control and Risk Self Assessment");

- "Stewardship Reporting" requires that designated managers at various levels of the organisation report upwards (usually at least annually at the financial year end, and often on a quarterly or half yearly interim basis) on the work they have done to keep risk and control procedures up to date and appropriate to circumstances within their particular area of responsibility. This process is compatible with RSA; managers may use RSA as a tool to inform the preparation of their Stewardship Report;

In addition to these formal tools, individuals, work groups and teams should constantly by considering the risk issues which they face in the work they are doing.

Internal Audit's work provides an important independent and objective assurance about the adequacy of risk management, control and governance. Internal audit may also be used by management as an expert internal consultant to assist with the development of a strategic risk management process for the organisation. It will have a wide ranging view of the whole range of activities which the organisation undertakes, and will already have undertaken some form of assessment to inform its planning of systems and processes to be audited. However it is important to note Internal Audit is neither a substitute for management ownership of risk nor a substitute for an embedded review system carried out by the various staff that have executive responsibility for the achievement of organisational objectives.

An organisation may have specialist review and assurance teams which have been established for a particular purpose (for example, Accounts Inspection Teams, or Compliance Review Teams). Their work contributes to the assurances available about the risk and control systems in use in the organisation. "Stewardship" assurance mechanisms, whereby line managers give account of their stewardship of their areas of responsibility, are also important, especially in organisations with highly devolved control structures.

6. COSO Framework

Introduction

The COSO Model which was previously mentioned in Chapter 2 is a framework which has become a popular method for implementing and assessing an effective internal control system.

Internal control consists of five interrelated components. These are derived from the way management runs the organisation, and are integrated with the management process. Although the components apply to all entities, small and mid-size organisations may implement them differently than large ones. Its controls may be less formal and less structured, yet a small organisation can still have effective internal control

Five Key Components

- Control environment;
- Risk assessment;
- Control activities;
- Information and Communication; and
- Monitoring of controls

These are the original five components that were established but these have since been increased to eight by separating the components. At this time the focus will be on the original five but the three incorporating the three additional components within the original model.

The new Enterprise Risk Management (ERM) COSO framework emphasizes the importance of identifying and managing risks across the enterprise. The new COSO framework consists of eight components:

1. Control environment;
2. Objective setting;
3. Event identification
4. Risk assessment
5. Risk response
6. Control activities
7. Information and communication
8. Monitoring.

6.1. Control Environment

In accordance with Article 7 of the Public Internal Financial Control Law the Control Environment emphasises the need for:

1) Personal and professional integrity and ethical values of heads and employees;
2) Management and method of governance;
3) Setting missions and goals;
4) Organisational structure, hierarchy in assignment of responsibilities and authorities, rights and obligations, and reporting levels;
5) Written rules and human resource management practices;
6) Competence of employees.

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

Control environment is the attitude toward internal control and control consciousness established and maintained by the management and employees of an organisation. 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 organisation.

The control environment is further affected by the organisation's structure and accountability relationships.

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

Ethical Values and Integrity are key elements contributing to a good control environment.

They are the standards of behaviour that form the framework for employee conduct. 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 organisation;
- Leadership by example;
- Commitment to excellence;
- Respect for authority;
- Respect for employees' rights; and
- Conformance with professional standards.

People in an organisation 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 organisation, it is everyone's responsibility to demonstrate integrity.

Management encourages integrity by:

- Establishing and publishing a code of conduct;
- Complying with the organisation's ethical values and code of conduct;
- Rewarding employee commitment to the organisation's ethical values;

- Establishing methods for reporting ethical violations; and
- Consistently enforcing disciplinary practices for all ethical violations.

Employees should know general acts governing the ethical behaviour of civil servants with the special attention paid to the rules on avoidance of the conflict of interest, prevention of fraud and reporting on suspected corruption, fraud and other illegal deeds. The head of the public entity adopts internal procedure that every new employee with the signing the work contract receives the legal document (e.g. code of conduct, civil servants act, work contract stipulations) and is given respective training. Public entities in a specific field of activity e.g. police, tax, customs and similar should have specific code of conducts and specific training for their employees. It is important that every case of infringement is taken in procedure as a demonstration of the decisive attitude of the management.

Supportive Attitude is a disposition that encourages desired outcomes. Since internal control provides management with reasonable assurance that the organisation's mission is being accomplished, management should have a supportive attitude toward internal control that permeates the organisation.

Executive management should set a tone that emphasises the importance of internal control.

Such a tone is characterised 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 that they understand their role.

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

The mission of an organisation should be a statement, approved by executive management and/or the governing board of the organisation. Management should tell employees about the organisation'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.

Structure is the framework in which the organisation's plans are carried out. It should define the functional sub-units of an organisation and the relationships among them. An organisation 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 organisation as a whole, the relationships among its various components and where they fit into the organisation. Management should review this chart periodically to ensure it accurately reflects the organisation's structure.

Management should delegate authority and responsibility throughout the organisation. Management is responsible for organising the entity's authority and accountability relationships among various functions to provide reasonable assurance that work activities are aligned with organisational 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 organisation helps ensure that employees are aware of their duties and responsibilities, and know the extent to which they are accountable for activities.

The entity should have internal organisation chart with clearly identified staff posts. Each post should have a job description that provides details of the key tasks, responsibilities and required qualifications and experience. The organisational chart is regularly updated reflecting changes of regulations and objectives. The head of the public entity provides for that

- ✓ every employee knows and understands the mission and objectives of the entity and of his organisational unit, his duties and expected results,
- ✓ every employee has the possibility of the necessary training in relation to his tasks,
- ✓ every employee has the opportunity of at least one meeting with his senior per year to discuss the objectives, results, career development and proposals for improvement,
- ✓ are all the employees included in the human resources programme development regarding their experiences, results, interests, career development possibilities and entities objectives,

The staff posts specifically exposed to risks (e.g. expressed conflict of interest, access to cash and information, special powers) should be identified and appropriate control measures put in place, such as segregation of duties, double signatures, rotation of personnel, use of holidays, mandate limitations, supervision.

The head of the public entity sets up an appropriate reporting system regarding the risk management, internal control and internal auditing with clear relations regarding the head of the public entity, the FMC Manager, the internal auditor and managers at all levels.

A good practice is that the FMC Manager has a post box for receiving reports and complaints including anonymous letters on possible irregularities and other information on weaknesses of internal control. All of these matters must be investigated as soon as possible.

6.2. Risk Management

Objectives setting at all levels

Risk should be assessed and managed through an organisation-wide effort to identify, evaluate and monitor those events that threaten the accomplishment of the organisation's objectives. 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.

The precondition of the risk management is the updated assessment of the entity's mission, specific and general objectives at all levels and at all working posts, together with the identification of the resources required. Good practice is likely to include:

- ✓ A transparent process for defining and prioritising objectives and targets that involves the participation, commitment and agreement of the head of the entity together with any other bodies who play a participative role in the likely achievement of objectives;
- ✓ The establishment of expected standards of performance together with the means by which the achievement of these standards can be measured;
- ✓ An identification of possible options for achieving objectives and an agreement on the best possible option taking into account internal and external factors;
- ✓ Clear forecasts of likely activity and operational needs;
- ✓ An identification of any factors or external influences that could have an impact on the achievement of objectives i.e. an identification of risks that may influence the achievement of objectives
- ✓ A consideration of how these risks should be managed and when necessary an outline of any contingency plans, should the chosen options to achieve objectives fail for any reason;
- ✓ A documentation of the entity's objectives, targets and plans and the communication of these to all relevant employees inside the entity and those with an interest or role outside the entity.

Risk identification and analysis

The head of the public entity is responsible for the identification and the analysis of the key risks that may affect the entity's ability to achieve its objectives. Risk identification shall be performed in relation to the objectives set for all major business processes and is done during the annual budget planning process of the entity. All risks should be clearly defined together with the measures for their control.

The entity should then design and implement processes on a basis of plan prepared by the FMC Manager and adopted by the head of the entity by which key risks can be managed to, and maintained at, an acceptable level. In doing so the head of the entity needs to consider:

- The nature and extent of the risks facing the entity;
- The likelihood of the risks occurrence;
- The impact of the risks if occurred;
- The extent and categories of risk which it considers acceptable for the entity to bear;
- The ability of the entity to reduce the incidence of the risks concerned occurring by applying key financial and other controls and
- The costs of operating certain controls relative to the benefits obtained in managing the related risks.

Risks may be general to the public sector or specific to a particular public entity and activity or as a result of the pursuit of a particular objective or strategy. Examples of key risks that may affect public entity could include:

- Incorrect or out of date objectives
- Unreliable inventory-assets are not evidenced

- Major entity restructuring
- Skills shortage
- Fraud and corruption
- Compliance with laws and regulations
- False and misguiding reporting
- Changing political, economic, legal or social environment
- Adequacy of key financial and management information
- Inadequate protection of assets and information
- Ineffective investment or use of obsolete technology
- Unrecorded liabilities
- Unauthorised access to IT systems
- Breakdown in accounting system
- Inadequate debt management
- Unreliable or untraceable accounting records
- Physical disasters
- Inadequate service from suppliers or delegated agents
- Inefficient processing
- Poor customer service
- Loss of reputation

This list can never be exhaustive and public entity should concentrate on prioritising and managing key risks to the achievement of its objectives. It is important to recognise that risk should not be seen only negatively as this could stifle initiative and potential improvements or opportunities may be missed.

Following risk identification, impact assessment of such risks is done in relation to the probability of risk occurrence and possible impact that may adversely influence the attainment of entity's objectives.

Risks being identified and analysed, the risk acceptance determined, the next step is to take measures to control them. This involves the consideration of cost-effective action, which is judged against risk ranking, likelihood of occurrence and impact. The proposed action to be taken is then mapped against the specified risk together with an implementation date reflected by the perceived urgency and the named person designated as responsible for managing the risk. Considering the adequacy of the control system avoids duplication of resources as several of the identified risks may already prove to be effectively controlled.

Assessed risks are entered in the central risk register (Annex 2a) of the entity containing business objectives, identified risks description, classification, probability of risk occurrence and possible impact, envisaged risk control measures and persons responsible for their implementation.

Risk register shall be regularly reviewed as the risks that affect the entity are unlikely to remain static but will be constantly changing.

Risk management strategy is compiled based on data from the risk register.

Objectives achievement monitoring

The head of the public entity ensures that:

- ✓ The person responsible for the maintaining of risk register, the FMC Manager, is appointed and given the necessary training, resources and information,
- ✓ The internal procedure referring to risk identification and analysis is adopted and updated,
- ✓ Every employee is informed about the general and specific objectives and expected results of each activity and work post,
- ✓ Objectives are clear and understandable, detailed and precise, compliant with the entity's mission, measurable and verifiable, ambitious and meaningful and time dependable.
- ✓ Objectives must be compliant with regulations, budget and human resources,
- ✓ Follow up of the objectives is assured and measures provided for the case of non achievement,
- ✓ Once yearly or in case of changes of objectives, activities or other, risks are systematically analysed for their probability of materialisation and impact, define the acceptable risk, asses the control measures, their weaknesses or over control and address the findings, appoint risk owners.

6.3. Control Activities

Control activities in the broader sense encompass all the measures i.e. policies, procedures, activities, actions adopted by the head of the public entity to control risks that may influence the achievement of the entity's objectives. As control is susceptible to cost/benefit judgments, human error, parties working together to circumvent controls, senior management being able to override controls, internal control can only provide reasonable and not absolute assurance.

The head of the public entity is responsible and should be accountable for the development of the appropriate control that provides reasonable assurance that entity's purpose, mission and objectives can be achieved and risks are properly controlled.

The attitude of the head of the entity and senior management is critical as it 'sets the tone' of the public entity by conveying the clear message to employees and stakeholders through words and actions, that integrity and ethical values must not be compromised.

The corporate culture of the entity is reflected in leadership, philosophy and operating style, the assignment of responsibilities and the way in which the head of the entity and the senior management observe the operation of control procedures.

The control environment reflects the commitment and attitude to the implementation and maintenance of effective control, influences the design and operation of control policies and procedures and determines how effective the control is in mitigating risks and assuring the achievement of objectives.

The existence of an internal audit function does not diminish the responsibility of the head of the entity for developing, implementing and monitoring effective control. Internal audit itself is a unique part of the overall internal control system as it evaluates the effectiveness of internal controls to give assurance to the head of the entity on the extent to which the control can be relied upon.

Control is a major but not the only responsibility of management. Control is only one aspect involved in managing an entity. Management must decide what strategy or objectives should be set.

Controls are dynamic and subject to change and must be developed over time and may be changed as a result of management initiative or in response to findings and recommendations by both internal and external auditors.

They must be adapted over time to respond to external factors, risks, changes in priorities and technological developments. The head of the entity should provide for the review of the adequacy of the control structure on a regular basis to ensure that it continues to meet existing and changing control requirements and is appropriate to assure the achievement of entity's objectives and strategies. Control should be cost-effective, risk-based and adding value.

Control requirements and application may vary between or within entities. The type, scope and strength of control may be different from one entity to other and often within the same one. This may be because of legitimate reasons such the nature of the entity, the purpose, mission, its objectives, the internal and external environment and the degree of risk that is involved or can be tolerated. Different control practices may also exist as a result of the degree of centralisation or decentralisation in public administration, within an entity or due to personnel and human factors.

Control should be considered as a component of a whole system rather than in isolation. A control should rarely be viewed in its own right but on how it inter-relates with other planned or existing controls. The absence of a control at a certain point may not necessarily be a weakness if there are controls elsewhere that compensate effectively for its absence.

It is important that the cost of implementing the control does not exceed the benefits derived. Control uses always relatively scarce resources and the inappropriate balance of control may lead to inefficiencies. Over-control is not only cost inefficient but may lead to a failure to meet objectives and targets. The head of the entity should make judgments about the relative costs and benefits of control and implement the one, necessary to achieve the entity's objectives within an acceptable risk he has set. Therefore the level and application of control should be based on a sound risk analysis and be commensurate with the risk involved.

It is important that after executing control it is clearly evidenced what was controlled, when and by whom. Possible way to evidence control is the utilisation of the check list that can be paper based or electronic documents.

To be effective, control should be consistently applied. Control must be designed and implemented to function consistently as planned throughout the period, effected with care by all employees involved and not bypassed when key personnel are away or the workload is heavy. Control should not be overruled by seniors and every exception to standard procedures should be justified, evidenced and timely reported to the FMC Manager.

Planning involves the determination of aims, objectives and targets of the entity together with the identification for their achievement necessary means. Good planning practice is likely to include:

- A transparent process for defining and prioritising objectives and targets that involves the understanding, participation and commitment of employees involved;
- Clear forecasts of likely activity and operational needs;
- An identification of the risks that may influence the achievement of objectives together with a consideration of how these risks should be managed;
- The establishment of criteria and indicators by which the objectives achievement can be measured;
- An identification of possible options for achieving objectives and an agreement on the best possible option taking into account risks;
- An outline of any contingency plans should the risk materialise;
- A documentation of the entity's objectives and plans and the communication of these to all relevant employees and those with an interest or role outside the entity.
- There should be a medium term period and more detailed short-term plans setting out the priorities and objectives for a specific budgetary period.

It is important to recognise that planning is a continuing process and plans should not be static. In particular there should be sufficient steps taken to highlight and investigate unexpected performance and to initiate corrective action to try to ensure that objectives are met.

General characteristics of controls

Timely	Detect problems early enough to limit costly exposures.
Economic	Provide "reasonable" assurance of achieving intended results at a minimum cost and with fewest undesirable side effects.
Accountable	Help people demonstrate their accountability for assigned tasks.
Well-placed	Positioned where they are most effective.
Flexible	Will accommodate changes to procedures without themselves needing to be changed.
Identify cause	Identify not only the problem but also the cause.
Appropriate	Meet management's needs.

For control activities to operate properly the following points should be considered:

- Duties are logically segregated among different people to reduce the risk of fraud or inappropriate actions;
- Management provides staff with suitable training in the key duties;
- Regular financial reconciliations take place;
- Access to operating systems is restricted by functionality – example read only access
- Passwords to operating systems are regularly changed;
- Data is backed up daily and stored off site;
- Exception reports are produced that inform management of large financial transactions;
- Management monitors actual performance compared to budget on a monthly basis.

- Arithmetic checks are performed for a sample of transaction on a regular basis.

Management should establish the control activities that reduce the risk exposures to a level that is reasonable to a prudent and informed manager in the public sector.

In addition the following control activities all add to improving the control environment:

1. Good supervision of staff;
2. Documented procedures;
3. Work kept up to date and regular reconciliation;
4. Monthly financial and operational reports;
5. Meetings to discuss monthly reports;
6. Open communication with all levels of staff;
7. Maintaining adequate staffing levels;
8. Providing support to staff in social and welfare issues.

Categories of Control

Controls can be categorised as follows:

Preventive – designed to prevent the occurrence of inefficiencies, errors or irregularities. These cannot guarantee that the controlled factor will not occur, but they do reduce the chance of it occurring.

Examples include segregation of duties and authorisation controls.

Detective – designed to detect and correct errors, inefficiencies or irregularities. They may not give absolute assurance since they operate after an event has occurred or an output has been produced but they should reduce the risk of undesirable consequences as they enable remedial action to be taken. Detective controls are most effective when they form part of a feedback loop in which their results are monitored and used to improve procedures or preventive controls.

Examples include post payment confirmation, stock verification and bank reconciliations.

Directive – designed to cause or encourage actions and events necessary to the achievement of objectives.

Examples include policies and procedures, the setting of targets, and adequate training and staffing.

Corrective controls are designed to correct errors that have been detected.

Examples are contingency or disaster recovery planning.

In practice, the above categories of control may not be clearly distinguished and a single control may operate to cover two or more functions. Supervision, for example, covers all four types. Well organised and managed corrective actions and processes are, obviously and logically, also necessary when control weaknesses and failures occur.

Examples of Controls

In order to improve the internal control system each organisation should consider having the following operational controls

Written Guidance

Key policies and procedures should be documented to ensure that all employees involved in a process are aware of their responsibilities and duties and know how to perform their tasks. Instructions, procedures and manuals should be clear, accessible to all who require them and easy to refer to. Guidance of this nature must be regularly reviewed as procedures can be enhanced or become obsolete. Employees should be made aware of changes to make sure that the new instructions are properly implemented. Documents should be version controlled so that there is an adequate trail between procedural changes. Instructions should include descriptions of who should perform a particular task together with a description of all the documents or computer programs that need to be used.

Defined responsibilities and Delegation

The responsibilities of management and all the employees regarding their role in achieving the entity's objectives must be clearly defined. When delegating it should be made clear that the head of the entity and management at all levels accordingly remain responsible and accountable to the senior for the functions that have been delegated. A delegation should be always in written form clearly expressing tasks and assignments, with precise definition and limits of responsibilities and authorities (regular tasks, limits of amounts,) in some circumstances it may be appropriate, economic or necessary to use the services of other organisations outside the entity to assist in achieving objectives. When this is the case, it is important that the nature of the service required and the performance expected is clearly defined in a formal agreement. This may be a signed memorandum or an agreement between the two public entities or with private entity. There must be suitable monitoring procedures in place to ensure that the delegated organisations perform the tasks required, in the manner required, and that any changes required are quickly implemented and instructions/contracts updated. Obligations must be placed on delegated organisations to adopt systems and procedures that are consistent with those of the entity. The written agreement should include the rights of access to information, premises and staff.

Span of Control

The most effective span of control between the different units of the entity and within those units should be set. The appointment of too many layers of management on one hand, or too many staff for managers to control, or too great a burden of responsibility on individual managers on the other, may result in an ineffective control.

Segregation of Duties

There should be a clear separation (wherever possible) of posts performing the tasks of initialisation, authorisation and payment, etc. In principle no individual should have responsibility for more than one of these tasks. In case of smaller organisation additional controls should be foreseen. Each entity should establish and maintain an entity chart that clearly sets out the structure of the entity and the roles and responsibilities of each unit and each separate function within that unit or work post.

Sensitive work posts and job rotation

There are work posts within the entity, which because of their nature, status, responsibility or speciality can be classified as sensitive work posts that require particular attention due to the risks associated with the failure or potential abuse by an individual occupying this work post. Entity should seek to limit the number of these work posts by introducing a segregation of duties. Where this is not possible the employees of these work posts should be subject to enhanced supervision. There should also be procedures put in place to ensure that there is regular job rotation. This may entail regularly shifting employees to deal with different case work, claimants, customers or accounts or by periodically transferring a different member of employees to perform these duties. It is important that entity maintains a register of each work post it considers to be sensitive and records the manner in which the sensitive work post is supervised. The status and supervision of sensitive work posts should be regularly reviewed to ensure that the measures are appropriate.

Key areas of Control

Recruitment Controls *(Annex 3a)*

The head of the entity must ensure that the entity is adequately staffed if it is to pursue the mission and achieve its objectives. Control over recruitment should particularly focus on the following aspects:

- There should be a clear identification of the numbers of staff required, the experience, minimum educational requirements and professional expertise or qualifications. These requirements are not static and change as the entity changes so they should be subject to regular review.

- All employees should be recruited on the basis of fair and open competition so that the most able and appropriate candidate is selected. Recruitment should be performed against a clear description of the task and the attributes required. Posts should be advertised in appropriate media. Applications should be encouraged on official application forms to ensure consistency of treatment. Candidates should undergo a formal interview and be assessed against a standard which is set out and documented in advance. Wherever possible, to control risk of conflicts of interest and assure objectivity this should be undertaken by a commission rather than by a single official. Those performing interviews should receive adequate training in recruitment interviewing. Where it is considered necessary, candidates may undergo additional selection procedures or tests. The qualifications and experience quoted by candidates should be validated before a confirmatory appointment is made. This may involve additional checks on career history, references and when required the confirmation of the lack of a criminal record. It may be appropriate for certain appointments to be made for a probationary period subject to adequate performance, before the appointment is made permanent.

- Weaknesses within human resources can lead to mismanagement, error and abuse, which can undermine the effectiveness of the financial management and control system. The performance of employees in the conduct of their duties should be regularly reviewed. Areas of strength and weakness should be identified and appropriate procedures employed to recognise good performance and deal with instances where performance needs to be improved. Entity needs develop and communicate disciplinary and inefficiency procedures for those who transgress expected codes of conduct or whose performance fails to meet expectations over a defined period of time.

- The Entity should implement measures to ensure that each employee is adequately trained to perform his duties and his potential developed to undertake wider duties in view of the career development.

- The Head of the entity must ensure that the work and performance of the employees comes under proper scrutiny by supervision to ensure that standards and instructions are being applied correctly. It should be remembered that inadequate supervision may lead to error, failure to achieve objectives or even fraud but too rigid a supervisory regime may also stifle innovation and slow down the process to an unacceptable degree.

Accounting Controls

Accounting procedures should follow the requirements set out in the relevant laws, acts and regulations. The head of the entity should ensure that all relevant employees are familiar with these requirements. The procedures should be adequate to ensure that any reports made are complete, accurate and timely, all errors and omissions identified, dealt with and corrected in good time. There should be regular reconciliation processes between accounts, ledgers, bank details and amounts authorised to assist in ensuring the accounts are accurate, up to date and properly controlled.

Finance and Accountancy Procedures

Entity should draw up and maintain a set of Internal Finance and Accountancy Procedures that is consistent with the delegated financial and accounting responsibilities. This should include procedures and principles set out in these guidelines but may also, where appropriate, incorporate detailed guidance in the following areas:

- drawing up the financial plan of receivables and expenses;
- preparation of the procurement plan;
- execution of public procurement;
- preparation of the grants plan;
- preparation of the borrowings/debt management and issuance of guarantees plan;
- authorisation of payments;
- preparation of the subsidies, grants and other transfers from the budget plan;
- preparation of the sale, disposal or substitution of assets;
- preparation of the plan regarding the use of the current and the long-term budget reserve;
- assumption of commitments debiting the central budget;
- chart of accounts;
- execution of payments from the central budget;
- recording and dealing with irregularities;
- recovery of claims in favour of the central budget;
- liquidity planning;
- repayments to the budget planning;
- safeguarding of physical assets.

Payments and Receipts

Payments and receipts may take place via a number of means. For instance:

- Electronic methods either directly to or from a bank account;
- Paying orders;
- Cash.

It is vital that payments are made only to those who are entitled or eligible to receive payment or aid. Each entity should maintain or have access to a register of individuals or entities that are entitled to receive payments.

Before any payment is made it is essential that all necessary steps have been properly performed in compliance with the procedures in place.

Registration

Each entity must ensure that their claimants or suppliers are uniquely identified so that payments can be correctly made in a timely manner and debts and receipts can be effectively recovered.

Procedures and controls must be introduced for:

- The allocation of registration details so that the names, addresses, bank details and other relevant information is accurately recorded, based on adequate supporting proof of identity and entitlement to register;

- The registration identifier or number should be quoted and used during all correspondence, payments and accounting. It should be unique to the claimant.

- Where registration numbers are allocated, consideration should be given to the use of algorithms or check digits which can often detect the incorrect transposition of numbers or attempts to abuse systems. Responsibility for the maintenance of the register should be vested in a unit that is separate from the units, processing and authorising payments or the unit responsible for making payments; i.e. no employee should be able to register a claimant and then authorise or make a payment to that individual or entity.

- Changes to registration details such as names, addresses or bank accounts must be made under controlled conditions using adequate supporting proof for the change. Similar control procedures should be in place to cover de-registration procedures.

Employing electronic paying methods:

- There must be adequate control over access to bank accounts and associated equipment. Using passwords that are regularly changed,

- Samples of payments batched for electronic payment should be checked for existence and accuracy before electronic payments are made.
- Payments made by electronic means must be reconciled in a timely manner against the amounts authorised for issue.

- Additional external checks should be considered e.g. limit checks on the value of transactions over a period, individual item limits and restrictions on the types of accounts to which payments can be made.

- Wherever possible non-transferable payments should be made so that the payment is restricted to the recipient’s bank account. If a payment cannot be made by non-transferable means they should only be made to the intended recipient or an authorised legal representative. The identity and signature of the recipient should be confirmed,

- Entity should introduce procedures to ensure that any payments that are not transferred are re-credited back to the appropriate budget or fund after a defined period of time has elapsed.

Cash

As a principle, methods of payment and receipt involving cash should be avoided wherever possible. If payments are made in cash, they should be made only to the intended recipient or to a person or body legally nominated by the recipient. Wherever possible the entity should obtain evidence of identity and a signature attesting the receipt. Where payments are received in cash it is vital that:

- Any post containing cash or cash handed in is safeguarded and secured

- If cash is likely to be received, post should be opened promptly by staff under supervision or at least two staff working together

- Receipts are immediately recorded in a daily register;

- Records are checked against bank paying in records and statements and cash books by staff independent of those opening post and receiving cash

- There are regular and unannounced checks by management on the post opening and cash handling processes

- An acknowledgement of cash receipt should be provided to the person or body making the payment. This acknowledgement should made using official forms that are serially numbered

- Cash should be banked as soon as possible, there should be adequate security arrangements for the banking of cash

- Cash awaiting banking or that is retained for whatever reason should be secured in such a way as to prevent theft or misuse.

Advances, Payments and Guarantees

As a general principle, advance payments should be avoided wherever possible and should be made very much as an exception.

Where they are made consideration should be given to obtaining some form of security or guarantee in the event of the recipient failing to fulfil the agreement or going out of business.

If, in exceptional circumstances, an advance payment is considered as part of a procurement or contract, it is important that this facility was open to all potential suppliers.

Advance payments should be separately identifiable as such in the books of account. It should be possible to identify at any time the amounts of advances made. These advances should be cleared when the final payment is made.

The advances awaiting the final payment are regularly monitored to ensure that entitlement conditions are not abused or time limits not exceeded.

Procedures for the authorisation of advances should be consistent with those for normal payments, except where the need for guarantees is required. Guarantees should not be released until entitlement to the full payment is provided or the claimant has met the conditions of the advance payment.

Procedures for the approval of release of guarantees should be consistent with payment authorisation procedures, such as the financial levels of delegated authority involved. Entity should establish clear procedures regarding the types of guarantee that is acceptable and from which institutions. Guarantees should be safeguarded whilst in the custody of the entity.

Overpayments

The general principle to be adopted when an overpayment has been made is that the amount overpaid should be recovered from the recipient as soon as possible. Each entity should record overpayments as soon as they are discovered. The action taken on overpayments should be documented and monitored. Any proposal to write-off the overpayment should be defensible and follow proper procedures. Legal advice should be sought where necessary. Consideration should be given to setting-off overpayments and recovering the amount from any future claim or invoice from the recipient of the overpayment.

Debtors

Each entity should have access to a system to keep a debtors ledger. This ledger should be centralised wherever possible. All potential debts that may be due should be recognised in a timely manner and recorded on the ledger as quickly as possible. The amount should be calculated and authorised by the operational area responsible before a request to recover the debt is submitted to a separate unit or department that has no responsibility for payment or claims authorisation. An invoice should usually be raised and issued to the debtor, informing of the amount of the debt, the reason why the debt has occurred and giving a strict deadline within which the debt should be paid. Regular reconciliations should be performed between the amounts recorded in the ledger and supporting information. The amount to be recovered should be regularly reviewed and any additional amounts such as penalties or interest correctly identified and recalculated. Amounts paid to clear the debt should be recorded in the ledger in a timely manner. Any debts or overpayments that are set-off against subsequent payments to the debtor should also be recognised and recorded. Debts that are not paid within laid down time limits must be effectively identified, monitored and pursued. The ledger should be able to produce analysis reports of debts outstanding by individual debtor and by the age of the debt. Long outstanding amounts should be highlighted. This information should be regularly reviewed and when necessary the action taken. There should be a set of escalation procedures to deal with long outstanding debts, including the potential use of legal action.

Write-Off of Unrecoverable Amounts

Procedures should be established to write-off debts that are not recovered for whatever reason. As a basic principle debts should be pursued wherever it is practical or economic to do so. Any proposals for write-off action should be properly authorised at an appropriate level of authority. The reasons for write-off should be recorded together with any potential lessons learned or control procedures that need to be enhanced as a consequence. All write-offs should be recorded and identified against debt in the ledger in a timely manner once authorisation has been given.

Physical Controls and the Safeguarding of Assets

Adequate physical and environmental controls should be established to safeguard the entity's assets and information. The level and strength of a physical control should be commensurate with the risks involved, the impact the temporary or permanent loss of or loss of use of the asset or information would have on the entity and the likelihood of such a loss occurring. Typical physical controls could involve:

Access Controls may include:

- Guards
- CCTV Surveillance
- Alarm systems
- Perimeter fencing
- Secured barriers or gates
- Identity cards
- Computer passwords
- Secure areas within buildings where high value or high risk items are kept
- Safes and fireproof cabinets
- Fire and Flood prevention or suppression systems
- Continuous power supply and back up to key computerised and other facilities
- Maintenance controls over key assets
- Environmental controls such as thermostats to ensure that key assets remain in optimal condition

Physical Checks – Inventory

There should be regular physical checks to gain assurance that assets exist, are in the correct location and are being used for the intended purpose. All assets of value or importance should be recorded in an inventory or register. Ideally this register should be computerised. Wherever possible these assets should have a unique identifier which should be recorded in the register and be fixed to the asset in some way. The register should identify the location of the asset and the manager responsible for its safekeeping. Details of the assets should be recorded as close to receipt as possible. Ideally the register should be centrally held within the entity and there should be robust controls over the entries and removal of details relating to the asset.

Entity must develop procedures to update the register with details of new assets and have management controls and authorisation procedures for the removal of any assets from the register. Each authorisation should include the reason for removal. Particular attention should be given to assets removed because of disappearance, theft or misuse to ensure that any control weaknesses that resulted in this event are identified and rectified.

If assets are sold there should be a segregation of duties between those responsible for valuing the asset and those responsible for selling it. Any asset proposed for sale should be professionally valued.

There should be regular stock-checks against the inventory or register of assets to confirm the assets continued existence. These checks should be performed by the management responsible for the asset and/or by a body independent of that management such as the centralised body who maintains the register or a security officer or equivalent appointed for that purpose.

There should also be regular checks to ensure that physical controls are operating as intended or will operate if called upon to do so. These checks may involve, regular management review by the body responsible for an asset’s security, on-the-spot unannounced checks of the security of assets by a body independent of management such as a security officer or equivalent appointed for the purpose and regular testing of emergency controls to ensure that they will operate should such an emergency occur.

Details of all checks of the existence of assets and the operation of physical controls should be properly documented together with the results.

Information Systems Procedures

Entity should establish and maintain an set of Information Systems Procedures. The nature of this manual should be consistent with the degree of automation within the entity and the levels of risk associated with the loss of use of facilities and the potential impact the accidental or deliberate abuse of systems could have on the achievement of the entity’s objectives. Dependent upon the nature of systems within the entity the manual may cover:

- ✓ Strategic, entity, management and review procedures;
- ✓ Physical security
- ✓ Logical security
- ✓ Systems development and application controls
- ✓ Programming and maintenance
- ✓ Operations
- ✓ Telecommunications
- ✓ Personal computers, terminals and networks
- ✓ Contingency and disaster recovery planning

Public procurement (Annex 3b)

Entity should establish and maintain a set of Public Procurement Procedures establishing procedures and systems of procurement of goods, works or services in compliance with the procurement legislation. The procedures should be communicated to all relevant staff. The basic principles that entity should consider when performing public procurement are:

- ✓ There should be open competition unless there are compelling reasons not to;
- ✓ There should be a clear specification of the roles and responsibilities of employees involved in procurement, such as specifying requirements, giving financial authority and making commitments, together with the role of any specialist purchasing unit or department;
- ✓ There should be a separation of duties between those initiating a purchase and those authorising the placement of an order. In addition there should be a separation during the procurement process between staff who place orders, those who receive goods and those who authorise payments;
- ✓ Procurement should be based on value for money with regard to propriety. Value for money is the best combination of cost and quality that meet requirements.
- ✓ Requirements should be specified by users but there should be a predetermination of need for the goods, works or services before an exercise is started;
- ✓ Dealings with potential and actual suppliers should be conducted with honesty, impartiality and objectivity;
- ✓ Legal and specialist advice should be sought wherever necessary.

Transaction Processing

All transactions should be checked to ensure that they are complete, correctly recorded and accurately processed. In particular:
- ✓ Transactions should be recorded as close to their origin or point of receipt as possible
- ✓ Transactions should be checked at appropriate times in the processing cycle. In particular where an invoice or claim has been received there should be sufficient checks to ensure that:
- ✓ The goods or services have been ordered and provided against a contract or agreement. Ideally there should be a purchase order against which the invoice can be matched;
- ✓ A claim for aid entitlement fits the eligibility or regulatory criteria and is supported by adequate proof;
- ✓ The claimant and invoice/claim has been uniquely identified for payment and accounting purposes and to make sure that payments are only made to bona fide claimants who are registered to receive the specific entitlement
- ✓ The claim is arithmetically correct, including the correct rate of aid or currency conversion rate if applicable
- ✓ Regular checks should be performed by staff independent of those responsible for processing. These checks may include sequence checks, comparisons with documents, control totals and re-performance checks.

Authorisation

Entity should not commit any expenditure or make any payments until it has been properly authorised. Authorisation of payments involves the confirmation that:

- ✓ There is authority for the service to be ordered or a claim of entitlement to be made
- ✓ The creditor or claimant has entitlement to the payment

- ✓ The obligations that a creditor or claimant must perform have been undertaken or the service has been received
- ✓ The charge complies with contractual or aid requirements and the amount is arithmetically correct
- ✓ The expenditure has been charged to the correct item in the budget
- ✓ Budgetary funding is available and
- ✓ A payment has not already been made (e.g. double invoicing).

Authorisation systems should be established that are appropriate to the risks associated with the various types of payments that may be involved and the level of automation in the process. There will not be a single system that is appropriate to all circumstances but the entity should develop systems that take into account the following considerations and requirements:

- ✓ The need for absolute clarity in the roles and responsibilities at each stage of the process together with the need for detailed written procedures for receiving, recording and processing requests for payment;
- ✓ An adequate separation of duties so that no individual can control all aspects of the payment process;
- ✓ The need for regular scrutiny by more senior officials of the work of those officials responsible for authorisation;
- ✓ The need for authorising officers to have checklists that set out the checks that need to be conducted to confirm that a payment is valid and correct. The level and types of check that need to be performed will depend on the amount of automated checks that exist in the process.
- ✓ Each act of authorisation should be recorded. The authorising officer should sign each checklist/claim as authorised and/or make this attestation if authorisation is via an automated system.
- ✓ Where automated systems exist, particular regard should be given to the need for authorisation and separation of duties over the input of standing data into systems such as rates of aid/payment, currency conversion rates, or rates of interest, particularly where these may be variable or subject to regular change.
- ✓ There may be additional control procedures that need to be adopted for any payments that are made in advance of proof of entitlement or provision of service. For instance these payments may be subject to the provision of an adequate security or guarantee before a payment can be made.

Documentation and Audit Trails

Details of the information and transactions conducted should be properly documented and retained. Documentation may be held in paper, electronic or other formats that comply with national and other legislative requirements. This should help to ensure that:

- ✓ There is adequate support for activities;
- ✓ There is continuity of operations in the event of disruption or the loss of key personnel.
- ✓ Documentation must be maintained in good order so that it is easily retrievable when required and accessible to only those employees who have the required authority. Entity must develop suitable filing system. All relevant information should be placed and retained on a registered file that is uniquely identifiable as such and can be indexed and retrieved when needed. Files and documents should be classified in line with state

requirements. Entity must develop adequate procedures for the creation, retention and safekeeping of documents or files, dependent upon their classification.

- ✓ Financial and documentary control can be enhanced by the use of standard documentation and forms. These can also enforce conformity with procedures and legal requirements. Entity should ensure that forms used for financial transactions include appropriate legal declarations which claimants should attest and sign that they have read, are aware of and comply with.
- ✓ Forms and documents should be designed to be as simple to use and complete as is possible. There should be an appropriate balance between the needs of the person and body completing form and the needs of the entity that will process the form. Particular consideration should be given to the design of forms that will be used for data entry into computer systems so that the form is consistent with the layout and format of the computer input screen and vice versa.
- ✓ Documentation should enable employees, internal and external auditors and other review bodies to follow the course of operations and transactions at all stages. It should be possible to trace transactions from summarised totals down to the individual details and vice versa and to identify in records any errors, abuse or poor performance. This trail should exist and be maintained regardless of whether the underpinning systems are electronic or manual although logs may need to be established and maintained to trace action taken on transactions within electronic systems.
- ✓ Documents, files and financial records must be retained in a manner consistent with national and international document and data retention rules and requirements. These requirements may vary between and within entities so it is important that entities set out and communicate the documents and data retention requirements that are pertinent to their sector of activity and responsibility.

When determining the retention of records the following must be considered:

- ✓ The statutory requirements
- ✓ The requirements of audit bodies and external institutions
- ✓ The sensitivity and classification of the documents or data
- ✓ The potential impact on accommodation , space and computer data storage capacity
- ✓ The potential for use of archiving facilities
- ✓ The administrative ease of retrieving and using archived files or data if required
- ✓ The security of the records and data that is stored
- ✓ The potential for retention of records and data in more cost-effective forms of media –e.g. microfiche, scanned technology
- ✓ The potential cost and risks if original documents are not possible to retrieve or produce, for instance in the event of legal activity

6.4. Information and Communication

Management should establish adequate information systems and communicate relevant information to the appropriate personnel.

Information and communication relating to the organisation's performance will create the possibility to evaluate the orderliness, ethicality, economy, efficiency and effectiveness of operations.

Relevant information must be identified, captured and communicated in a form and timeframe that enable people to carry out their responsibilities.

Information systems produce reports, containing operational, financial and compliance-related information, that make it possible to run and control the business.

They deal not only with internally generated data, but also information about external events, activities and conditions necessary to informed business decision-making and external reporting.

Effective communication also must occur in a broader sense, flowing down, across and up the organisation. All personnel must receive a clear message from top management that control responsibilities must be taken seriously.

They must understand their own role in the internal control system, as well as how individual activities relate to the work of others. They must have a means of communicating significant information upstream.

There also needs to be effective communication with external parties, such as customers, suppliers and regulators.

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

Information

A precondition for reliable and relevant information is the prompt recording and proper classification of transactions and events.

Pertinent information should be identified, captured and communicated in a form and timeframe that enables staff to carry out their internal control and other responsibilities (timely communication to the right people). Therefore, the internal control system as such and all transactions and significant events should be fully documented.

For example, one of the objectives of internal control is fulfilling public accountability obligations. This can be achieved by developing and maintaining reliable and relevant financial and non-financial information and communicating this information in annual reports.

In many cases, certain information has to be provided or communication has to take place in order to comply with laws and regulations.

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

Transactions and events must be recorded promptly when they occur if information is to remain relevant and valuable to management in controlling operations and making decisions. This applies to the entire process or life cycle of a transaction or event, including the initiation and authorisation, all stages while in process, and its final classification in summary records.

It also applies to promptly updating all documentation to keep it relevant.

Proper classification of transactions and events is also required to ensure that reliable information is available to management. This means organising, categorising, and formatting information from which reports, schedules, and financial statements are prepared.

Information systems produce reports that contain operational, financial and non-financial, and compliance-related information, and that make it possible to run and control the operation. The systems deal not only with quantitative and qualitative forms of internally generated data, but also with information about external events, activities and conditions necessary for informed decision-making and reporting.

Management's ability to make appropriate decisions is affected by the quality of information which implies that the information is:

- appropriate (is the required information there?);
- timely (is it there when required?);
- current (is it the latest available?);
- accurate (is it correct?);
- accessible (can it be obtained easily by the relevant parties?).

In order to help ensure the quality of information and reporting, carryout the internal control activities and responsibilities, and make monitoring more effective and efficient, the internal control system as such and all transactions and significant events should be fully and clearly documented(e.g. flow charts and narratives). This documentation should be readily available for examination.

Documentation of the internal control system should include identification of an organisation's structure and policies and its operating categories and related objectives and control procedures.

An organisation must have written evidence of the components of the internal control process, including its objectives and control activities.

The extent of the documentation of an entity's internal control varies however with the entity's size, complexity and similar factors.

Communication

Information is a basis for communication, which must meet the expectations of groups and individuals, enabling them to carry out their responsibilities effectively.

One of the most critical communications channels is that between management and its staff. Management must be kept up to date on performance, developments, risks and the functioning of internal control, and other relevant events and issues.

By the same token, management should communicate to its staff what information it needs and provide feedback and direction. Management should also provide specific and directed communication addressing behavioural expectations.

This includes a clear statement of the entity's internal control philosophy and approach, and delegation of authority.

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

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

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

Performance Monitoring and Management Information

Head of the entity and the management at all levels must set up or assure an information system that gives clear, accurate and timely information on the likely achievement of key objectives. This information should include any corrective activities that are deemed necessary.

Performance monitoring and management information may take the form of:

- ✓ Statistics;
- ✓ Budgetary expenditure reports
- ✓ Staffing and headcount reports
- ✓ Unit cost, productivity and value for money analysis
- ✓ Accounting information, including debt management information
- ✓ Data analysis
- ✓ Key performance indicators
- ✓ Reports, for example security incidents, asset inventory check reports.

Management information should be regularly reviewed to ensure that it remains relevant to needs and is being used as intended.

Fraud and Irregularity

Procedures to deal with fraud and irregularity should be consistent with the relevant legislation. The head of the entity should develop a fraud policy statement which is communicated to all employees and, where necessary outside the entity. This statement should clearly promote an anti-fraud culture and commitment to ethical behaviour. Employees should be encouraged or obliged to report any suspicion of fraudulent activity they may have,

The fraud policy should be supported by a fraud response plan, which should set out the action to be taken in the event that a fraud or potential fraud is discovered. The action required should be timely and effective to try and ensure that potential losses are minimised and the chances of a successful investigation are increased. The plan may need to distinguish between frauds perpetrated within the entity, by external parties or where there is collusion between internal and external parties.

The plan should set out the scope and limitations of the powers of officials to act if a potential fraud is discovered. It should also identify the state bodies that should be contacted or involved.

Should a fraud be perpetrated, entity should conduct an analysis of the reasons why the fraud took place, examine whether there are any other similar cases and should make any necessary changes in systems and procedures to prevent frauds of a similar nature taking place in the futures

Corrective Action

The head of the entity must adopt formal procedures for all managers and staff that set out their responsibility to report any weaknesses in financial management and control systems to more senior managers or to the FMC Manager and to deal with complaints and queries from customers or other bodies to ensure that any issues that may relate to weaknesses in the systems of financial management and control are addressed and rectified.

6.5. Monitoring

The purpose of monitoring is to determine whether internal control is adequately designed, properly executed, and effective. Internal control is adequately designed and properly executed if all five internal control components (Control Environment, Risk Assessment, Control Activities, Information and Communication, and Monitoring) are present and functioning as designed.

Internal control systems need to be monitored--a process that assesses the quality of the system's performance over time. This is accomplished through ongoing monitoring activities, separate evaluations or a combination of the two.

Ongoing monitoring occurs in the course of operations. It includes regular management and supervisory activities, and other actions personnel take in performing their duties.

The scope and frequency of separate evaluations will depend primarily on an assessment of risks and the effectiveness of ongoing monitoring procedures. Internal control deficiencies should be reported upstream, with serious matters reported to top management and the board.

It is here that Internal Audit has an important role to play. They should perform audits on systems that are identified as priorities based on a risk assessment.

Types of Monitoring

- ✓ Regular review of the risk register with reference to changes of objectives, internal and external environment – The internal act on setting up and keeping the risk register should provide for regular review by the head of the entity. As the risk register reflects the systematic approach to risk management any changes in internal and external environment and objectives can give reason for undertaking the commensurate measures addressing changes in risks. The head of the entity is responsible for the achievement of objectives; he sets the acceptable risk and adopts the appropriate measures for control.

- ✓ The internal system of information and communication should provide the head of the entity with regular and ongoing information in written or oral form regarding the objectives achievement thus enabling him to timely react and take the corrective measures.

- ✓ Self assessment questionnaires can be used and they are usually prepared by the head and senior employees of the entity. The problem is that they only take place once a year and by the time the controls may have weakened. Also the results may not truly reflect the circumstances as managers may not be objective in their reply.

- ✓ Interviews with employees can reveal weaknesses of internal control and provide suggestions on possible improvements. This kind of involvement of employees as crucial component of internal control cannot be overemphasised.

- ✓ Other forms of monitoring are on going on the spot checks, control of check lists and other evidence of performed internal control, comparison of different data bases, benchmarking in form of comparing performance with other entities, etc.

- ✓ Head of the entity should receive reports of noncompliance with established rules and reports on irregularities.

A specific form of monitoring is provided to the head of the entity by the internal auditor who in respect of his integrity and using the professional guidance assesses according to his risk analysis the effectiveness of internal controls; to identify weaknesses and to provide recommendations for improvement.

The head of the entity should:

- Meet with internal auditor to discuss and endorse his annual audit plan,
- Read and agree audit reports and
- Address all worthwhile recommendations.

7. Internal Control Review

Introduction

In 2008 Montenegro adopted the Public Internal Financial Control (PIFC) Law which provides general guidance and explanations on the requirements of putting in place an adequate system of financial management and control and establishing an independent and functional internal audit service.

Financial management and control (FMC) is the most important area of internal control as it affects all activities of the organisation. In public financial management great attention is paid to the concept and activity of financial control. All managers have a duty and obligation for financial control to ensure the best use of resources and to minimise loss, waste, and mis-use of assets, fraud and corruption.

There is no doubt that Montenegro already has a reasonable level of financial control operating in public sector organisations in accordance with the Budget Law and Directions on State Treasury Operations.

The adoption of the PIFC Law and the FMC Rulebook is recognition by Montenegro that change is required so that ministries take greater control in managing their financial matters by increasing decentralisation, improving the managerial accountability and establishing internal audit to review their system of financial control

Efficient public financial management is important in creating trust, transparency and a shared consensus between government and citizens.

As a start in this development of a FMC Framework each organisation should prepare a FMC Internal Rules and Procedures that includes detailed procedures in separate chapters for all their main financial matters. This Internal Rules and Procedures will be a working document that should be regularly updated to meet the needs of the organisation.

To achieve effective financial management and control in the public sector it is essential that organisations concentrate on developing the following key areas of financial management:

1 Financial Regulations;

2 Financial Planning;

3 Financial Monitoring and Review;

4 Financial Control

5 Financial Information;

Current Status of FMC

In order to improve the system of FMC and in accordance with Article 4 of the FMC Rulebook there is a need to assess the current status of FMC. The results of the review will identify weaknesses that need addressed in order to upgrade their FMC Framework to be more appropriate and aligned to the best practice in EU countries. In accordance with Article 6 of the FMC Rulebook they should prepare an Action Plan that will provide a basis for change and should identify the key tasks to be addressed.

To identify the current status of Financial Management and Control (FMC) requires that each organisation performs a self assessment of the FMC process within the organisation in the form of an Internal Control Review (ICR). The Public Internal Financial Control (PIFC) Law 73/08 provides more information about the need for Financial Management and Control. The PIFC Law - Articles 11, 13 and 15 explains that the Head of Entity shall be accountable for monitoring, assessing and reporting on the financial management and control system.

The ICR is to identify if the organisation has an adequate FMC framework with financial procedures and policies to ensure they are functioning as intended and that they assist the organisation in meeting its goals and objectives. Examples of financial procedures and policies that should exist include financial planning activities, asset management, the budget preparation and execution, payroll transactions, payment transactions, accounting information systems, cash activities, financial reporting and monitoring, and capital programs. All of these procedures and the framework for FMC should be developed in the form of an internal FMC Internal Rules and Procedures.

Upon completion of the ICR, a report should be produced that provides the results of the ICR. The report should include a list of recommendations and action plan to address any weaknesses that are discovered. The recommendations will require the preparation of an FMC Internal Rules and Procedures that includes the various financial procedures that cover all financial matters in the organisation. If recommendations are accepted, a set of deadlines for should be agreed along with the allocation of responsibility.

The results of the review will also form the basis of the annual report (self assessment questionnaire) required by the PIFC Law – Article 15. By the end of January each organisation must report to CHU on activities related to the establishment and development of financial management and control.

This approach is only a guide and may be modified as necessary to meet the unique characteristics, circumstances and requirements of an organisation.

Each organisation should develop its own FMC Internal Rules and Procedures to include the policies, procedures and guidelines contained herein. ***There is no a standard model of internal control so it is the task of each organisation to decide what is appropriate for them.***

The FMC Internal Rules and Procedures should include specific information reflecting the degree of commitment the organisation, such as the formation of a working group, the appointment of a FMC Manager, a list of the main financial systems and processes, procedures for all financial processes, final reporting, financial monitoring and review.

Once Internal Audit is functional the FMC Internal Rules and Procedures can include the audit process that will be used to evaluate the weaknesses and effectiveness of internal controls.

Internal controls are already part of our daily operations. The controls developed and exercised by managers and their staff are the substance of internal control. Procedures help to ensure that the controls are properly documented and that they are functioning as intended.

The goal is not to make each person an expert in internal controls, but to increase the awareness and understanding of internal controls. In fact, the single most important success factor in Internal Control is a high level of individual awareness and understanding. Internal controls are everyone's responsibility. Therefore, it is critical that each manager is able to identify the internal controls that exist in their section. All managers are responsible for knowing what internal controls exist and how to evaluate their effectiveness.

A successful Internal Control System will help to streamline the financial processes and improve the level and quality of our services.

Objective – Assess the Current Status of the Financial Management and Control System

The recommended general approach to the ICR includes the following five main steps:

1. Organise the ICR.
2. Decide the Scope of the Review
3. Prepare Checklists for the Review
4. Perform the Review
5. Prepare report with results and recommendations with corrective actions.

The report will provide each organisation with an assessment of the current status of their FMC system and should allow them to prepare an improvement plan to address any weaknesses in their FMC system.

This assessment will also allow each organisation to inform the CHU about the progress made in implementing a sound FMC Framework which is a requirement as per Article 15 of the PIFC Law.

The appointment of Internal Audit will then allow regular monitoring and evaluation of the internal control system.

Step 1 - Organise the Internal Control Review

It is necessary to appoint someone to manage the ICR- probably the FMC Manager and then select key two or three staff to perform the review.

The objective of the review is simply to identify the current status of FMC and IA in regard to what is required for PIFC. This is expected to take place each year in December and should take no longer than five days to perform and then produce a report.

It is expected that every organisation would eventually have a fully documented FMC Framework in the form of a FMC Internal Rules and Procedures that is a live and working document that informs all staff about the FMC process in the organisation

Step 2 – Decide the Scope of the Review

There is a need to identify the scope of the review that needs to be assessed. This will require a checklist of activities to be prepared to assess what is the current situation for FMC. The recommendation for the scope of the first review is that all organisations consider the only two matters for their first review:

1 **Area and Scope of Financial Matters within the Ministry.**
2 **Control Environment – COSO Model**

In future it is recommended that reviews are more detailed in regard to the specific financial processes, financial reporting, risk management, financial monitoring and review.

Step 3 - Prepare Checklists for the Review

The checklists should include a series of activities for the 2 sections mentioned in Step 2. The checklists should have a choice for 5 levels of answers.

For example for section 1- Area and Scope of Financial Matters within the Ministry -

List the financial matters that relate to your organisation- for example -budget preparation and execution, revenue collection, payroll, payments and determine if adequate controls exist for each of these systems. Try and be objective and ensure that there is evidence to support your assessment.

As a guide the main systems/processes as per The Treasury Directions are as follows and they are the areas that should be reviewed:

1. Budget Execution;
2. Financial Control- Payments, Receipt of Goods and Commitments
3. Accounting and Expenditure Control;
4. Collection of Public Revenue;
5. Cash Security;
6. Irregularities;

7. Banking;
8. Payroll - Salaries;
9. Borrowing- Debt and Loans
10. Financial Records;
11. Advances;
12. Donor Funded Programs.

The above list covers all the main financial processes that a line ministry must address for applying internal controls to minimise the risk of loss, waste and mismanagement.

A checklist should be prepared to assess the extent of FMC and as a guide should include the following 5 questions which must be supported by evidence:

1 Is there a set of written procedures for all financial matters managed by the Ministry?
2 Do staff have adequate training for each financial activity?
3 Does the organisation have a management team who manage the budget and planning process?
4 Is financial reporting adequate to manage and control the budget execution process?
5 Does financial monitoring and review take place on a regular basis to ensure that the senior staff are aware of the current financial situation?

This list is only a guide and should be the minimum as a starting point which should be increased as required.

If the answer is no or insufficient to satisfy the Minister then this is an area of weakness that must be improved. There must always be evidence to support any answer of yes.

Checklist 1- Area and Scope of Financial Matters within the Ministry

Consider the financial matters that relate to your organisation- for example -budget preparation and execution, revenue collection, payroll, payments and determine if adequate controls exist for each of these systems. Try and be objective and ensure that there is evidence to support your assessment.

a) Is there a set of written procedures for all financial matters managed by the Ministry?

- *YES, on all financial matters,* ☐
- *YES, on most financial matters,* ☐
- *YES, on some financial matters,* ☐
- *NO, but the activities are started,* ☐
- *NO.* ☐

Comment:...
....

b) Do staff have adequate training for each financial matter?

- *YES, on all financial matters,*
- *YES, on most financial matters,*
- *YES, on some financial matters,*
- *NO, but the activities are started,*
- *NO.*

Comment:..
....

c) Does the organisation have a management team who manage the budget and planning process? Give an assessment

- *YES, with staff from all operational areas,*
- *YES, with staff from most operational areas*
- *YES, with staff from some operational areas*
- *NO, Finance staff only*
- *NO. Minister only*

Comment:..
....

d) Is financial reporting adequate to manage and control the budget execution process?

YES, for all operational areas,
- *YES, for most operational areas*
- *YES, for some operational areas*
- *NO, Finance staff only*
- *NO. Minister only*

Comment:..
....

e) Does financial monitoring and review take place on a regular basis to ensure that the senior staff are aware of the current financial situation?

YES, for all operational areas,
- *YES, for most operational areas*
- *YES, for some operational areas*
- *NO, Finance staff only*
- *NO. Minister only*

Comment:..
....

Checklist 2 – Control Environment

A questionnaire based on the COSO Model is prepared by the CHU which should be used for this assessment. See Annexes 1a and 1b for the questionnaire and instructions. Note that this may be changed by the CHU in the Ministry of Finance.

Step 4 - Perform review

Using the checklists, perform the review and answer each of the questions objectively. Remember that there must be evidence such as a set of procedures if the answer is yes.

Step 5 - Prepare report with results and recommendations with corrective actions.

A report should be prepared which not only identifies the weaknesses, but also provides recommendations on how to correct them.

The recommendations should be considered by management, and a decision should be made them to prioritise on what has to be done, when and by whom. In any case, approved corrective actions should be initiated as promptly as possible.

An Action Plan should be prepared to list and track the weaknesses identified; identify the priorities and list the actions taken. This system should identify responsible personnel and target dates. Last but not least the action plans should be monitored on a regular basis in order to ensure their timely implementation.

Management reports should be prepared on a regular basis to apprise senior organisation management of the status of the internal control program. These reports should include such topics as: areas with nonexistent or inadequate control techniques, areas with controls that are not functioning properly, and areas where excessive controls exist, as well as the plans and schedules for addressing the identified concerns.

An Annual report on FMC implementation should be prepared by the organisations and delivered to the CHU. Overall, the report should reflect the design and functioning of the internal control system, as well as the actions undertaken with a view to address corrective measures that are needed for the purposes of strengthening the FMC system.

The CHU should use these reports to

- Assess the overall state of FMC;
- Focus on problems and assist organisations to improve their position;
- Consider the need for issuing new overall guidance;
- Report to the Government through the Minister of Finance.

Internal Audit

Good internal controls have no impact unless they are followed in practice. A testing programme provides the assurance that functions operate as intended. An effective testing programme does not have to be onerous, and eventually internal audit will conduct audits of the main financial systems. These audit programmes should be adequate enough to inform managers whether procedures are being followed and controls are working as intended. Periodic testing of internal controls should be performed on all areas identified in the risk assessment process as high risks.

An effective audit programme consists of the following:

- Identification of the main financial processes to be tested and
- Identification of the key control objectives and key controls for that process
- Determination of standards that apply to the function and expectations for performance.
- Development of a testing plan.

Then with the programme agreed the auditor should

- Assess the system.
- Conduct the test.
- Prepare a report with recommendations
- Discuss findings
- Review progress

d---d

Glossary of Definitions

Used by the European Commission in the framework of Public Internal Financial Control (PIFC)

Version of November 11, 2005

Acknowledgement

(DG BUDG.D.6 has developed this glossary in co-operation with DG ELARG)

Term	Definition
Accounting Control System	A series of actions, which are part of the total internal control, system concerned with realising the accounting goals of the entity. This includes compliance with accounting and financial policies and procedures, safeguarding the entity's resources and preparing reliable financial reports.
Administrative Control System	A series of actions, which are part of the internal control system, concerned with administrative procedures needed to make managerial decisions, realise the highest possible economic and administrative efficiency and ensure the implementation of administrative policies, whether related to financial affairs or otherwise.
Audit	In its most generic sense this can mean any examination ex-post of a transaction, procedure or report with a view to verifying any aspect of it – its accuracy, its efficiency, etc. The word usually needs to be qualified more narrowly to be useful.
Audit Evidence	Information, which supports the opinions, conclusions or reports of the auditors, internal audit services or SAI. It should be: Competent: information that is quantitatively sufficient and appropriate to achieve the auditing results; and is qualitatively impartial such as to inspire confidence and reliability. Relevant: information that is pertinent to the audit objectives. Reasonable: information that is economical in that the cost of gathering it is commensurate with the result, which the auditor or, the internal audit service or the SAI is trying to achieve.
Audit Mandate	The auditing responsibilities, powers, discretion and duties conferred on any audit body (e.g. the SAI under the constitution or other lawful authority of a country (as set out in primary or secondary national legislation).

Audit Objective	A precise statement of what the audit intends to accomplish and/or the question the audit will answer. This may include financial, regularity or performance issues.
Audit Procedures	Tests, instructions and details included in the audit programme to be carried out systematically and reasonably.
Audit Scope	The framework or limits and subjects of the audit.
Audit Trail	The phrase has a rather imprecise general meaning in general audit usage. However, annex 1 of Council Regulation 2064/97 has provided a specific detailed description of the requirements of 'a sufficient audit trail' for the purposes of the structural funds managed by the Member States on behalf of the Commission. In brief summary it requires the maintenance of records giving the full documentation and justification at all stages of the life of a transaction together with the ability to trace transactions from summarised totals down to the individual details and vice versa. The overriding objective of the audit trail is to ensure a 'satisfactory audit from the summary amounts certified to the Commission to the individual expenditure items and the supporting documents at the final beneficiary'. The word "audit trail" in the Regular Reports and the Accession Partnerships is to be understood in the light of the above definition which should be applied in the context of all Pre-Accession Funds to Candidate Countries.
Audited Entity	The organisation, programme, activity or functions subject to audit by the SAI or the (internal) audit service.
Auditing Standards	Auditing standards provide minimum guidance for the auditor that helps determine the extent of audit steps and procedures that should be applied to fulfil the audit objective. They are the criteria or yardsticks against which the quality of the audit results are evaluated.
Charter (Internal Audit Charter)	Also called Internal Audit Mission Statement, especially in non-US (-linked) organisations. The Charter/Mission Statement of the internal audit activity is a formal, written document that defines the internal audit activity's purpose, scope, and responsibility. It aims to ensure that the internal audit is looked upon with trust, confidence and credibility. The charter should: Ensure the functional independence including specification of the position of the internal audit activity within the organisation; Permit unrestricted access to records, personnel, and physical properties relevant to the performance of engagements; Define the scope of internal audit activities; Define reporting requirements to auditees and, where necessary, to judiciary institutions and State the relationship with the State Audit Office.
Compliance Audits	See Regularity Audits.

Constitutional	A matter which is permitted or authorised by, the constitution of fundamental law of a country.
Controls	Any kind of control on an organisation or beneficiaries of public funds, both internal and external controls on an organisation – i.e. both internal controls and controls from outside the organisation.
Due Care	The appropriate element of care and skill which a trained auditor would be expected to apply having regard to the complexity of the audit task, including careful attention to planning, gathering and evaluating evidence, and forming opinions, conclusions and making recommendations.
Economy	Minimising the cost of resources used to achieve given planned outputs or outcomes of an activity (including having regard to the appropriate quality of such outputs or outcomes).
Effectiveness	The extent to which objectives of an activity are achieved i.e. the relationship between the planned impact and the actual impact of an activity.
Efficiency	Maximising the outputs or outcomes of an activity relative to the given inputs.
Evaluation	Can mean a) The evaluation of tenders as part of the contracting process; or b) Specific reviews designed to examine the overall performance of a programme or project. Its scope may vary. Its core should be setting out, obtaining or calculating the outcomes of the programme or project and considering their economy, effectiveness and efficiency, but it usually covers a much wider range of issues including the appropriateness and achievement of output objectives as well. It may be carried out before, during or after the programme or project has been completed (usually known as ex-ante, mid-term or ex-post). It shares many characteristics with performance audit.
Ex ante financial control (EAFC)	Ex ante financial control (EAFC) is the set of control activities prior to carrying out financial decisions relating to appropriations, commitments, tender procedures, contracts (secondary commitments), and related disbursements and recovery of unduly paid amounts. Such decisions can only be made on the basis of the explicit approval of the ex ante financial controller. EAFC is sometimes also called "preventive control". This is the narrower meaning of financial control. If described as EAFC there can be no ambiguity.
Ex post internal audit (EPIA)	The set of audit activities that take place ex-post. I.e. in this context, after financial decisions have been made by the management. EPIA can be carried out by centralised government audit bodies, responsible and reporting to the highest levels of government (Ministry of Finance or even the Cabinet of Ministers) or decentralised audit bodies (Internal Audit Units in government budget implementation spending units, like Ministries or Agencies).
Ex-post	When referring to audit, "ex post" usually means an audit performed after the initial legal commitment of a transaction. When referring to evaluation, "ex post" usually means an evaluation performed after

	the transaction has been fully completed.
External audit	Any audit carried out by an auditor who is independent of the management being audited. In public finance, it means audit external to the Government financial management and control policy is carried out by the national Courts of Auditors (or similar institutions) Supreme Audit Office to objectively ensure that such management and control systems are compliant with the definition of PIFC as mentioned elsewhere in this glossary above.
Field Standards	The framework for the auditor to systematically fulfil the audit objective, including a) planning and supervision of the audit, b) gathering of audit evidence which is competent, relevant and reasonable, and c) an appropriate study and evaluation of internal controls.
Financial Audits	Cover the examination and reporting on financial statements and examine the accounting statements upon which those statements are based.
Financial controller	The function of the financial controller may mean different things in different organisations e.g.;. a) the role which gives ex-ante approval to individual transactions that they are in conformity with regulations and procedures; or. b) the same as auditor; or. c) the management role which combines responsibility for the recording and processing of transactions (financial accounting) with the preparation of and reporting against budget targets (management accounting). In the Commission, Financial Control was originally (1973) defined as ex ante approval of any kind of financial decisions, later the internal audit function was added to the functions of the Finance Controller. Recently the trend is to split the two functions and the term "financial control" refers again only to ex ante approval. In the framework of Enlargement the term is used for the ex ante approval function.
Financial controls	The phrase has a wide meaning in some organisations and a narrow meaning in others (very broadly, organisations from further North take the wider meaning and those from further South take the narrower meaning). The wide meaning follows the meaning of internal controls except that it refers to controls, which have a specific financial component. In practice, in this context, there are few controls, which do not have a financial component and the phrase financial control can often be virtually interchangeable with internal control. The narrower meaning follows the narrower meaning of financial controller and refers to the specific review of the conformity of transactions with regulations and procedures described in ex-ante financial control.
Financial management (FM)	In the framework of Enlargement the term is understood to be the set of responsibilities of the management (which is responsible for carrying out the tasks of government budget handling units) to establish and implement a set of rules aiming at an efficient, effective and economic use of available funds (comprising income,

	expenditure and assets). It refers to planning, budgeting, accounting, reporting and some form of ex ante financial control. FM is subject to internal and external audit.
Financial Systems	The procedures for preparing, recording and reporting reliable information concerning financial transactions.
Findings, Conclusions and Recommendations	Findings are the specific evidence gathered by the auditor to satisfy the audit objectives; conclusions are statements deduced by the auditor from those findings; recommendations are courses of action suggested by the auditor relating to the audit objectives.
Functional Independence (FI)	The special status of a financial controller (narrow sense) or an internal auditor (whether central or decentralised), providing him/her with the power of maintaining a free professional judgement vis-à-vis his superior of the organisation in matters of control and audit. This concept requires the maintenance of a balance between those who are responsible for managing the organisation and those who are controlling/auditing the organisation. FI should be embodied in relevant legislation. Another way to ensure FI is to have the central control/audit organisation nominate a delegate Internal Auditor into the organisation to be audited or to allow the Internal Auditor (in case of conflict of interests) to report his findings freely to the central audit body.
Fundamental	A matter becomes fundamental (sufficiently material) rather than material when its impact on the financial statements is so great as to render them misleading as a whole. See also Significant Control Weakness.
General Standards	The qualifications and competence, the necessary independence and objectivity, and the exercise of due care, which shall be required of the auditor to carry out the tasks related to the fields and reporting standards in a competent, efficient and effective manner.
Impact	The same as result or outcome.
Independence	For an external audit it means the freedom of the national Courts of Auditors or similar institutions in auditing matters to act in accordance with its audit mandate without external direction or interference of any kind. From an internal audit viewpoint it means that the internal audit service should be organised directly under the top management. Nevertheless, the internal audit service should be free to audit any area that it considers to be an area of risk for material errors, even when management might not think so. (see also functional independence)
Internal Audit	The Institute of Internal Auditors definition is: Internal audit is an independent, objective assurance and consulting activity designed to add value and improve an organisation's operations. It helps an organisation accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes. More concretely, it is the functional means by which the managers

	of an entity receive an assurance from internal sources (including internally subcontracted sources) that the internal controls are achieving their internal control objectives. It will cover, inter alia, Financial Audits, System Based Audits, Performance Audits, IT-Audits It has most of the characteristics of external audit except that it finally reports to the management and therefore can never have the same level of independence as external audit. In public finance a distinction is made between centralised internal audit and decentralised internal audit as follows:
Centralised internal audit (CIA)	CIA is public ex post internal audit performed by a centralised body (e.g. the Ministry of Finance or another Internal Audit body (like the Government Control Office in Hungary or the Internal Audit Board in Malta)) on systems.
Decentralised internal audit (DIA)	DIA is the internal audit performed by specialised Internal Audit Units located inside government or lower public budget implementation spending centres (Ministries or Agencies).
Internal Auditor (IA)	The Internal Auditor (IA) (whether located outside or inside the organisation of the Managing Director) is responsible for carrying out all relevant kinds of ex post internal audit. In public finance terms, the IA should be subject to a special "statute" (preferably written in the Internal Audit Law governing the PIFC-system in a given country) allowing him an adequate degree of functional independence. The IA can report to the MD or be assigned by a central Public Internal Audit Service, like the Ministry of Finance or an Internal Audit Board responsible to the Prime Minister of the Cabinet of Ministers.
Internal Control	The whole system of financial and other controls, including the organisational structure, methods, procedures and internal audit, established by management within its corporate goals, to assist in conducting the business of the audited entity in a regular, economic, efficient and effective manner. Internal control covers the totality of the policies and procedures conceived and put in place by an entity's management to ensure the economic, efficient and effective achievement of the entity's objectives; the adherence to external rules and to management policies and regulations; the safeguarding of assets and information; the prevention and detection of fraud and error, and the quality of accounting records and the timely production of reliable financial and management information. Internal control relate to the following categories: Control environment; Risk assessment; Information and Communication; Control activities and Monitoring of controls.
Internal Control Objective	The primary objectives of internal control are to ensure: The reliability and integrity of information. Compliance with policies, plans, procedures, laws, and regulations. The safeguarding of assets. The economical, efficient and effective use of resources.

	Each organisation should design its own system of internal control to meet the needs and environment of the organisation.
International Organisation of Supreme Audit Institutions (INTOSAI)	An international and independent body which aims at promoting the exchange of ideas and experience between Supreme Audit Institutions in the sphere of public financial control.
IT systems audits	Examine the sufficiency and adequacy of the protection of the security of the systems of IT applications in order to guarantee the confidentiality, integrity and availability of information and IT systems.
Managerial Accountability	Represents the obligation to be accountable for a given task. Accountability covers issues like separation of duties (authorising officer, accountant, ex ante financial controller); development of Financial Management and Control manuals, powers, responsibilities, reporting and risk management), all financial transactions (commitments, contracts, disbursements, recovery of unduly paid amounts), links with the central harmonisation facilities, and evaluation and reporting on F/C systems .
Management control	Control by management: the same as internal control, including financial control.
Materiality and Significance (Material)	In general terms, a matter may be judged material if knowledge of it would be likely to influence the user of the financial statements or the performance audit report. Materiality is often considered in terms of value but the inherent nature or characteristics of an item or group of items may also render a matter material - for example, where the law or some other regulation requires it to be disclosed separately regardless of the amount involved. In addition to materiality by value and by nature, a matter may be material because of the context in which it occurs. For example, considering an item in relation to the overall view given by the accounts, the total of which it forms a part; associated terms; the corresponding amount in previous years. Audit evidence plays an important part in the auditor's decision concerning the selection of issues and areas for audit and the nature, timing and extent of audit tests and procedures.
Mission Statement	See Charter (Internal audit Charter).
Opinion	The auditor's written conclusions on a set of financial statements as the result of a financial or regularity audit.
Outcomes	The effects of a programme or project measured at the highest meaningful level in proportion to the programme or project (e.g. jobs created). In practice there are always at least some external non-controllable elements, which influence whether outcomes are achieved or not. The same as results or impacts.
Outputs	The directly tangible deliverables of a programme or project insofar as they are, for practical purposes, completely under the control of the implementers of the project (e.g. training seminar executed).
Performance Audit	An audit of the economy, efficiency and effectiveness with which

	the audited entity uses its resources in carrying out its responsibilities. In practice there can be difficulty distinguishing Performance Audit from Evaluation. Sometimes Performance Audits are limited to consideration of outputs but this considerably limits the value of the audit. Also Evaluation may create data, particularly on outcomes, whilst Performance Audit would usually be limited to a review of data which was available (and if necessary identification of missing data) Performance Audit is usually concerned with testing performance against some given standards.
Planning	Defining the objectives, setting policies and determining the nature, scope, extent and timing of the procedures and tests needed to achieve the objectives.
Postulates	Basic assumptions, consistent premises, logical principles and requirements which represent the general framework for developing auditing standards.
Public Accountability	The obligations of persons or entities, including public enterprises and corporations, entrusted with public resources to be answerable for the fiscal, managerial and programme responsibilities that have been conferred on them, and to report to those that have conferred these responsibilities on them.
Public Internal Financial Control (PIFC)	PIFC is the overall financial control system performed internally by a Government or by its delegated organisations, aiming to ensure that the financial management and control of its national budget spending centres (including foreign funds) complies to the relevant legislation, budget descriptions, and the principles of sound financial management, transparency, efficiency, effectiveness and economy. PIFC comprises all measures to control all government income, expenditure, assets and liabilities. It represents the wide sense of internal control. It includes but is not limited to ex ante financial control (EAFC) and ex-post internal audit (EPIA).
Reasonable Assurance	Internal control, no matter how well designed and operated, can provide only reasonable assurance to management regarding the achievement of an entity's objectives. The likelihood of achievement is affected by limitations inherent in all internal control systems. These limitations may include faulty decision-making with respect to the establishment or design of controls, the need to consider costs as well as benefits, management override, the defeat of controls through collusion, and simple errors and mistakes. Additionally, controls can be circumvented by collusion of two or more people. Finally, management may be able to override elements of the internal control system. Reasonable assurance is provided when cost-effective actions are taken to restrict deviations to a tolerable level. This implies, for example, that material errors and improper or illegal acts will be prevented or detected and corrected within a timely period by employees in the normal course of performing their assigned duties. Management during the design of systems considers the cost-benefit relationship. The potential loss associated with any risk is weighed against the cost to control it.

Regularity Audit	Attestation of financial accountability of accountable entities, involving examination and evaluation of financial records and expression of opinions on financial statements; attestation of financial accountability of the government administration as a whole; audit of financial systems and transactions, including an evaluation of compliance with applicable statutes and regulations; audit of internal control and internal audit functions; audit of the probity and propriety of administrative decisions taken within the audited entity ; and reporting of any other matters arising from or relating to the audit that the SAI considers should be disclosed. This is normally not applicable to Internal Audit Services.
Report	The auditor's written opinion and other remarks on a set of financial statements as the result of a financial or regularity audit or the auditor's findings on completion of a performance audit.
Reporting Standards	The framework for the auditor to report the results of the audit, including guidance on the form and content of the auditor's report.
Results	The same as outcomes or impacts.
Risk	An event which can result in an undesirable or negative outcome. It is characterised by the probability or likelihood of the event occurring and the resulting impact or consequence if it does occur. These two factors combine to result in a level of risk exposure.
Risk assessment	Auditor's tool to help identifying audit projects offering the highest added value to the organisation. Risk assessment is the identification of all local financial management and control (FMC) systems and of their associated risks according to a number of risk factors (IIA). The risk assessment approach has to be used at, at least two levels: A. for the establishment of the annual audit programme, selecting projects of highest expected return and B. In the planning phases of the individual audit itself. Risk factors are: assessment of volume, sensitivity and materiality of data, the control environment, confidence in management, complexity of activities and Information systems, geographical diversity, and prior audit knowledge.
Risk Management (RM)	The overall process of identifying, assessing and monitoring risks and implementing the necessary controls in order to keep the risk exposure to an acceptable level. Best practice suggests that it should be an embedded part of the management process rather than something, which is added at a later stage. RM acts as awareness raising exercise and as a forum for sharing views at all levels in organisations; it informs and trains management and staff and increases the likelihood for success in the achievement of the objectives. Management creates the conditions and establishes tools necessary to evaluate, prioritise and decide before carrying out an activity to allow it to obtain a reasonable assurance of achieving the objectives with reasonable value for money. The internal control system ensures that management protects itself from unacceptable risks.

	Processes need to be developed to identify these risks and conceive and implement a system to control the most significant risks. A success factor for implementing the risk management system throughout the organisation is the management's general interest in the exercise. RM should be put on the agenda for the development of its own system for assessing the risks to which the organisation is subject.
Significant Control Weakness	Significant is the level of importance or magnitude assigned to an item, event, information, or problem by the internal auditor. Significant audit findings are those conditions that, in the judgement of the director of internal auditing, could adversely affect the organisation. Significant audit findings (as well as weaknesses cited from other sources) may include conditions dealing with irregularities, illegal acts, fraud, errors, inefficiency, waste, ineffectiveness, conflicts of interest, and control weaknesses.
Supervision	An essential requirement in auditing which entails proper leadership, direction and control at all stages to ensure a competent, effective link between the activities, procedures and tests that are carried out and the aims to be achieved.
Supreme Audit Institution (SAI)	The Public Body of a State which, however designated, constituted or organised, exercises by virtue of law, the highest public auditing function of that State.
Systems based Audit	Systems based audit refers to an in-depth evaluation of the internal control system with the objective to assess to extent to which the controls are functioning effectively. It is designed to assess the accuracy and completeness of financial transactions, the legality and regularity of underlying transactions and the economy, efficiency and effectiveness of operations.

Legal Framework

This section contains the main documents applicable to the PIFC Legal Framework:

1. PIFC Law;

2. FMC Rulebook

PIFC Law

PUBLIC INTERNAL FINANCIAL CONTROL LAW - 73/08

I. GENERAL PROVISIONS

Article 1

This Law governs the system of internal financial control in the public sector in Montenegro (hereinafter referred to as: “the Public Sector”), including financial management and control and internal audit and sets forth the methodology and standards and other issues important for establishment, development and carrying out the public internal financial control system.

Article 2

The public sector under this Law shall refer to: the users of the Budget of Montenegro, budgets of municipalities, state funds, independent regulatory bodies, shareholders companies and other legal entities in which the government or municipalities have a controlling stake (hereinafter referred to as: Entity).

Article 3

The public internal financial control system consists of:
- Financial management and control,
- Internal audit and
- Central unit for the harmonization of financial management and control and internal audit.

A Head of the budget user, or a head of the legal entity from the Article 2 of this Law (hereinafter referred to as: the Head of the Entity) shall be responsible for the establishment of the public internal financial control system from the paragraph 1, item 1 and 2 of this Article.

Ministry of Finance shall coordinate the establishment and development of public internal financial control system.

Article 4

Individual terms used in this law have the following meaning:
1. **Internal control system in the public sector** means the system of financial and other controls, including organisation structure, working methods and procedures and internal audit, established and implemented by the head of the entity, aimed at successful management and accomplishment of tasks of the entity in a transparent, proper, economic, efficient and effective manner.
2. **Financial management and control** means the comprehensive internal control system that is established by and is the responsibility of the head of the entity, and which, together with risk management, provides reasonable assurances that the Budget and other public funds will be used properly, economically, efficiently and effectively in the accomplishment of relevant objectives of the entity.
3. **Reasonable Assurance** means satisfactory degree of security referring to specific issue being considered with respect to expenses, benefits and risks.
4. **Risk** means a possibility for the occurrence of events that may have a detrimental impact on the accomplishment of objectives of the entity.
5. **Prior (ex ante) controls** established by the head of the entity and are necessary for taking decisions on the collection and usage of funds, undertaking of obligations, conducting procedure of public procurement, conclusion of contracts and related payments and return of incorrectly made payments.
6. **Audit trail** is a documented flow of financial and other transactions from their commencement to the completion and vice-versa, aimed at facilitating the reconstruction of all individual activities and approvals thereof.
7. **Internal audit** means an independent, objective assurance and advisory activity, aimed at providing added value and improving the operations of entity, which assists an entity in achieving their objectives by providing a systematic, disciplined approach to the evaluation and improvement of risk management, controls and management processes.
8. **Internal audit charter** means an internal act signed by the internal audit unit head and the head of the entity, setting out the purpose, authorities and responsibilities of internal audit and the head of the entity in relation to internal audit.
9. **Code of Ethics** refers to the Code of Ethics of The Institute of Internal Auditors (IIA).
10. **International internal control standards** mean the Guidelines for Internal Control Standards for the Public Sector, of the International Organisation of Supreme Audit Institutions (INTOSAI).
11. **International internal audit standards** mean the international standards of the Institute of Internal Auditors (IIA).
12. **Fraud indications** means materially significant activities, pointing out the existence of elements of offence, or criminal offences, or errors on the basis of which may be concluded that there is an intentional or wrong representation of material and financial facts.

II. FINANCIAL MANAGEMENT AND CONTROL

1.Purpose of financial management and control

Article 5

Financial management and control shall be implemented for the purpose of improving financial management and decision making in achieving objectives of the entity, especially including:

1) Compliance of operations with legislation, regulations, internal policies, contracts and procedures,
2) The provision of reliable, complete and timely financial and commercial reporting,
3) Economic, efficient and effective use of funds,
4) Protection of assets, liabilities and other resources against losses caused by mismanagement, unjustified spending and use, and against irregularities and fraud.

The Financial Management and Control relates to both financial and non financial processes and activities in the operation of the entity.

Financial management and controls are carried out in all organisational units and at all levels of the entity, and cover all resources of the entity, including EU funds.

2.Financial management and control components

Article 6

The financial management and control shall be based on the internationally accepted standards on internal control, through the application of the following, inter-related components:

1) Control environment;
2) Risk management;
3) Control activities;
4) Information and communication;
5) System monitoring and assessment.

Control environment

Article 7

Control environment from the Article 6, item 1 of this Law includes:

7) Personal and professional integrity and ethical values of heads and employees;
8) Management and method of governance;
9) Setting missions and goals;
10) Organizational structure, hierarchy in assignment of responsibilities and authorities, rights and obligations, and reporting levels;
11) Written rules and human resource management practices;
12) Competence of employees.

Risk management

Article 8

Risk management represents a procedure for identification, assessment, control and monitoring potential events and situations that may have an adverse impact the achievement of established goals of the entity and undertaking necessary measures for the purpose of reducing risk and obtaining reasonable assurance that the goals will be achieved.

Risk management from the paragraph 1 above, shall be performed on the basis of risk management strategies annually adopted by the head of the entity.

Control activities

Article 9

Control activities shall be established with the aim to reduce risk to an acceptable level applying written rules, principles and procedures.

Control activities need to be appropriate to operations or activities of the entity, timely and costs of their introduction must not exceed the expected benefits.
Control activities cover shall especially include:

1) Authorisation and approval procedures;
2) Segregation of duties in a manner that does not allow the same person to be simultaneously responsible for authorization, implementation, recording and control;
3) Double signature system whereby no commitment may be undertaken and no payment may be made without signatures of the head of the entity and a financial service head or other authorised person;
4) Access to funds and information
5) Prior control of legality performed by ex-ante financial controller or other person appointed by the head of the entity;
6) Procedures for full, correct, regular and updated recording of all business transactions;
7) Assessment of transaction effectiveness and efficiency;
8) Procedure oversight;
9) Human resource management procedures and reporting;
10) Documenting all transactions and operations related to activity of the entity in accordance with established rules.

Information and communication

Article 10

Business Information of the entity must be appropriate, updated, accurate and accessible for:

1) Effective communication at all hierarchical levels of entities;
2) Development of appropriate information system that enables all employees to have clear and precise guidelines and instructions in their role and responsibilities regarding financial management and control;
3) Documenting all processes and transactions, including system descriptions, through flow diagrams, accounting and filing system intended for the preparation of appropriate audit trail;
4) Establishment of effective, timely and reliable reporting system, including reporting levels and time frames, types of reports submitted to management and manner of reporting in case of detected errors, irregularities, misuse of funds and information, deceit or non-allowed actions.

System monitoring and assessment

Article 11

The head of the entity shall be accountable for monitoring and assessment of the financial management and control system for the purpose of assessing its adequacy and functioning and providing timely updating.

System monitoring and assessment from the paragraph 1 of this Article, is performed by continuing monitoring, self-assessment and internal audit.

3.Management responsibility

Article 12

The managers of the entities under Article 2 shall be accountable for achieving the objectives of the entities by managing public funds in a legal, economical, efficient and effective manner.

Article 13

The head of the entity is responsible for:

1) Putting in place adequate system of financial management and control;
2) Setting the objectives of the entity managed by him/her; preparation and implementation of strategic and other plans, and action programmes for achieving those objectives;
3) Identification, assessment and management of risks that may prevent achievement of the objectives of the entity, and the introduction of adequate controls to manage those risks in accordance with this law and international internal control standards;
4) Lawful, economic, efficient and effective use of available funds;
5) Effective human resource management and maintaining needed level of expertise;
6) Keeping and protecting resources and information from losses, disclosure, unauthorized use and misuse;
7) Segregation of duties with respect to decision making, implementation and control;
8) Comprehensive accurate and timely recording of all transactions;
9) Documenting all transactions and operations within the entity;
10) Monitoring and updating of the financial management and control system and undertaking measures for the improvement of the system, in accordance with recommendations of internal audit and other assessments;
11) Reporting on the development and the adequacy of the financial management and control system;
12) Introduction of internal rules, procedures and guidelines for financial management and control systems;

On the basis of Internal Systematization and Organization Act, the head of the entity may delegate individual duties and responsibilities or authorizations to other employees within the same entity.

The delegation of authorizations and responsibilities from the paragraph 2 above does not eliminate the accountability of the head of the entity.

Internal organisational unit heads are responsible to the head of the entity for financial management and control activities put in place in organizational units under their responsibility.

Article 14

The head of the entity shall appoint a person to be responsible for the establishment, implementation and development of financial management and controls.

The establishment of the financial management and control system shall be done on the basis of the plan for the aforementioned and methodology for the implementation of the plan determined by the head of the entity.

The Ministry of Finance shall adopt a regulation on the manner and procedure for the establishment of the financial management and control system.

4. Financial management and control reporting

Article 15

The head of the entity shall be responsible to submit to the Central harmonization unit of the Ministry of Finance annual report on activities related to the establishment and development of financial management and control, by the end of January of the current year for the previous year.

Ministry of Finance shall adopt a regulation on the form and the content for reporting referred to in paragraph 1 above shall be prescribed by the.

III. INTERNAL AUDIT

1. Role and tasks of internal audit

Article 16

Internal audit shall be carried out in order to provide objective and expert opinion and advice on the adequacy of the financial management and control systems with the objective of providing improvement in the operation of the entity.

Internal audit helps the entity in achieving its goals by applying a systematic and disciplined approach in evaluating operation of the entity involving:

1) The planning of audit work through the identification and assessment of the nature and level of risk relating to each activity in the entity;
2) Assessment of the adequacy and efficiency of financial management and control system with respect to:
    a) Risk identification, assessment and management by the head of the entity;
    b) Compliance with laws and other regulations, operational guidelines, internal policies and contracts;

c) Accurate, reliable and complete financial and other operational information;
d) Efficiency, effectiveness and economy of operations;
e) Protection of resources and information;
f) Implementation of tasks and achievement of goals;

3) Making recommendations to the entity for improvements to the financial management and control system.

Internal audit may provide consulting services for special unplanned tasks initiated by the heads of the entity, which objective is to create added value and improve the management process, risk management and control, without being responsible for the implementation of its recommendations.

The scope and objective of any consulting services engagement from the paragraph 3 of this Article shall be harmonized between the head of the entity and the head of the internal audit unit.

Article 17

The work of Internal Audit involves the following elements:

- risk assessment,
- planning,
- audit implementation,
- reporting and
- follow-up on the given recommendations.

The Internal audit types are: system audit, compliance audit, successful operation audit (performance audit), financial audit and information technology audit.

Internal audit is carried out through objective evaluation of evidence by internal auditors, aimed at giving an objective, independent opinion or conclusion related to the process, system or other area covered by the audit.

2. Establishment and independence of internal audit

Internal audit establishment

Article 18

Entities are obliged to establish internal audit in one of the following ways:

1) By organizing an independent organizational internal audit unit within the entity which will report directly to the head of the entity;
2) By organizing a joint internal audit unit upon proposal of two or more entities, subject to the prior approval of the Ministry of Finance;
3) By agreement that internal audit shall be performed by the internal audit unit of another entity or local government unit, subject to the prior approval of the Ministry of Finance.

Internal audit units of the Entities shall perform internal audit of the units that are the users of budget funds within budget funds of the entity, if they do not have their units established.

Internal audit units of the Entities shall coordinate the work of the internal audit units of users from the paragraph 2, of this Article that has established the internal audit units.

The manner and the criteria for the establishment of internal audit from the paragraph 1, of this Article shall be determined on the basis of the regulation of the Government of Montenegro (hereinafter referred to as: “the Government”).

The number of employees in the internal audit unit shall be at least three internal auditors, including the head of internal audit unit.

Article 19

The head of the entity is responsible for the provision of conditions for functioning of internal audit including:

1. The appointment of a Head of Internal Audit after consultation with the Ministry of Finance;
2. The signing of an Audit Charter;
3. The provision of resources to enable internal audit to function effectively;
4. Endorsing the strategic and annual plans of internal audit;
5. The implementation of agreed internal audit recommendations;
6. Recording non-agreed recommendations on the basis of internal audit report;
7. Providing an annual report on internal audit activities to the Ministry of Finance.

The Head of the entity, having established an independent internal audit unit, may establish an audit committee in accordance with International Internal Audit Standards, as an advisory body for internal control and internal audit issues.

Internal audit independence

Article 20

Internal audit unit must be functionally and organizationally independent from other organizational units of the entity.

Functional independence is established through independent planning, implementation and reporting of completed internal audits.

Internal audit head and internal auditors may perform only internal audit.

Article 21

The head of the internal audit unit shall be independent in his/her work and may not be reassigned to other work position or dismissed due to the disclosure of facts or making recommendations in the internal audit report.

3. Internal audit standards and methodology

Article 22

Internal audit is carried out in accordance with legislation governing internal audit and International internal audit standards.

In their work, internal auditors must adhere to the internal audit charter, the ethical code of internal auditors, internal audit working methodology, directions and instructions.

Methodology, directions and instructions from the paragraph 2 of this Article shall be determined on the basis of the regulation of the Ministry of Finance.

The Internal audit unit of the Entity may, due to the complexity of work and tasks of the entity, develop additional methodological instruction and guidance for performing internal audit, specifying in more details methods to be used in the process of audit.

Internal audit planning, conducting and reporting

Article 23

Internal audit shall be conducted on the basis of:

1) strategic plan
2) annual plan and
3) individual audit plan.

Strategic and annual internal audit plans, shall be prepared by the internal audit unit head on the basis of objective risk assessment, and will be endorsed by the head of the entity.

The strategic plan is adopted for the next three-year.

The Strategic plan shall be reviewed against risks and audit scope at least once a year.

The annual internal audit plan, developed on the basis of strategic plan, shall be adopted by the end of the current year for the next year.

Individual audits are performed on the basis of the plan describing in detail the subject matter, objectives, duration, distribution of resources, techniques, types and coverage of audit examinations.

Internal audit unit head approves the individual audit plan and related programmes, describing in detail the audit procedures.

Article 24

The audit is performed by direct review of the documentation, determining, analysing, assessing and documenting data that are sufficient for giving an expert opinion on set goals of the entity.

Any completed audit must result in a draft audit report containing summary, goals and scope of audit, findings, conclusions and recommendations.

Draft audit report shall be submitted to the responsible person of the entity that was subject to audit for the purpose of stating its opinion on the statements from the draft audit report.

The responsible person from the paragraph 3, of this Article shall have the right to object to the draft audit report, which will be included in the final report. Objections to the draft audit report and proposal of the activity plan for implementation of accepted recommendation shall be submitted to the head of the internal audit unit within eight days following the day of receiving the draft audit report.

After consultation with the responsible person of the entity that was subject to audit and after stating its opinion on the draft report, the internal auditor finalises the audit report with a proposal for an action plan for the implementation of its recommendations and sends it both to the Head of Internal Audit and the Head of the Entity.

The Head of Entity shall inform the internal audit unit in writing about the adoption of the action plan from the paragraph 5, of this Article, within thirty days after the presentation of the final audit report and about the actions taken to implement the recommendations.

Ministry of Finance shall adopt a regulation on more detailed manner and procedure of work in the internal audit.

4. Rights and responsibilities of internal audit unit head and internal auditors

Rights of Internal Audit Unit head and internal auditors

Article 25

Internal audit unit heads and internal auditors have a right to:

1) Free access to heads, employees and resources of the entity who are related to the conduct of audits;
2) Free access to all information, as well as all available documents and records, including electronic ones, which are needed for the conduct of audits;
3) Demand from responsible persons any necessary data, statements, opinions, documents or other information needed for the conduct of audits.

Article 26

In addition to the rights specified in Article 25 above, internal audit unit head has a right to:
1) Report to the head of the entity on all major remarks regarding the conduct of a particular audit;
2) Propose to the head of the entity to hire experts whose special knowledge and skills are needed during the audit.

Responsibilities of Internal Audit Unit head and internal auditors

Article 27

Internal audit unit head is responsible to carry out planned internal audits and other activities of the internal audit unit, especially including:

1) Preparation and submission to the head of the entity for approval of the draft internal audit charter,
2) Preparation and submission to the head of the entity for endorsement of the Strategic and annual internal audit plans;
3) Organization, coordination and distribution of work assignments to internal auditors in accordance with their knowledge and skills;
4) Approval of conduct of individual audit plans;
5) Monitoring of the implementation of annual internal audit plans and application of internal audit methodology based on international internal audit standards;
6) Monitoring of the implementation of internal audit recommendations;
7) Professional and overall performance of internal audit.
8) Assessment of new financial management and control systems;
9) Preparation and submission for approval to the head of the entity of a plan for the continuous professional training and development of internal audit staff.

Article 28

Internal audit head is obliged to submit to the head of the entity:

1) Annual report on the work of internal audit and assessment of adequacy and effectiveness of financial management and control system;
2) Report on the results of each individual audit and all major findings and recommendations for the improvement of operation of the entity;
3) Periodic reports on the implementation of internal audit annual plans;
4) Reports on all cases where activities of internal audit head and internal auditors have been confronted with restrictions
5) Report on adequate resources for the conduct of internal audit.

Article 29

Internal audit unit head and internal auditors must possess appropriate knowledge in order to be able to recognise indications of fraud.

When fraud indications have been identified, internal audits shall be obliged to discontinue the audit process and immediately report to the internal audit unit head, who will immediately notify the head of the entity in writing.

Upon receiving the notification from the paragraph 2 of this article, the head of the entity shall be responsible to undertake all necessary actions and inform responsible public authorities.

Article 30

Internal audit unit head and internal auditors shall be obliged to keep the documents and data and information made available to them during the audit confidential.

Article 31

Internal audit unit head and internal auditors are obliged to cooperate and coordinate their work with Central Harmonization Unit of the Ministry of Finance, with the objective to receive recommendations and instructions necessary for their work.

Article 32

The head of the entity shall be obliged to submit to the Central Harmonization Unit of the Ministry of Finance annual report on the work of internal audit, by the end of January of the current year for the previous year.

The content of the annual report and the manner of reporting from the paragraph 1 of this Article shall be prescribed by the regulation of the Ministry of Finance.

Article 33

Internal auditor shall be obliged to suspend all activities regarding an audit and inform, with no delay, a head of the internal audit unit about the existence of the conflict between his personal and business interests, as well as about the activities he was engaged in during the year preceding the year of audit, which are related to the subject of the audit.

5. Requirements for internal audit unit head and internal auditors

Article 34

In addition to general requirements defined by the Law, an internal auditor must have:

1) university education;
2) at least two years work experience in auditing, financial control and accounting – financial operations;
3) passed the examination for authorised internal auditor.

Examination for authorized internal auditor from the paragraph 1, item 3 of this Article is taken on the basis of curricula prescribed by the Ministry of Finance.

Examination from the paragraph 2, of this Article shall be conducted in front of the Commission established by the Ministry of Finance.

The manner of conducting the examination for authorized internal auditor shall be prescribed by the Ministry of Finance.

Article 35

Internal audit unit head may be a person who in addition to requirements from the Article 34, paragraph 1, item 1 and 3, has at least five years of work experience, of which a minimum of two years in auditing.

Article 36

Internal auditor performs internal audit tasks with a certain title.

Titles of internal auditors shall be determined by the Government.

6. Internal audit of EU funded programmes and projects

Article 37

Entities from the Article 2, of this Law, using the EU funds, when defining financial management and control and internal audit activities, shall be obliged to apply requirements defined by the European Commission.

The internal audit units of the entities from the Article 2, of this Law, shall be obliged to conduct internal audit for entities and other beneficiaries implementing programmes and wholly or partially financed from the EU funds, including all other participants that have received funds on account of EU programs and projects.

The audit of EU programmes and funds is carried out in accordance with internationally accepted audit standards, provisions of international agreements for the use of such funds and appropriate regulation in the area of management and control of all EU funds.

IV. CENTRAL HARMONIZATION UNIT

Article 38

The Central Harmonization Unit with the Ministry of Finance shall be established for the purpose of:

1) preparation of professional basis for development of laws and enabling regulations in the area of financial management and control and internal audit;
2) development of methodology and work standards in financial management and control and internal audit;
3) preparation, organising and running training programs for taking examinations for authorised internal auditors;
4) ensuring a continuing professional development plan for authorised internal auditors;
5) preparing, organising and running training programmes and training of persons responsible for and involved in financial management and control and internal audit;
6) coordination of establishment and development of internal financial management and control and internal audit;
7) maintaining register of: internal audit units, internal audit charters, authorized internal auditors and persons included in financial management and control;
8) monitoring of the implementation of laws, enabling regulations and internal rules, standards for financial management and control and internal audit, ethical code of internal auditors, instructions and methodologies for financial management and control and internal audit;
9) review of quality of the financial management and control system and internal audit with entity, with the objective of monitoring over implementation of recommendations for the purpose of collecting information for the improvement of work methodologies and standards;
10) cooperation with professional bodies and institutions in the area of financial management and control and internal audit.

Central harmonization unit prepares an annual consolidated report on the system of internal financial controls, based on the Report from the Article 15 and 32 of this Law, and delivers to the Government by the end of March of the current year for the previous year.

The report referred to in paragraph 2 above contains data on financial management and control, material more significant findings and recommendation of internal audit and relevant activities undertaken by the head of the entity for the purpose of improving internal financial control systems.

V. TRANSITIONAL AND FINAL PROVISIONS

Article 39

Enabling regulations for this Law shall be passed within 9 (nine) months of the effective date of this Law.

Article 40

Pursuant to provisions of Article 18 above, users of the funds of the Budget of Montenegro and the Capital City are obliged to establish internal audit within 12 months and other entities from the Article 2 of this Law within 24 months, after the effective date of the regulation from the Article 39, of this Law.

Article 41

Persons who have not passed examination for authorized internal auditor, and who meet other conditions from Article 34 above, may perform duties of authorized internal auditor without passed examination for a maximum of 2 years after the date of adoption of the programme for taking the examination for authorised internal auditors.

Article 42

Provisions of the Article 35 of this Law shall be effective from 1st January 2012.

Article 43

On the effective date of the Articles 39 and 40 of this Law, chapters: «IX. INTERNAL AUDIT» and Articles 56, 57 and 57(a) of the Law on Budget («Official Gazette of RoM», No. 40/01, 44/01, 71/05 and 12/07) shall cease to exist.

Article 44

This Law becomes effective on the eighth day upon its publication in the "Official Gazette of Montenegro".

FMC Rulebook - 37/10

Pursuant to Article 14 paragraph 3 of the Law on Public Internal Financial Control (Official Gazette of Montenegro, 73/08) and Article 46 of the Budget Law (Official Gazette of the Republic of Montenegro, 40/01, 44/01, 71/05, Official Gazette of Montenegro 12/07, 73/08 and 53/09), the Ministry of Finance passed the following

RULEBOOK
ON THE MANNER AND PROCEDURE FOR ESTABLISHING AND IMPLEMENTING PUBLIC FINANCIAL MANAGEMENT AND CONTROL

Article 1

This Rulebook shall govern the manner and procedures for establishing and implementing financial management and control.

Article 2

Financial management and control shall include all activities, relating in particular to budget planning and execution, conducting public procurement procedures, payments as par valid agreements and other commitments, protection of property against loss, misuse, malpractice and fraud, as well as other non-financial activities in the operation of an entity.

Article 3

Financial management and control shall be established in order to attain the goals of the entity which are specific, measurable, attainable, realistic and time-bound, and implemented through programmes, activities and projects.

Article 4

Establishing and implementing financial management and control shall be carried out based on a plan for establishing financial management and control, which shall contain in particular:

- activities on establishing financial management and control,
- persons in charge of conducting the activities, and
- timeframes for the implementation of activities.

Article 5

The person designated to establish, implement and develop financial management and control in an entity shall perform the tasks relating in particular to the following:

- prepare and monitor the implementation of the Plan for Establishing Financial Management and Control;
- coordinate the activities on establishing and developing financial management and control,

- assist the head of the entity in establishing the risk management strategy,
- prepare and monitor the implementation of the plan for rectifying deficiencies of internal control,
- prepare annual reports on financial management and control,
- report to the head of the entity on the current status and development of financial management and control,
- cooperate with the Central Harmonization Unit of the Ministry of Finance.

Article 6

Establishing and implementing financial management and control shall be carried out through:

- setting the entity's mission (reason for existence and main activities of the entity) and goals,
- adoption of written internal rules and procedures pursuant to the law and regulations,
- reviewing financial management and control components, as referred to in Article 6 of the Law on Public Internal Financial Control assessing the adequacy of the existing control, the deficiencies and remedial actions,
- production of the list of major business processes and activities carried out in the entity,
- description of major business processes and activities including the financial and other transactions document flow – audit trail from the very beginning to the end, persons responsible for their implementation, method and deadline for implementing certain processes and activities,
- risk identification and assessment in relation to major business processes and activities,
- analysis of existing and identification of additional control needed or redundant control, and
- adoption and monitoring the implementation of the plan for rectifying deficiencies of internal control.

Article 7

The head of an entity, in line with laws and regulations, shall give instructions and guidance particularly:

- to persons he/she designated for financial management and control,
- for establishing control of the right to access funds, records and the use thereof,
- for receiving, recording, referral for operation, processing, archiving and keeping of accounting documents and other business-related documentation,
- for financial tasks referring to ex-ante financial control,
- for data checks and verification in subsidiary ledgers and harmonisation with the data in the Main Ledger,
- for the use, safety and protection of IT system data,
- for execution of certain types of expenditures,
- for informing the staff at all levels on the data relevant for the implementation of business activities of the entity in order to attain effectiveness, diligence and legality of the work of all members of staff.

Article 8

One or more officers shall be designated to perform the tasks of ex-ante financial control including: approval, certifying documents, authorisation of payments, revenue control and cashier operation.

The tasks referring to approval of financial transactions, certification of documents used as the basis for the financial transaction and authorisation of payments shall be performed by different persons.

Article 9

Risk identification shall be performed in relation to attainment of goals of major business processes.

Risk identification is done during the annual budget planning process of the entity.

Following risk identification, impact assessment of such risks shall be done in relation to the probability of risk occurrence and possible consequences that may adversely impact the attainment of entity's goals.

Assessed risk shall be entered in the risk register containing: business goals, identified risks, probability of risk occurrence and possible consequences, envisaged risk management measures and persons responsible for their implementation.

Risk management strategy shall be compiled based on the data from the risk register.

Article 10

Upon the completion of risk assessment, the control activities in place within a business process shall be analysed to assess risk management or to reduce the risks to an acceptable level and introduce more effective and efficient control or remove redundant control.

Following the analysis referred to in paragraph 1 herein, the remedial plan shall be compiled containing measures and activities for rectifying deficiencies of internal control stipulating the relevant deadline and responsible persons.

Article 11

This Rulebook shall come into force on the eighth day upon its publication in the Official Gazette of Montenegro.

Minister,
Igor Lukšić, (m.p.)

This Rulebook has been published in Official Gazzette of Montenegro no. 37/ 10 - 9. July 2010.

Annexes

These Annexes are included as examples and should be adapted to suit the needs of the organisations. If you need any assistance with the self assessment then contact CHU in the Ministry of Finance.

Annex 1a – Internal Control Self Assessment Questionnaire

Public Internal Financial Control comprises a system of financial management and control including internal audit in the public entity, based on uniform standards and continuous assessment of the system. Public Internal Financial Control is not limited to financial or accounting activities only but to all operations of the public entity.

Public Internal Financial Control is based on the presumption that the achievement of the mission and objectives of the entity is exposed to risks. Hence it is the responsibility of the head of the entity to clearly define the mission, general, specific and operational objectives at the level of the entity as well as at the level of all organisational units, functions and processes, identify and analyse risks, take appropriate measures for their control and permanently assess their economy, efficiency and effectiveness helped by internal auditing.

Measures that the entity takes to address risks represent internal control, i.e. a system of methods and procedures that assure to the head of the entity:

- ✓ the compliance of operations with acts and regulations,
- ✓ reliable and timely reporting,
- ✓ economic, efficient and effective use of resources,
- ✓ safeguarding of assets
- ✓ prevention of fraud and corruption.

The internal control framework encompasses five interrelated components

- ✓ Control environment
- ✓ Risk analysis
- ✓ Control activities,
- ✓ Information and communication,
- ✓ Monitoring and supervision.

1) Control environment

The control environment is the entirety of the integrity, relation, awareness and of to the objectives oriented approach of the head of the public entity and management at all levels regarding the setting up and maintaining the internal control what is reflected in the entire staff of the entity. Every employee and especially the management must have knowledge of the internal control and understand the purpose and significance of it. The control environment is efficient only if all the staff understands proper authorities and responsibilities, respects the ethic code, and fulfils the requirements of the work posts and the entity as whole has transparent and effective recruitment procedures.

2) Risk analysis

Risk analysis is a systematic and disciplined process of defining entity's mission and objectives, identifying risks that may influence the achievement of the objectives, evaluation of risks regarding the probability of their occurrence and the impact and taking measures to control risk at the acceptable level considering the costs and advantages.

The result of the process is a risk register, a list of objectives, risks with respective probabilities and impacts, measures to control them and persons in charge. Risk register is a process not a finite product and must be continuously reviewed and updated.

3) Control activities

To control risks at the acceptable level the head of the entity takes measures in form of instructions, procedures, processes, activities. Internal control is based on written procedures, use of check lists, detailed description of procedures and tasks, adequately occupied work posts, continuity of activities, double signature, segregation of duties, identification and supervision of critical work posts, staff rotation, physical safeguarding, delegation of duties in writing, evidencing and reporting nonstandard procedures,…

4) Information and communication

The public entity must have procedures in place that provide for the flow and exchange of information and communication in all directions and at all levels in form of regular and ad hoc meetings, work group reports, information reception direction, whistle blowing, and other. It is important that employees have access to their superiors and that they dispose of sufficient information for their work.

5) Monitoring and supervision

The head of the entity must provide for continuous assessment of the internal control. The basic task of internal auditor is the assessment of the internal control, reporting on weaknesses and recommending improvements. Besides internal auditing, internal control is assessed through self assessments, irregularity reports, assessments by other bodies and institutions and other exchange of information.

1. INTERNAL (CONTROL) ENVIRONMENT

Internal control environment is the basis of internal control. It is represented by the control culture, typical for each entity, defining the entire attitude of the management and all the employees regarding the setting and achievement of the objectives, risk management, internal control and internal auditing. The internal control environment is mostly influenced by ethical values, integrity, ability of all the employees, conduct and methods of the management (the delegation of authorities and responsibilities, human resources practices), the internal organisation and other.

1.1 Integrity and ethical values

a) Procedure is implemented assuring that all the employees are acquainted with the code of conduct of civil servants?

- *YES, on all operations,* ☐
- *YES, on majority of operations,* ☐
- *YES, on certain operations,* ☐
- *NO, activities started,* ☐
- *NO.* ☐

Comment:..
....

b) Entity's operations adapted code of conduct is adopted?

- *YES, on all operations,* ☐
- *YES, on majority of operations,* ☐
- *YES, on certain operations,* ☐
- *NO, activities started,* ☐
- *NO.* ☐

Comment:..
....

c) Employees sign to adhere to the general code of conduct of civil servants and to the specific code of conduct when existing?

- *YES, on all operations,* ☐
- *YES, on majority of operations,* ☐
- *YES, on certain operations,* ☐
- *NO, activities started,* ☐
- *NO.* ☐

Comment:..
....

d) Sanctions are foreseen in case of non adherence of employee to the code of conduct or of non respect of laws, regulations, guidance and instructions of the superiors.

- *YES, on all operations,* ☐
- *YES, on majority of operations,* ☐
- *YES, on certain operations,* ☐
- *NO, activities started,* ☐
- *NO.* ☐

Comment:..
....

e) Sanctions in case of non adherence of employee to the code of conduct or of non respect of laws, regulations, guidance and instructions of the superiors are strictly implemented.

- *YES, on all operations,* ☐
- *YES, on majority of operations,* ☐
- *YES, on certain operations,* ☐
- *NO, activities started,* ☐
- *NO.* ☐

Comment:...

1.2 Human resources politics and procedures

a) The entity has for the achievement of the mission and the objectives appropriate and with the regulations compliant systemisation that is continuously updated.

- *YES, on all operations,* ☐
- *YES, on majority of operations,* ☐
- *YES, on certain operations,* ☐
- *NO, activities started,* ☐
- *NO.* ☐

Comment:...

b) Human resources policy exists and assures the recruitment of appropriate candidates.

- *YES, on all operations,* ☐
- *YES, on majority of operations,* ☐
- *YES, on certain operations,* ☐
- *NO, activities started,* ☐
- *NO.* ☐

Comment:...

c) The criteria for the assessment of the effectiveness of human resources/recruitment exist and are regularly used.

- *YES, on all operations,* ☐
- *YES, on majority of operations,* ☐
- *YES, on certain operations,* ☐
- *NO, activities started,* ☐
- *NO.* ☐

Comment:...

d) The recruitment commission is appointed according to the adopted internal procedure. It prepares in advance the recruitment selection criteria.

- *YES, on all operations,* ☐
- *YES, on majority of operations,* ☐
- *YES, on certain operations,* ☐
- *NO, activities started,* ☐
- *NO.* ☐

Comment:..

e) For every employee expected individual results are identified and represent criteria for employee's performance assessment and bonus.

- *YES, on all operations,* ☐
- *YES, on majority of operations,* ☐
- *YES, on certain operations,* ☐
- *NO, activities started,* ☐
- *NO.* ☐

Comment:..

f) Employee's performance is assessed on regular basis.

- *YES, on all operations,* ☐
- *YES, on majority of operations,* ☐
- *YES, on certain operations,* ☐
- *NO, activities started,* ☐
- *NO.* ☐

Comment:..

g) Employees are assured continuous professional training.

- *YES, on all operations,* ☐
- *YES, on majority of operations,* ☐
- *YES, on certain operations,* ☐
- *NO, activities started,* ☐
- *NO.* ☐

Comment:..

h) For the entity a plan for continuous professional development of employees is adopted and person is in charge for the coordination of the preparation, needs coordination and efficient and effective implementation.

- *YES, on all operations,* ☐
- *YES, on majority of operations,* ☐
- *YES, on certain operations,* ☐
- *NO, activities started,* ☐
- *NO.* ☐

Comment:...
....

1.3 Management philosophy and methods

a) The head of the entity and the management at all levels is aware of the advantages of risk management, internal control and internal auditing for the achievement of mission and objectives.

- *YES, on all operations,* ☐
- *YES, on majority of operations,* ☐
- *YES, on certain operations,* ☐
- *NO, activities started,* ☐
- *NO.* ☐

Comment:...
....

b) The head of the entity and management at all levels plan their activities for the achievement of objectives.

- *YES, on all operations,* ☐
- *YES, on majority of operations,* ☐
- *YES, on certain operations,* ☐
- *NO, activities started,* ☐
- *NO.* ☐

Comment:...
....

c) The head of the entity and the management meet and discuss the achievement of objectives.

- *YES, on all operations,* ☐
- *YES, on majority of operations,* ☐
- *YES, on certain operations,* ☐
- *NO, activities started,* ☐
- *NO.* ☐

Comment:...
....

1.4 Entity structure

a) The organisational structure, authorities and responsibilities of employees are clearly defined and included in internal acts.

- *YES, on all operations,* ☐
- *YES, on majority of operations,* ☐
- *YES, on certain operations,* ☐
- *NO, activities started,* ☐
- *NO.* ☐

Comment:...
....

b) For the achievement of the objectives required activities, actions and tasks are identified an attributed to appropriate work posts.

- *YES, on all operations,* ☐
- *YES, on majority of operations,* ☐
- *YES, on certain operations,* ☐
- *NO, activities started,* ☐
- *NO.* ☐

Comment:...
....

c) For each action/task a responsible employee is identified.

- *YES, on all operations,* ☐
- *YES, on majority of operations,* ☐
- *YES, on certain operations,* ☐
- *NO, activities started,* ☐
- *NO.* ☐

Comment:...
....

d) The number, education and skills of employees satisfy the needs for the achievement of objectives.

- *YES, on all operations,* ☐
- *YES, on majority of operations,* ☐
- *YES, on certain operations,* ☐
- *NO, activities started,* ☐
- *NO.* ☐

Comment:...
....

1.5 Responsibility

a) A reporting system regarding the risk management, internal control and internal audit to the head of the entity and to the management at all levels is set up.

- *YES, on all operations,* ☐
- *YES, on majority of operations,* ☐
- *YES, on certain operations,* ☐
- *NO, activities started,* ☐
- *NO.* ☐

Comment:...
....

2. RISK MANAGEMENT

The public entity must set clear, inter compatible and measurable objectives, identify objectives that may influence the achievement of objectives and implement measures to control risks at acceptable level.

2.1 Objectives: The public entity must set clear objectives that are inter compatible and support the strategy of the public entity and the budget. The objectives must be measurable, and the management must inform about the objectives the employees.

a)Long term objectives are set and documented.

- *YES, on all operations,* ☐
- *YES, on majority of operations,* ☐
- *YES, on certain operations,* ☐
- *NO, activities started,* ☐
- *NO.* ☐

Comment:...
....

b) Short term objectives are set and documented.

- *YES, on all operations,* ☐
- *YES, on majority of operations,* ☐
- *YES, on certain operations,* ☐
- *NO, activities started,* ☐
- *NO.* ☐

Comment:...
....

c) Short term objectives support the achievement of long term objectives.

- *YES, on all operations,* ☐
- *YES, on majority of operations,* ☐
- *YES, on certain operations,* ☐
- *NO, activities started,* ☐
- *NO.* ☐

Comment:...
....

d) Employees are aware of long term and short term objectives.

- *YES, on all operations,* ☐
- *YES, on majority of operations,* ☐
- *YES, on certain operations,* ☐
- *NO, activities started,* ☐
- *NO.* ☐

Comment:..

e) Criteria are set for the measurement of the achievement of objectives.

- *YES, on all operations,* ☐
- *YES, on majority of operations,* ☐
- *YES, on certain operations,* ☐
- *NO, activities started,* ☐
- *NO.* ☐

Comment:..

f) The entity monitors the achievement of objectives and analyses causes in case of non achievement.

- *YES, on all operations,* ☐
- *YES, on majority of operations,* ☐
- *YES, on certain operations,* ☐
- *NO, activities started,* ☐
- *NO.* ☐

Comment:..

2.2 Risks related to objectives: The public entity sets a system for the identification, analysis and control of risks.

a) Risks are identified?

- *YES, on all operations,* ☐
- *YES, on majority of operations,* ☐
- *YES, on certain operations,* ☐
- *NO, activities started,* ☐
- *NO.* ☐

Comment:..

b) Risks are analysed.

- *YES, on all operations,* ☐
- *YES, on majority of operations,* ☐
- *YES, on certain operations,* ☐
- *NO, activities started,* ☐
- *NO.* ☐

Comment:..
....

c) The risk response is set and internal control identified.

- *YES, on all operations,* ☐
- *YES, on majority of operations,* ☐
- *YES, on certain operations,* ☐
- *NO, activities started,* ☐
- *NO.* ☐

Comment:..
....

d) The entity identifies and monitors identified risks in a systematic way.

- *YES, on all operations,* ☐
- *YES, on majority of operations,* ☐
- *YES, on certain operations,* ☐
- *NO, activities started,* ☐
- *NO.* ☐

Comment:..
....

e) Risk register is regularly assessed and updated.

- *YES, on all operations,* ☐
- *YES, on majority of operations,* ☐
- *YES, on certain operations,* ☐
- *NO, activities started,* ☐
- *NO.* ☐

Comment:..
....

f) Effectiveness and efficiency of internal control is assessed.

- *YES, on all operations,* ☐
- *YES, on majority of operations,* ☐
- *YES, on certain operations,* ☐
- *NO, activities started,* ☐
- *NO.* ☐

Comment:..
....

g) The system is set that assures employees the information on risks of their concern.

- *YES, on all operations,* ☐
- *YES, on majority of operations,* ☐
- *YES, on certain operations,* ☐
- *NO, activities started,* ☐
- *NO.* ☐

Comment:..

3. CONTROL ACTIVITIES

Control activities are guidance and procedures set by the head of the entity to control risks.

a) Processes are documented in detail with descriptions of flow of documents, points of decision and internal controls.

- *YES, on all operations,* ☐
- *YES, on majority of operations,* ☐
- *YES, on certain operations,* ☐
- *NO, activities started,* ☐
- *NO.* ☐

Comment:..

b) Detailed descriptions of processes and operations are available to the employees.

- *YES, on all operations,* ☐
- *YES, on majority of operations,* ☐
- *YES, on certain operations,* ☐
- *NO, activities started,* ☐
- *NO.* ☐

Comment:..

c) There are written operations instructions for every work post.

- *YES, on all operations,* ☐
- *YES, on majority of operations,* ☐
- *YES, on certain operations,* ☐
- *NO, activities started,* ☐
- *NO.* ☐

Comment:..

d) Operation instructions include internal control.

- *YES, on all operations,* ☐
- *YES, on majority of operations,* ☐
- *YES, on certain operations,* ☐
- *NO, activities started,* ☐
- *NO.* ☐

Comment:..
....

e) Segregation of duties: the same employee cannot perform following tasks: initialisation, authorisation, execution in evidencing?

- *YES, on all operations,* ☐
- *YES, on majority of operations,* ☐
- *YES, on certain operations,* ☐
- *NO, activities started,* ☐
- *NO.* ☐

Comment:..
....

f) Internal acts, process descriptions, operation instructions, organisation charts are regularly updated.

- *YES, on all operations,* ☐
- *YES, on majority of operations,* ☐
- *YES, on certain operations,* ☐
- *NO, activities started,* ☐
- *NO.* ☐

Comment:..
....

g) Accounting system includes accounting controls.

- *YES, on all operations,* ☐
- *YES, on majority of operations,* ☐
- *YES, on certain operations,* ☐
- *NO, activities started,* ☐
- *NO.* ☐

Comment:..
....

h) Access to data and evidences is controlled.

- *YES, on all operations,* ☐
- *YES, on majority of operations,* ☐
- *YES, on certain operations,* ☐
- *NO, activities started,* ☐
- *NO.* ☐

Comment:..
....

i) Supervision: Management supervision procedures are implemented.

- *YES, on all operations,* ☐
- *YES, on majority of operations,* ☐
- *YES, on certain operations,* ☐
- *NO, activities started,* ☐
- *NO.* ☐

Comment:..
....

4. INFORMATION AND COMMUNICATION

Information and communication allows for the collection and exchange of information, necessary for the management, execution and monitoring of operations.

a) The head of the entity and management at all levels receive reliable, relevant, timely and sufficient information (summaries, analytical, reports on exceptions, special information,..), to take necessary decisions.

- *YES, on all operations,* ☐
- *YES, on majority of operations,* ☐
- *YES, on certain operations,* ☐
- *NO, activities started,* ☐
- *NO.* ☐

Comment:..
....

b) Information enables the head of the entity and management at all levels to monitor the achievement of objectives and operations supervision.

- *YES, on all operations,* ☐
- *YES, on majority of operations,* ☐
- *YES, on certain operations,* ☐
- *NO, activities started,* ☐
- *NO.* ☐

Comment:..
....

c) Information and communication system adapts to the changes in the entity, objectives and strategy.

- *YES, on all operations,* ☐
- *YES, on majority of operations,* ☐
- *YES, on certain operations,* ☐
- *NO, activities started,* ☐
- *NO.* ☐

Comment:..
....

d) The effective and efficient system of communication assures that employees receive necessary information for their work.

- *YES, on all operations,* ☐
- *YES, on majority of operations,* ☐
- *YES, on certain operations,* ☐
- *NO, activities started,* ☐
- *NO.* ☐

Comment:...
....

e) Employees assure constructive follow up to the complaints of other organisational units or external clients.

- *YES, on all operations,* ☐
- *YES, on majority of operations,* ☐
- *YES, on certain operations,* ☐
- *NO, activities started,* ☐
- *NO.* ☐

Comment:...
....

.

f) The head of the entity and management are informed with the extent and contents of complaints.

- *YES, on all operations,* ☐
- *YES, on majority of operations,* ☐
- *YES, on certain operations,* ☐
- *NO, activities started,* ☐
- *NO.* ☐

Comment:...
....

g) Employees have means to report on irregularities and problems and submit suggestions for improvements.

- *YES, on all operations,* ☐
- *YES, on majority of operations,* ☐
- *YES, on certain operations,* ☐
- *NO, activities started,* ☐
- *NO.* ☐

Comment:...
....

5. Monitoring and supervision

The process of risk management and internal control is regularly assessed, evaluated on the efficiency and effectiveness and improved in relation to weaknesses identified and changes in operations, objectives or environment.

a) The entity has set up a system of regular assessment of risk management and internal control.

- *YES, on all operations,* ☐
- *YES, on majority of operations,* ☐
- *YES, on certain operations,* ☐
- *NO, activities started,* ☐
- *NO.* ☐

Comment:...

b) Internal control is adapting to the changes in the entity and the environment.

- *YES, on all operations,* ☐
- *YES, on majority of operations,* ☐
- *YES, on certain operations,* ☐
- *NO, activities started,* ☐
- *NO.* ☐

Comment:...

c) The entity has provided for internal auditing.

- *YES, on all operations,* ☐
- *YES, on majority of operations,* ☐
- *YES, on certain operations,* ☐
- *NO, activities started,* ☐
- *NO.* ☐

Comment:...

d) The internal audit recommendations are properly addressed.

- *YES, on all operations,* ☐
- *YES, on majority of operations,* ☐
- *YES, on certain operations,* ☐
- *NO, activities started,* ☐
- *NO.* ☐

Comment:...

e) The findings of the Supreme Audit Institution are properly addressed.

- *YES, on all operations,* ☐
- *YES, on majority of operations,* ☐
- *YES, on certain operations,* ☐
- *NO, activities started,* ☐
- *NO.* ☐

Comment:..

Annex 1b – Instructions for Internal Control Self Assessment

The following instructions should assist the staff to assess the current status of FMC.

1. Control Environment

1.1 Integrity and ethical values

a) There is a Procedure to ensure that all the employees are acquainted with the code of conduct of civil servants.

The answer is YES if employee signs the work contract that includes ethical code stipulations or refers to the existing obligatory ethical code.

It is a good practice that employees are officially informed about the ethical code and ethical behaviour of a civil servant. The good practice is recommended but doesn't influence the answer.

b) Entity's specific operations adapted code of conduct is adopted.

It is a good practice and it is recommended that entities with specific operations for which the general ethical code doesn't satisfy the needs (police, army, tax or customs office) or there are specific groups of employees (sportsmen,..) have an additional specific ethic code.

However this is not necessary for the majority of entities. The entities that have this specific code answer with YES, others don't reply. Specific professional ethic codes (auditors) are not taken into consideration as they must be respected by professionals according to specific legislation.

Even the highest functionaries should be submitted to specific ethical codes (ministers, secretaries) which they sign at the occasion of their nomination.

c) Employees sign to adhere to the general code of conduct of civil servants and to the specific code of conduct when existing.

It is not enough that employees are informed about the code of conduct. The answer YES is possible when employees sign and confirm adherence to the code.

A good practice is regular (annual) discussion regarding the code of conduct and the adherence to it with practical examples. The good practice is recommended but doesn't influence the answer.

d) Sanctions are foreseen in case of non adherence of employee to the code of conduct or of non respect of laws, regulations, guidance and instructions of the superiors.

Such cases are formally regulated by legislation. The practical implementation of the legislation and the treatment of such cases mostly depend upon the head of the entity. It is important that the head of the entity adopts internal acts regarding the cases of infringement of the code of conduct and act accordingly expressing the zero tolerance for unethical behaviour, fraud and corruption.

Answer yes can be given if entity has such internal acts or instructions that can have as well forms of minutes of the meetings of the management with decisions.

e) Sanctions in case of non adherence of employee to the code of conduct or of non respect of laws, regulations, guidance and instructions of the superiors are strictly implemented.

Only two answers are possible YES (for all operations) or NO. The answer YES is possible in case of a practical example of such a case with the impact (disciplinary *measure, termination of the work contract, additional training, and change of organisational structure or process) if there were no such cases in the past year, the entity doesn't answer.*

1.2 Human resources policies and procedures

a) The entity has for the achievement of the mission and the objectives appropriate and with the regulations compliant systemisation that is continuously updated.

The systemisation is appropriate when compliant with acts, regulations and needs of the entity enabling it to fulfil the mission and objectives. (Indicate the date of the last updating regarding the change in regulations, change of objectives or processes).

b) Human resources policy exists and assures the recruitment of appropriate candidates.

The answer YES is possible when document exists (instructions, human resources plan, and strategy) as a demonstration of the policy.

c) The criteria for the assessment of the effectiveness of human resources/recruitment exist and are regularly used?

For the measurement of human resources objectives achievement, criteria must be developed (objectives achievement, achievement of the human resources strategy, of the recruitment plan)

d) The recruitment commission is appointed according to the adopted internal procedure. It prepares in advance the recruitment selection criteria.

The answer YES is possible when the internal procedure is strictly employed.

e) For every employee expected individual results are identified and represent criteria for employee performance assessment and bonus.

The answer YES is possible when individual objectives are clearly identified, that support objectives of the organisational unit, and that of the entity. The individual performance is measured upon the achievement of individual objectives

f) Employee's performance is assessed on regular basis.

The answer YES is possible, when the assessment of individual performance is done in compliance with regulations and for all employees.

g) Employees are assured continuous professional training.

The answer YES is possible when the continuous professional development is done in accordance with the plan adopted by the head of the entity on the basis of needs, which is financially evaluated and included in the budget.

h) For the entity a plan for continuous professional development of employees is adopted and responsible person appointed for the coordination of the preparation, needs coordination and efficient and effective implementation.

The answer YES is possible, when responsible person is appointed, in charge of the implementation and follow up of the continuous professional development plan.

A good practice is the identification and analysis of needs for continuous professional development at all organisational levels, identification of less successful areas, expressing needs for improvement, evaluation of possible professional development and identification of best measures. The lack of proper needs identification and their analysis doesn't help improve the performance but represents waste of resources.

Often, the entity doesn't have continuous professional development strategy, identifying standards, preferences, objectives. Management at all levels is not obliged and involved in this process, there is no follow up regarding the specific methods of training and education and their impact on better operations of the entity.

1.3 Management philosophy and methods

a) The head of the entity and management at all levels is aware of the advantages of risk management, internal control and internal auditing for the achievement of mission and objectives.

The answer is purely subjective.

b) The head of the entity and management at all levels plan their activities for the achievement of objectives.

The answer YES is possible when the activities for the achievement of objectives are translated to the tasks of the head of the entity and managers in documents (minutes, action plans, programs)

c) The head of the entity and the management meet and discuss the achievement of objectives.

The answer YES is possible if the achievement of objectives follow up is a continuous planed process (meetings, reports to the management),

1.4 Organisational structure

a) The organisational structure, authorities and responsibilities of employees are clearly defined and included in internal acts.

The answer is largely subjective and based on the assessment of the head of the entity regarding the everyday management, e.g. unclear responsibilities and authorities of the employees.

(Act on internal organisation and systemisation of work posts, written delegations, instructions, manual)

b) For the achievement of the objectives required activities, actions and tasks are identified an attributed to appropriate work posts.

This question is more detailed that the precedent. It can happen that certain operational tasks are not clearly defined or not included in the description of work post.

c) For each action/task a responsible employee is identified.

Work post should be occupied by appropriately qualified employee with clearly defined authorities and responsibilities, restrictions

d) The number, education and skills of employees satisfy the needs for the achievement of objectives.

1.5 Responsibility

a) A reporting system regarding the risk management, internal control and internal audit to the head of the entity and to the management at all levels is set up.

Regular reporting is in written form. The reporting obligation must be fixed in writing.

The obligation of reporting is not valid only for internal audit but for all appointed by the head of the entity within his responsibility to manage risks. (Internal audit reports, reports by FMC Manager, reports on implementation of measures, reports on objectives achievement,…)

2. Risk Management

2.1 Objectives: The public entity must set clear objectives that are inter compatible and support the strategy of the public entity and the budget. The objectives must be measurable, and management should inform the employees regarding the objectives.

a) Long term objectives are set and documented.

The answer should refer to documents, i.e. mission, strategy.

b) Short term objectives are set and documented.

The answer should refer to indicated documents. Objectives must be understandable, measurable, achievable, and appropriate and time defined.

c) Short term objectives support the achievement of long term objectives.

Compliance with long term objectives should be assured. The objectives setting procedure should assure such compliance.

d) Employees are aware of long term and short term objectives.

When answering with YES refer to documents that support this, e.g. meetings minutes, annual meetings, ..)

e) Criteria are set for the measurement of the achievement of objectives.

With objectives identification, criteria for the measurement of the achievement should be identified too. When answering, refer to documents supporting the answer.

f) The entity monitors the achievement of objectives and analyses reasons in case of non achievement.

Regular monitoring means at least monthly reporting of progress and the implementation of corrective measures.

2.2 Risks related to objectives: The public entity sets a system for the identification, analysis and control of risks.

a) Risks are identified?

Refer to documents supporting your answer. The supporting document can be risk register, minutes of meetings and other documents.

b) Risks are analysed.

To each identified risk, probability of occurrence and impact should be attributed. Refer to appropriate documents.

c) The risk response is set and internal control identified.

For each identified risk control measure should be attributed taking into account costs and advantages. Refer to appropriate documents. (Risk registers, internal instructions, work post description, trainings,)

d) The entity identifies and monitors identified risks in a systematic way.

As objectives and risks change a procedure must be in place for the updating of risk register and responsible persons appointed.

e) Risk register is regularly assessed and updated.

The procedure in place should ensure regular updating of the risk register.

f) Effectiveness and efficiency of internal control is assessed.

The internal control provides no assurance without regular assessment. Systematic assessment can be provided by internal audit.

g) The system is set that assures employees the information on risks of their concern.

Your answer should refer to documents that support it (minutes of meetings, instructions, and communications)

3. Control Activities

a) Processes are documented in detail with descriptions of flow of documents, points of decision and internal controls.

Principal processes are:
- *execution of basic tasks,*
- *public procurement, commitments, grants, transfers, payments,*
- *planning, accounting, reporting,*
- *IT,*
- *human resources, wages..*

Principal processes of the entity should be based on written internal acts, regulations, instructions, standards,… and available to employees concerned. Written procedures must be updated and employees must be provided with latest editions.

b) Detailed descriptions of processes and operations are available to the employees.

The internal organisational chart with work posts description is not enough. For each work post a specific written description of tasks that are part of the process, clearly identified in chart flow as well as the precedent and following tasks and flow of documents.

c) There are written operations instructions for every work post.

Available operations descriptions for each work post should satisfy the needs of every employee to perform his work.

d) Operation instructions include internal control.

Operation descriptions should include internal controls and their procedures descriptions. Control procedures should consider internal control criteria, e.g. segregation of duties, double signature, ex post control, evidence of non standard procedures, continuity of execution, employee rotation, supervision,…

e) Segregation of duties: the same employee cannot perform following tasks: initialisation, authorisation, execution in evidencing?

In case that segregation of duties is not possible, economical or appropriate for different reasons, other controls should be implemented, e.g. double signature, ex post control

f) Internal acts, process descriptions, operation instructions, organisation charts are regularly updated.

An internal control procedure should exist assuring that procedures are continuously updated and employees dispose of the most recent edition. Individuals must be appointed are responsible for updating of written procedures, processes and organisational charts.

g) Accounting system includes accounting controls.

Accounting controls are e.g. reconciliation of different forms of evidencing the same information or event, control of order of precedence, control of timely evidencing, control of sets of documents,…

h) Access to data and evidences is controlled.

To access IT, written procedure should exist for requesting passwords to be changed on regular basis. Authorities of employees to access to different documents should be set as well as follow up of access of documents, safeguarding of information and respect of confidentiality in compliance with regulations.

i) Supervision: Management supervision procedures are implemented

Management and supervision controls are performed by management and appointed employees in order to obtain assurance that controls set are implemented as foreseen.

4. Information and Communication

a) The head of the entity and management at all levels receive reliable, relevant, timely and sufficient information (summaries, analytical, reports on exceptions, special information,..), to take necessary decisions.

The answer is based upon the judgment of the head of the entity.

b) Information enables the head of the entity and management at all levels to monitor the achievement of objectives and operations supervision.

The head of the entity base his answer upon the methods and means that enable him and the management to follow up the realisation of objectives and control over operations of the entity.

c) Information and communication system adapts to the changes in the entity, objectives and strategy

The answer is based upon the documentation regarding changes and instructions regarding corrective measures.

d) The effective and efficient system of communication assures that employees receive necessary information for their work.

Difficulties regarding the operations owing to the lack of information should be considered. Management should consult employees.

e) Employees assure constructive follow up to the complaints of other organisational units or external clients.

Procedure for follow up of complaints and improvements should be in place.

f) The head of the entity and management are informed with the extent and contents of complaints.

Procedure should assure that the head of the entity and managers are informed about complaints and their follow up.

g) Employees have means to report on irregularities and problems and submit suggestions for improvements.

Procedure should enable employees to report on irregularities and problems and submit suggestions for improvements

5. Monitoring

a) The entity has set up a system of regular assessment of risk management and internal control.

A procedure that the head of the entity and management are informed about the performance and weaknesses of internal control should be in place. The procedure is an integral part of the risk management.

b) Internal control is adapting to the changes in the entity and the environment.

The changes of objectives, internal and external environment are dealt on meetings on regular basis and risk register is updated accordingly.

c) The entity has provided for internal auditing.

The entity should have internal auditing assured on regular basis. External auditing, inspections and reviews of Supreme audit institution cannot be considered as internal auditing

d) The internal audit recommendations are properly addressed.

The head of the entity should properly address the recommendations of internal audit. If not, internal audit should have the possibility to inform independent control body, e.g. CHU.

e) The findings of the Supreme Audit Institution are properly addressed

The answer YES is based on the report of the Supreme audit institution that the entity has correctly addressed all the recommendations.

Annex 2a – Risk Register Template

Public entity	**Risk Register**	
	Last reviewed:	
	Signature:	

Ref.	***Risk description***	***Risk category***	***Risk analysis*** *Probability*	*Impact*	*Total*	***Treatment***	***Risk owner***	***Delay***	***Observation***

Annex 2b - Instructions for establishing a Risk Register

1. On the basis of the Law on Public Internal Financial Control (PIFC); the Rulebook on the manner and procedure for the establishing and implementing PIFC and Guidelines on internal control the head of the public entity adopts this regulation referring to the setting up and maintaining the risk register.

2. Every public entity serves for a purpose that it fulfils with the achievement of objectives. The objectives can be divided in specific regarding the delivery of goods and services and general regarding the conduct of the public entity and its member's i.e.

- Executing orderly, ethical, economical, efficient and effective operations,
- Fulfilling accountability obligations,
- Complying with applicable laws and regulations,
- Safeguarding resources against loss, misuse and damage.

Other general objectives are represented in the description of the entity's mission, the realisation of which depends upon the achievement of the specific and operational objectives represented in long and short term plans at the level of the entity, organisational units, functions and work posts. Objectives must be realistic, measurable and time dependent. For each objective criterion for the measurement of the achievement must be developed.

Most crucial objectives are together with the indicators for the measurement of their achievement represented in the budget documents.

3. Risk is an uncertainty of the materialisation and of the impact of an event that may influence the achievement of an objective. Risks can be categorised upon different criteria i.e.:

- General and specific with relation to general and specific objectives,
- External and internal regarding their resource from outside or inside of the public entity,
- Risks related to politics, security, human resources, economy, finances, and other,.

The entity decides the most appropriate risk categorisation that enables the transparency and effective risk management e.g.:

External:

- political
- budgetary
- legislation,
- specific.

Internal:

- Respect of deadlines,
- Quality assurance,
- IT
- General

4. Risk is analysed and evaluated taking into account the probability of occurrence and the possible impact or impact on the entity. Risk must be evaluated without considering the measures already adopted for its control at a tolerable level.

For risk evaluation different scales are possible, i.e.□ ,

Risk probability:

✓ unlikely
✓ possible,
✓ very possible,
✓ highly possible.

Risk impact:

✓ insignificant,
✓ significant,
✓ very significant,
✓ disastrous.

All identified risks must be evaluated against the same scale and criteria.

5. The risk analysis serves for risk prioritisation from the most to least important risk and the list of risks represents the entity's risk exposure.

6. The responsibility for the risk control rests with the head of the entity. He decides the acceptable level for each risk and approves the measures to be undertaken for risk control. and appoints risk owners.

7. The risk register represents risks, their description, their importance according to the probability of the occurrence and the impact, risk owners and measures for their control. As the environment and objectives change, risk change and the risk register must be regularly discussed and updated.

8. The risk identification and risk analysis in the entity is performed at the level of the entity and at the level of organisational units under the responsibility of heads of units taking into consideration.

- Objectives setting
- Achievement of objectives included in the long and short term budgets,
- Legality of operations,
- Economy, efficiency and effectiveness,
- Reliability and timeliness of reporting,
- Protection of resources against misuse,

- Internal and external information (internal audit, Court of Audit, European Commission, European Court of Audit)
- Risks occurred and their impact,
- Any other information indicating internal and external risks.

9. For each specific risk the head of the unit fills in the risk description and send it to the FMC Manager, who checks it on completeness and prepare it for the submission to the head of the entity. Upon the approval the risk is entered in to the risk register.

10. The risk register is examined at least twice per year by the head of the entity and the highest management, or upon proposal of the head of the organisational unit, FMC Manager or internal auditor.

Risk Description				
Organisational unit:		***Responsible:***	***Last reviewed:***	
Objective:				
Ref.:		***Risk category:***		

Risk description:		
	Analysis:	***Score:(1-4)***
Probability :		
Impact:		
Total:	*(Probability X Impact)*	
Decision taken:		
Measures:		
	Delay:	
Comments:		
Risk control assessment:		

Signature:

Risk category	
Risk category	***Risk description***
External risk:	*The entity cannot influence these risks, control measures can be implemented*
○ *political*	*Change of priorities, objectives, support.*
○ *budgetary-financial*	*Availability of resources, recruitment,*
○ *legislative*	*Adoption of legislative acts influencing the existence and performance of the entity, mission, tasks*
○ *special tasks*	*Attribution of additional not planned task, that exceed the capacities or authorities of the entity*
Internal risk:	*Entity can influence risks or avoid them at setting the objectives or implement measures for control*
○ *respect of deadlines*	*Certain tasks and deadliness are legally imposed or included in contracts*
○ *quality assurance*	*Public entity must assure quality public services to its customers and demand the same from suppliers*
○ *Information technology*	*The reliability of functioning and information protection is crucial for the work of the entity,*
○ *General*	*Compliance with regulations, safeguarding of resources, economy, efficiency, efficiency, reputation*

Risk evaluation scale	
Likelihood of Occurrence	***Score***
Unlikely, very rare events	*1*
Possible, the risk can occur in medium term	*2*
Very possible, the risk can occur often in medium term	*3*
Highly possible, the risk can occur often in short term	*4*
Impact	**Score**
Insignificant, the reputation is not influenced, no judicial impact, performance and mission are not threatened, negligible financial loss,	*1*
Significant, short term reputation damage, need of organisational changes, considerable financial loss,	*2*
Very significant, long term reputation loss, change of plans needed, reorganisation needed, substantial financial loss,	*3*
Disastrous, loss of trust in the mission and performance, high financial loss, lives endangered,	*4*

Annex 3a - Human Resources Risk Identification

Objectives	Risks	Process	Risk owner
Transparent and legal recruitment to satisfy the entity's needs	Lack of appropriate human resources to achieve entities objectives Recruitment non complying with entities needs Non transparent recruitment Fraud Non compliance with budget Contract not compliant with regulations	Human resources needs identification	
		Recruitment plan preparation	
		Recruitment plan approval	
		Determination of recruitment procedures	
		Public tender	
		Reception of applications	
		Candidates selection	
		Drafting the work contract	
		Signing the work contract	
		Wage assignment	
		Entering the work contract in Human Resources	
		Entering the work contract in Payroll	
The performance is evaluated, reported and remunerated	Lack of motivation Conflicts Fraud Bad performance Non achievement of objectives	Regular evaluation of performance	
		Ex ante check of available performance related funds	
		Signature of performance evaluation	
		Entering of data into Human Resources	
		Entering of data into Payroll	
The wage and contributions are correctly calculated and paid	Non compliance with the contract No performance evaluation included The payment on the wrong account Taxes and contributions are not paid Fraud - Ghost wages	Compliance assessment with Human Resources	
		Calculation of wages	
		Calculation of performance related wages if applicable	
		Calculation of compensations	
		Calculation of taxes and contributions	
		Checks of confirmations of payments	
The work contract is legally terminated, the follow up assured and payments stopped	The replacement work contract is not signed and the entities objectives will not be achieved The due restitutions are not done The end of contract is no entered in Human Resources and Payroll The wage payments are not stopped	Accept the end of the contract	
		Validated the due obligations	
		Enter the end of the contract in HR	
		Enter the end of the contract in payroll system	

Annex 3b – Public Procurement Risk Identification

Objectives	Risks	Process	Risk owner
Preparation of the Public procurement plan in compliance with entities objectives and legislation	Noncompliance with the legislation Noncompliance with the budget Noncompliance with entities needs	Identification of needs in relation to objectives	
		Systemisation of needs and prioritisation	
		Preparation of procurement plan	
		Validation of procurement plan	
		Report on realisation of procurement plan	
The transparent selection of supplier in compliance with regulations	Non compliance with regulations Fraud and corruption No achievement of objectives Additional costs Delays	Initiation of the public procurement procedure	
		Validation of the public procurement procedure	
		Preparation of tender documents	
		Invitation of Tenderers	
		Reception of the offers	
		Selection of the supplier	
		Signature of the contract	
The goods are supplied /services delivered in compliance with the contract	Noncompliance with the contract Noncompliance with the budget Conflict with supplier Fraud No achievement of objectives	Preparation of the order	
		Validation of the order	
		Control of the goods/services delivered	
		Control of the deliveries with the order	
		Confirmations of the reception	
		Communication to the financial services	
The supplier is paid, warranty is assured	Payment is not in compliance with the contract The same invoice is paid more times Hidden errors	Confirmation of the invoice in compliance with the contract, order and receipt	
		Preparation of the payment order	
		Filing of the payment	
		Updating the public procurement plan	