Internal Audit and Investigations Department

Risk Management Procedures Manual

Integrating Risk Management in day-to-day operations and decisions

Version 1

December 2015

Internal Audit and Investigations Department, Cabinet Office, Office of the Prime Minister, Valletta Buildings, Lower Ground Floor, South Street, Valletta VLT 1103 Malta. Telephone: (356) 21237737 Facsimile: (356) 21237681 E-mail: info.iaid@gov.mt

Contents

Glossary of Key Terminology[1]

Assurance Services
An objective examination of evidence for the purpose of providing an independent assessment on governance, risk management and control processes for the organisation. Examples may include financial, performance, compliance, system security and due diligence engagements.

Conflict of Interest
Any relationship that is, or appears to be, not in the best interest of the organisation. A conflict of interest would prejudice an individual's ability to perform his or her duties and responsibilities objectively.

Control
Any action taken by management, the board and other parties to manage risk and increase the likelihood that established objectives and goals will be achieved. Management plans, organises and directs the performance of sufficient actions to provide reasonable assurance that objectives and goals will be achieved.

Control processes
The policies, procedures (both manual and automated) and activities that are part of a control framework, designed and operated to ensure that risks are contained within the level that an organisation is prepared to accept.

Enterprise Risk Management[2]
Enterprise risk management is a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.

Fraud[3]
Fraud affecting the European Communities' financial interests shall consist of:
(a) in respect of expenditure, any intentional act or omission relating to:

- the use or presentation of false, incorrect or incomplete statements or documents, which has as its effect the misappropriation or wrongful retention of funds from the general budget of the European Communities or budgets managed by, or on behalf of, the European Communities;
- non-disclosure of information in violation of a specific obligation, with the same effect; and
- the misapplication of such funds for purposes other than those for which they were originally granted.

(b) in respect of revenue, any intentional act or omission relating to:

[1] Source: Chartered Institute of Internal Auditors
[2] Source: Committee of Sponsoring Organizations of the Treadway Commission *Enterprise Risk Management – Integrated Framework* Executive Summary, September 2004 Available Online: http://www.coso.org/documents/coso_erm_executivesummary.pdf
[3] Source: CONVENTION Drawn up on the basis of Article K.3 of the Treaty on European Union, on the protection of the European Communities' financial interests

- the use or presentation of false, incorrect or incomplete statements or documents, which has as its effect the illegal diminution of the resources of the general budget of the European Communities or budgets managed by, or on behalf of, the European Communities;
- non-disclosure of information in violation of a specific obligation, with the same effect; and
- misapplication of a legally obtained benefit, with the same effect.

Governance
The combination of processes and structures implemented by the board to inform, direct, manage and monitor the activities of the organisation toward the achievement of its objectives.

Residual Risk
The risk remaining after management takes action to reduce the impact and likelihood of an adverse event, including control activities in responding to a risk.

Risk
The possibility of an event occurring that will have an impact on the achievement of objectives. Risk is measured in terms of impact and likelihood.

Risk appetite
The level of risk that an organisation is willing to accept.

Risk management
A process to identify, assess, manage and control potential events or situations to provide reasonable assurance regarding the achievement of the organisation's objectives.

1. Background

Introduction

1.1 This procedures manual is to be followed for integrating Risk Management in day-to-day operations and decisions.

Risk Management

1.2 With the development of Public Service Agreements and the setting of objectives the identification of risks is essential to ensure the achievement of those objectives. Risks need to be managed and controlled to ensure the chances of success are maximised.

1.3 Risk management is one aspect of an organisation's system of internal control and has a key role in the management of risks that are significant to the fulfilment of objectives.

1.4 The purpose of risk management is to manage and control risks, not eliminate them. Risk can be defined as:

"The uncertainty of outcome, whether positive opportunity or negative threat, of actions and events."[4]

A risk has to be assessed in respect of the combination of the likelihood of something happening, and the impact which arises if it does actually happen. Risk management includes identifying and assessing risks and responding to them. In short, risk management can be seen as the process of analysing risk exposure[5] and an attempt to minimise it through various means.

1.5 Enterprise risk management (ERM) deals with risks and opportunities affecting value creation or preservation. ERM consists of eight interrelated components. These are derived from the way management runs an enterprise and are integrated with the management process.

These components are:

• *Internal Environment* – The internal environment encompasses the tone of an organisation, and sets the basis for how risk is viewed and addressed by an entity's people, including risk management philosophy and risk appetite, integrity and ethical values, and the environment in which they operate.

• *Objective Setting* – Objectives must exist before management can identify potential events affecting their achievement. Enterprise risk management ensures that management has in place a process to set objectives and that the

[4] HM Treasury (2004) The Orange Book, Management of Risk-Principles and Concepts.
[5] The consequences, as a combination of impact and likelihood, which may be experienced by the organisation if a specific risk is realised.

chosen objectives support and align with the entity's mission and are consistent with its risk appetite.

• *Event Identification* – Internal and external events affecting achievement of an entity's objectives must be identified, distinguishing between risks and opportunities. Opportunities are channelled back to management's strategy or objective-setting processes.

• *Risk Assessment* – Risks are analysed, considering likelihood and impact, as a basis for determining how they should be managed. Risks are assessed on an inherent and a residual basis.

• *Risk Response* – Management selects risk responses – avoiding, accepting, reducing, or sharing risk – developing a set of actions to align risks with the entity's risk tolerances and risk appetite.

• *Control Activities* – Policies and procedures are established and implemented to help ensure the risk responses are effectively carried out.

• *Information and Communication* – Relevant information is identified, captured, and communicated in a form and timeframe that enable people to carry out their responsibilities. Effective communication also occurs in a broader sense, flowing down, across, and up the entity.

• *Monitoring* – The entirety of enterprise risk management is monitored and modifications made as necessary. Monitoring is accomplished through ongoing management activities, separate evaluations, or both.[6]

[6] Source of Section 1.5: Committee of Sponsoring Organizations of the Treadway Commission *Enterprise Risk Management – Integrated Framework Executive Summary*, September 2004 Available Online: http://www.coso.org/documents/coso_erm_executivesummary.pdf

1.6 The Risk Management model below highlights the process necessary if risk management is to be effective. The model illustrates how the risk management process is not isolated, but takes place in a context; and, how certain key inputs have to be given to the overall process in order to generate the outputs which will be desired to manage risks.

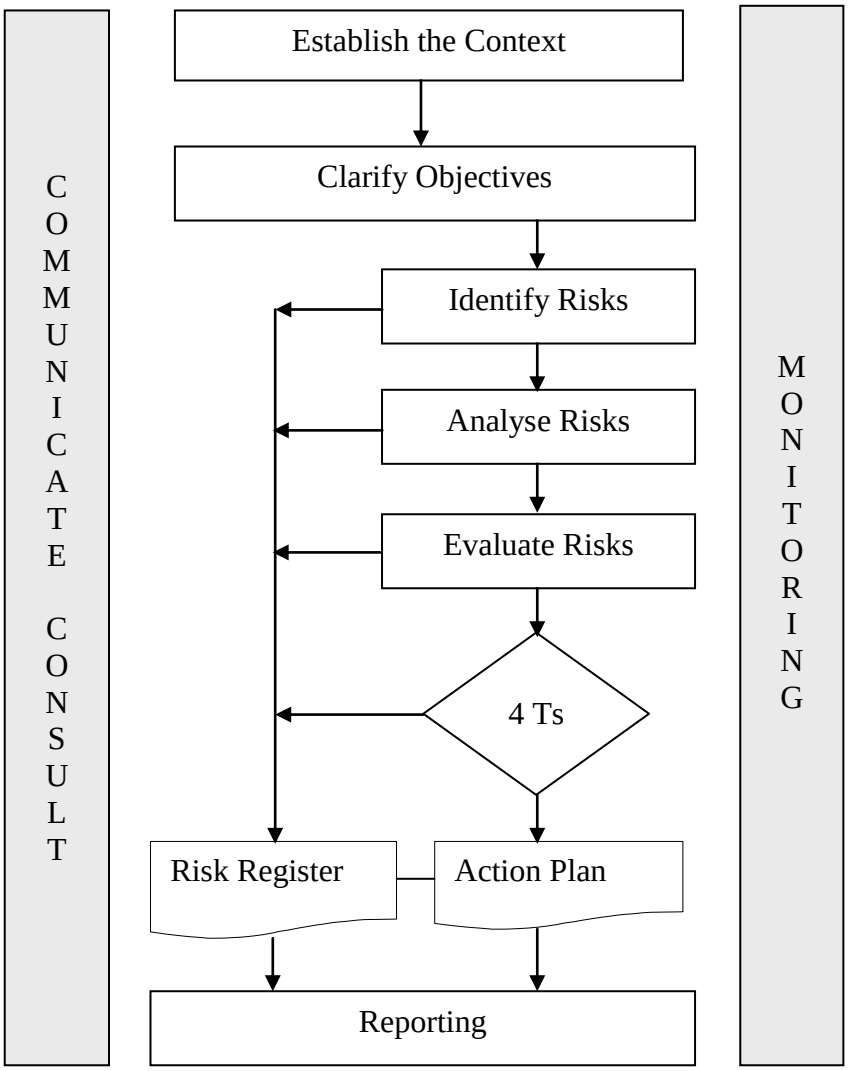

Figure 1 – Risk Management Process[7]

2. Step 1: Establishing the Context and Identifying Objectives

2.1 The first step in the risk management process is to establish the "context" within which the activity is being conducted and risks may arise. The focus will be on obtaining information about the planned activity i.e. fulfilling an objective.

[7] Diagram reproduced courtesy of kind consent from Stephen Maycock, 2015

2.2 Clarify objectives – these need to be specific, measurable, attainable, realistic and timely (SMART)[8]:

2.2.1 **Specific:** A specific objective should be concrete, detailed and well defined so that one knows where he/she is going and what to expect when he/she arrives. A specific objective provides an answer to the following questions:

- Who: Who is involved?
- What: What do I want to accomplish?
- Where: Identify a location.
- When: Establish a time frame.
- Which: Identify requirements and constraints.
- Why: Specific reasons, purpose or benefits of accomplishing the goal.

2.2.2 **Measurable:** Establish concrete criteria for measuring progress toward the attainment of each objective you set. Numbers and quantities provide means of measurement and comparison. The objective needs to provide an answer to the following questions:

- How much? How many?
- How will I know when it is accomplished?

2.2.3 **Attainable:** Most objectives can be reached if there is adequate planning, including time considerations.

2.2.4 **Realistic:** The objective must represent an objective towards which you are both *willing* and *able* to work. Considers constraints such as resources, personnel, cost, and time frame

2.2.5 **Timely:** An objective should be grounded within a time frame.

T can also stand for Tangible – An objective is tangible when you can experience it with one of the senses, that is, taste, touch, smell, sight or hearing. When the objective is tangible, there is a better chance of making it specific and measurable and thus attainable.

2.3 Objectives are to be defined for the following categories:

2.3.1 *Strategic Objectives* – high-level goals, aligned with and supporting its mission

2.3.2 *Operations Objectives* – these pertain to the efficient and effective use of resources and efficiency and effectiveness of the entity's operations:

- Operational and financial performance goals (including consideration of outputs and customers);
- Staff Learning and Growth; and

[8]References: http://topachievement.com/smart.html and http://www.cdc.gov/phcommunities/resourcekit/evaluate/smart_objectives.html

- Safeguarding assets against loss.

2.3.3 *Reporting Objectives – reliability of reporting*:

- Internal and external financial and non-financial reporting (may encompass reliability, timeliness, transparency, or other terms as set by regulators, recognised standard setters, or the entity's policies);

2.3.4 *Compliance Objectives*:

- Adherence to the applicable laws and regulations

The objectives defined are then checked in regards to their validity. Furthermore an understanding of aspects such as the following aspects is also required:

- Who are the stakeholders and what are their objectives?
- Where the activity fits in relation to the aims and objectives of the organisation?
- What assumptions have been made regarding the business objectives and how they will be fulfilled?
- The financial and Human Resources conditions within which it operates;
- The technology that is currently used to perform the activity; and
- The involvement of other Government departments, partner organisations or sponsored bodies.

3. Step 2: Identifying Risks

Inherent Risk

3.1 When the context has been determined and the objectives have been defined, the next step in the process is to identify the "inherent" risks to the activity that would reduce or remove the likelihood of meeting the objectives while maximising the opportunities that could lead to improved performance.

3.2 Inherent risks can be described as the exposure arising from a specific risk before any action has been taken to manage it. In other words the effect, in terms of likelihood of occurrence and impact of the risk on objectives in the event that no control actions are in place.

3.3 A risk consists of the probability of a perceived threat occurring and the magnitude of its impact on objectives. Within this definition, "Threats" could have a negative impact on objectives.

3.4 The most popular technique used at this stage is a *Risk Identification Workshop*. In practical terms this may mean a divisional meeting focused on discussion of its objectives and what risks, both threats and opportunities, may arise.

Tools that can be used at the workshop include Risk Checklists or Risk Prompt Lists, which provide categories of risks and an in-house list of risks that were identified or occurred during previous organisational activities. A Risk

Checklist permits managers to capture lessons learned and assess whether similar risks are relevant to current activities. Such checklist should be used as a means of kick starting and facilitating discussions on risks which may impact on the achievement of business objectives.

3.5 It is important that all staff involved in the activity participate in the "Risk Identification" stage, as without their knowledge and experience risks may be missed. Staff involved in actively using systems and processes will be more acutely aware of the risks that are likely to be encountered when conducting an activity.

3.6 Risks are to be clearly defined and not described in general terms. Only in this way it can be ensured that the precise nature of the risk is understood and action could be taken thereon.

4. Step 3: Analysing Risks

Likelihood/Impact

4.1 Once the inherent risk has been identified and understood the next step is to assess the "likelihood" of its occurrence and its potential "impact" on objectives. In each case, the potential impact should be related back to the relevant objectives at the appropriate level.

4.2 This Risk Assessment[9] is of a qualitative nature based on knowledge and experience in the particular area. When making an assessment it is important that decisions are not influenced by the perceived acceptability of a risk and how Senior Management are likely to react.

Assessing the Likelihood/Impact of an Inherent Risk

4.3 The likelihood of the inherent risk being realised before controls are in place, will be expressed in terms of Very Likely (VL), Likely (L), Medium (M), Unlikely (U) and Very Unlikely (VU) using the definitions below:

- **VL:** There is a strong likelihood that the risk will be realised;
- **L:** The risk is more likely to occur than not;
- **M:** There is a reasonable chance that the risk will be realised;
- **U:** The risk in unlikely but not impossible to occur; and
- **VU:** There is relatively little chance of the risk being realised.

4.4 The impact of the inherent risk on the achievement of objectives, before controls are in place, will be expressed in terms of High (H), Medium/High (MH), Medium (M), Low/Medium (LM) or Low (L) using the definitions below. In quantum terms they should be relative to the achievement of the objective:

[9] The evaluation of risk with regards to the impact if the risk is realised and the likelihood of the risk being realised.

- **H:** major loss; death; key deadlines missed; very serious legal concerns (e.g. high risk of successful legal challenge, with substantial implications for the Department); major environmental impact; loss of public confidence;
- **MH:** Likely to cause major operational changes in many areas of the organisation;
- **M:** significant loss; significant public health effects; deadlines renegotiated with customers; potentially significant legal implications (e.g. risk of successful legal challenge); significant environmental impact; longer-term damage to reputation;
- **LM:** Likely to cause minor loss in many areas of the operation; and
- **L:** low/medium losses; minor or reversible health effects; reprioritising of delivery required; minor legal concerns raised; minor impact on the environment; short-term reputation damage.

Risk Appetite

4.5 A risk should be assessed in relation to the risk appetite of that particular strategic, programme, project or operational activity. Risk appetite can best be expressed as a series of boundaries which give clear guidance on the limits of risk which can be taken. Each activity will have boundaries, determined by matters such as legislation, regulations, policies, procedures and available human and financial resources.

5. Step 4: Evaluating and Responding to Risks

Risk Response – Introduction of the necessary controls

5.1 The primary goal of this step is to prepare and implement specific management responses to the threats and opportunities identified. Ideally this will be to reduce or remove the threats and to maximise the opportunities. At this stage consideration will need to be given to the risk appetite as this may determine what steps are taken to address the risk.

5.2 There are four methods of addressing risk, being:

- **Tolerate** – 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.
- **Transfer** – For some risks the best response may be to transfer them. This might be done by conventional insurance.
- **Treat** – By far the greater number of risks will be addressed in this way. The purpose of treatment is that whilst continuing with the activity giving rise to the risk, action (control) is taken to constrain the risk to an acceptable level.
- **Terminate** – Some risks will only be treatable, or containable to acceptable levels, by terminating the activity.

5.3 In practical terms this means identification of the controlling actions or activities that will lessen the likelihood or impact of the risk materialising or remove the risk completely.

5.4 Identified controls that are already in place are classified as 'Current Controls'. When these are determined an assessment must be made by Management as to whether or not they are deemed adequate. If they are, then there may not be a need for any further actions other than routine monitoring of the risk.

Residual Risk

5.5 The 'residual risk' is what remains after considering the relevant controls. The residual risk is the assessment in terms of likelihood and impact of the risk, taking account of the controlling actions that have been put in place.

5.6 The steps described for "*assessing the Likelihood/Impact of an Inherent Risk*" should now be repeated; only this time taking account of the controls that have been put in place.

5.7 If the controls are deemed inadequate, there are two options:

- Accept the risk – linked to the Tolerate section; or
- Not accept the risk and identify further 'Actions to improve control'.

5.8 New actions to improve control are classified as 'Actions to improve control'. These will have a date for completion and a designated person responsible for action. A new action will also have an assessed criticality, dependant on the need for the control to be in place within a certain timescale.

Risk Owner

5.9 The risk owner needs to take overall responsibility for the management of risks.

5.10 The Risk Owner will be someone responsible for the management and control of all aspects of the risks, including ensuring that individual actions identified to further strengthen control are carried out effectively.

6. Step 5: Documenting the Process

6.1 Each officer is to prepare a detailed process flowchart for each area under his/her responsibility. This diagram needs to depict all the tasks carried out in the course of deploying the day-to-day duties associated with their role. Each officer is to identify the objectives of the tasks undertaken and describe (by listing down all the steps) what is done to complete each task. The flowchart is to reflect the tasks carried out.

6.2 Subsequently, brainstorming sessions are to be held to identify risks.

Risk Register

6.3 The principle tool used for recording risks is the Risk Register (Annex A). The following risk registers will be implemented across Government:

a. *Risk Register (Corporate)*
This document records the key risks identified that need to be monitored and managed at Ministerial level.

b. *Risk Register (Public Organisational)*
This document records the key risks identified that need to be monitored and managed at Agencies, Entities and Government Department level.

c. *Risk Register (Sectional)*
This document records the key risks identified that need to be monitored and managed at Directorates, Sections, Branches, Units, etc. level.

6.4 The aim of the risk register is to capture, maintain and monitor information on all of the identified risks to a specific organisational activity and the associated controlling actions that have been identified.

6.5 The layout of the risk register reflects the sequence in which information is captured and documented and it should contain enough detail to enable risk response planning and subsequent control.

6.6 Risk registers will contain the following headings for completion:

Risks and Current Controls

- *Objective* – These are to be defined in accordance with the public organisation's operational, reporting and compliance obligations.

- *Risk Reference* – This is a numeric or alpha-numeric code unique to that particular risk. Alpha-numeric codes are to be given when risks are grouped by type;

- *Risk Description: Cause and Consequence* – The risk itself is detailed in a **cause and consequence** statement i.e. as a result of **x** (**cause**), there is a risk that **y** (**consequence**) will happen;

- *Risk Owner* – A named individual responsible for the management and control of all aspects of the risks;

- *Inherent Risk* (Probability) – The probability of the risk occurring before any controls are put in place. These are recorded using a 5 point scale of low, low/medium, medium, medium/high and high;

- *Inherent Risk* (Impact) – The potential impact on the fulfilment of the organisation's objectives before any controls are put in place. These are

recorded using the same 5 point scale of low, low/medium, medium, medium/high and high;

- *Inherent Risk (Total Risk Score)* – This is the probability of the inherent risk occurring multiplied by the impact that the inherent risk has.

- *Current Controls* – Actions that have been taken to provide a response to the inherent risk;

- *Residual Risk (Probability)* – The probability of the risk occurring after controlling actions have been put in place. These are recorded using a 5 point scale of low, low/medium, medium, medium/high and high;

- R*esidual Risk (Impact)* – The potential impact on fulfilment of the organisation's objectives after controlling actions have been put in place. These are recorded using the same 5 point scale of low, low/medium, medium, medium/high and high;

- *Residual Risk (Total Risk Score)* – This is the probability of the residual risk occurring multiplied by the impact that the residual risk has.

- *Residual Risk Acceptable (Yes or No)* – This refers to whether the residual risk is acceptable to management. If not acceptable then the next section of *"Planned Risks and Mitigating Actions*" becomes relevant.

Planned Mitigating Actions

- *Actions* – Those actions that have been identified to further reduce the likelihood or impact of the risk. Some risks may have more than one mitigating action;

- *Person Responsible for Action* – A named individual responsible for the management and control of all the new actions identified to mitigate the risk within the due date;

- *Due Date* – The time period during which the mitigation actions have to be implemented;

- *Task Status* – Whether the new actions have been implemented or not. If these were not implemented within the due date, the reason for such delay is to be noted and reviewed by the Director/Director General as appropriate. It is then the responsibility of this same Director/Director General to ensure that the necessary action is taken in this regard and with respect to that risk.

Forecast for the next 6 months

- A forecast of the risk for the next six (6) months will mobilise management to address risks in a proactive and timely manner.

Monitoring and Updating

6.6 Risk Management is a continuous process with new risks being identified and controls in place changing the likelihood and impact assessments of the risks. In this regard, the Risk Registers should be updated at least quarterly, for example, following discussions at management and team meetings. Risks should be re-ranked as necessary. Mitigating actions are to be identified and acted upon for any new risks identified.

Risk Matrix

6.7 The technique being proposed to present the assessments of the residual risks in summary format is a 5x5 grid (see Figure 2 below). This helps to visually communicate the range of severity of residual risks identified (representing a combination of likelihood and impact).

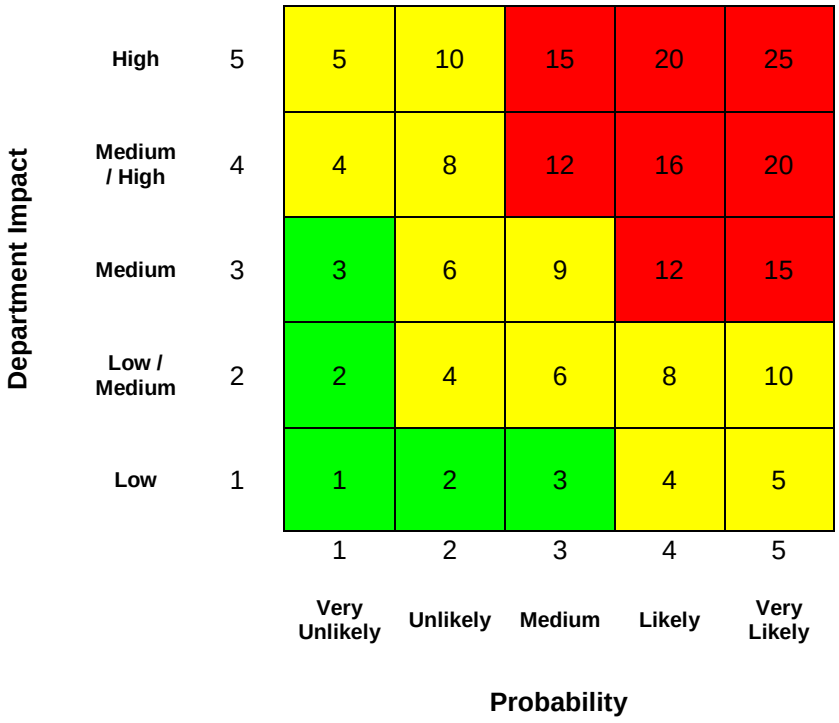

Figure 2 – Risk Matrix

Risk Tolerance and Escalation

6.8 In case when a risk cannot be dealt with at the specific level, the Risk Owner will then be responsible for either deciding a course of action or escalating the information to a more senior level. This encapsulates the 'bottom-up' side of the risk management process, where risks identified at operational level can, if appropriate, become strategic risks to the organisation.

6.9 It is also likely that some risks will be identified across two or more sections/units within a Public Organisation. Risks such as these, which are generic across a number of areas will be escalated and considered at a higher level within the organisation.

7. Components of Internal Controls to be put in place by Management[10]

It is recommended that Management puts in place the necessary internal controls. It is recommended that the system of internal control put in place complies with the criteria set out below.

It is being recommended that the internal control consists of five integrated components.

A. Control Environment

This is the set of standards, processes and structures that provide the basis for carrying out internal control across the organisation. Top Management establish the tone at the top. The control environment comprises:

a. The integrity and ethical values of the organisation;
b. The parameters within which governance oversight responsibilities are to be carried out;
c. The organisational structure and assignment of authority and responsibility;
d. The process for attracting, developing and retaining competent individuals; and
e. The rigidness governing performance measures, incentives and rewards to drive accountability for performance.

Principles drawn directly from this component:

1. The organisation demonstrates a commitment to integrity and ethical values;
2. A body independent from management need to exercise oversight of the development and performance of internal control;
3. Management establishes structures, reporting lines and appropriate authorities and responsibilities in pursuit of objectives;
4. The organisation demonstrates a commitment to attract, develop and retain competent individuals in alignment with objectives; and
5. The organisation holds individuals accountable for their internal control responsibilities in the pursuit of objectives.

[10]Source: Committee of Sponsoring Organizations of the Treadway Commission *Internal Control – Integrated Framework* Executive Summary, May 2013 Available Online: http://www.coso.org/documents/990025P_Executive_Summary_final_may20_e.pdf

B. Risk Assessment

Management specifies objectives within categories relating to operations, reporting and compliance with sufficient clarity to be able to identify and analyse risks to those objectives. Management also considers the suitability of the objectives for the entity. Risk assessment also requires management to consider the impact of possible changes in the external environment and within its own business model that may render internal control ineffective.

Principles drawn directly from this component:

6. The organisation specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives;
7. The organisation identifies risks to the achievement of its objectives across the entity and analyses risks as a basis for determining how the risks should be managed;
8. The organisation considers the potential risk for fraud/irregularities in assessing risks to the achievement of objectives; and
9. The organisation identifies and assesses changes that could significantly impact the system of internal control.

C. Control Activities

These are to be performed at all levels of the entity, at various stages within business processes and over the technological environment. They may be preventive or detective in nature and may encompass a range of manual and automated activities such as authorisations and approvals, verifications, reconciliations and business performance reviews. Segregation of duties is typically built into the selection and development of control activities.

Principles drawn directly from this component:

10. The organisation selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels;
11. The organisation selects and develops general control activities over technology to support the achievement of objectives; and
12. The organisation deploys control activities through policies that establish what is expected and procedures that put policies into action.

D. Information and Communication

Information is necessary for the entity to carry out internal control responsibilities to support the achievement of its objectives. Management obtains or generates and uses relevant and quality information from both internal and external sources to support the functioning of other components of internal control. Communication is the continual, iterative process of providing, sharing and obtaining necessary information. Internal communication is the means by which information is disseminated throughout the organisation, flowing up, down and across the entity. It enables personnel to receive a clear message from senior management that control responsibilities must be taken seriously. External

communication is twofold: it enables inbound communication of relevant external information, and it provides information to external parties in response to requirements and expectations.

Principles drawn directly from this component:

13. The organisation obtains or generates and uses relevant, quality information to support the functioning of internal control;
14. The organisation internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control; and
15. The organisation communicates with external parties regarding matters affecting the functioning of internal control.

E. Monitoring Activities

Ongoing evaluations, separate evaluations or combination of these two are used to ascertain whether each of these five components, including controls to effect the principles within each component, is present and functioning. Findings are to be evaluated against set criteria. Deficiencies are to be communicated to the appropriate levels.

Principles drawn directly from this component:

16. The organisation selects, develops and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning; and
17. The organisation evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action as appropriate.

An entity can achieve an effective internal control by applying all principles. However, the Framework recognises that while internal control provides reasonable assurance of achieving the entity's objectives, **limitations** do exist. Internal control cannot prevent bad judgement or decisions, or external events that can cause an organisation to fail to achieve its operational goals. An effective system of internal control can experience a failure. Limitations may result from the:

- Suitability of objectives established as a precondition to internal control;
- Reality that human judgement in decision making can be faulty and subject to bias.
- Breakdowns that can occur because of human failures;
- Ability of management to override internal control;
- Ability of management, other personnel, and/or third parties to circumvent controls through collusion; and
- External events beyond the organisation's control.

Management should be aware of such limitations when selecting, developing and deploying controls that minimise, to the extent practical, these limitations.

ANNEX A – SAMPLE RISK REGISTER

RISKS AND CURRENT CONTROLS													PLANNED MITIGATING ACTIONS					
					Inherent Risk				Residual Risk									
Objective Reference	Objective	Risk Ref	Risk Description: Cause and Consequence	Risk Owner	Department Impact Score	Probability Score	Total Risk Score	Current Controls	Department Impact Score	Probability Score	Total Score	Residual Risk Acceptable	Actions	Person Responsible for Action	Due Date			Task Status		Forecast Risk for the Next 6 Months
							0				0									