german
cooperation
DEUTSCHE ZUSAMMENARBEIT

giz Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH

Risk Management

Participants' Handbook
April 2014

SULGO
better lives through better services

The United Republic of Tanzania

Support to Local Governance Processes (SULGO) in Tanzania
Project: Strengthening internal controls at sub-national level

Summary Guide
Part B

Risk Management

Participants' Handbook
April 2014

Foreword

Tanzania's local government budgets account for over 25 per cent of the total national budget – and the proportion is increasing. This trend mirrors the responsibilities that have so far been transferred to LGAs over the past decade under the national decentralisation by devolution policy. At the same time, LGAs are facing ever-increasing demands for quality services and for strict adherence to regulations and transparency, pushed by, amongst others, the National Audit Office as seen in the critical audit opinions it issued to various LGAs.

The effectiveness of LGAs' internal control systems determines not only how public funds are used but also the extent to which local governments are becoming the drivers for development as they are expected to be. Further advancements in the national decentralisation process depend heavily on the way LGAs control the resources they are entrusted with. LGAs' internal control systems also play a key role with respect to the legitimacy of the state because local governments are the institutions closest to the ordinary citizens. Hence, the way the LGAs actually use their resources has a big impact on the public's opinion and perception of the performance of the government as a whole. In the context of rising tensions within a transforming society, the importance of strong LGA internal control systems cannot be overemphasized.

Several government bodies such as the Prime Minister's Office for Regional Administration and Local Government (PMO-RALG), Regional Secretariats (RSs), and the Office of the Internal Auditor General are required to capacitate LGAs in the area of internal controls. Yet, developing capacities for nearly 170 LGAs constitutes an enormous task in addition to the challenges already being encountered as the LGAs attempt to cope with recently introduced higher national standards, such as those relating to risk management or to accrual accounting.

PMO-RALG and GIZ, in close collaboration with the Office of the Internal Auditor General, launched an initiative to assist selected district, municipal and city councils and corresponding Regional Secretariats (RS) in the application of and adherence to internal controls standards and regulations. The focus of this initiative was on learning-by-doing, capacitating public servants through coaching on-the-job, and on formulating respective methods of capacity development at sub-national level.

The present book is a direct outcome of the coaching and forms part of a series that covers the four thematic areas of Accounting & Administrative Controls, Risk Management, Internal Audit and Audit Committees in the councils, as well as the backstopping role of Regional Secretariat in monitoring and evaluation of LGAs' internal controls. Each of the areas comprises two books: a participants' handbook for the public servant for reference, and a handbook for facilitators tasked with capacitating staff from LGAs or RSs.

We wish the users of the present book interesting and stimulating reading and hope that it helps to perform better their tasks.

Achim Blume

Head of GIZ Governance Programmes Tanzania

Table of contents

List of Tables 6

List of Figures. 7

List of Abbreviations. 8

Introduction to the Handbook 9

Session 1: Introduction to Risk Management 10
1.1 Introduction. 10
1.2 Learning Objectives 10
1.3 Definitions of Risk 10
1.4 Confusion between an existing Problem and a Risk 11
1.5 Types and Categories of Risks 11
1.6 What is Risk Management? 13
1.7 Benefits of Managing Risks in LGAs 13
1.8 Review Questions 13

Session 2: Government Policy and Legal Context of Risk Management 14
2.1 Introduction 14
2.2 Session Objectives 14
2.3 Legal Context of Risk Management 14
2.4 Government Policy on Risk Management. 14
2.5 Implementation of Requirements for LGAs 15
2.6 Review Questions 15

Session 3: Principles and Standards on Risk Management 16
3.1 Introduction 16
3.2 Session Objectives 16
3.3 Definitions 16
3.4 Principles of Risk Management 17
3.5 International standards on Risk Management 17
3.6 Review Questions 20

Session 4: Embedding Risk Management in the LGA's Activities 21
4.1 Introduction. 21
4.2 Session Objectives 21
4.3 Definitions 21
4.4 Embedding Risk Management Culture in the LGA 21
4.5 Features of an Embedded Risk Management System in the LGA. 22
4.6 Integrating Risk Management Activities in the LGA Planning Process 22
4.7 Allocating Resources for Risk Management Activities 23
4.8 Review Questions 23

Session 5: The Risk Management Framework – Main Components of a Framework 24
5.1 Introduction 24
5.2 Session Objectives 24
5.3 Definitions 24
5.4 Components of the Risk Management Framework 25
5.5 Developing a Risk Management Framework 25
5.6 Review Questions 26

Session 6: The Risk Management Framework – Risk Management Policy 27
6.1 Introduction 27
6.2 Session Objectives 27
6.3 Definitions 27
6.4 Purpose of a Risk Policy Statement. 27
6.5 Formulating Risk Management Policy Statements 28
6.6 Review Questions 29
Session 7: The Risk Management Framework – Risk Architecture 30
7.1 Introduction 30
7.2 Session Objectives 30
7.3 Definitions 30
7.4 Purpose of Risk Architecture. 31
7.5 Formulating Roles and Responsibilities for Risk Management 31
7.6 Review Questions 33
Session 8: The Risk Management Framework - Risk Protocols 34
8.1 Introduction. 34
8.2 Session Objectives 34
8.3 Definitions 34
8.4 Purpose for Developing the Risk Protocols 34
8.5 Outlining the LGA's Risk Protocols 34
8.6 Risk Assessment Protocols Based on International Standards 35
8.7 Review Questions 36
Session 9: The Risk Management Process – Preliminaries to Risk Assessment . . 37
9.1 Introduction 37
9.2 Session Objectives 37
9.3 Definitions 37
9.4 Position of Risk Assessment in The Risk Management Process 37
9.5 Choosing the Approach to Conduct the Risk Assessment Exercise 38
9.6 Selecting the Level for The Risk Assessment 38
9.7 Review Questions 39
Session 10: The Risk Management Process – Conducting the Risk Assessment . . 40
10.1 Introduction 40
10.2 Session Objectives. 40
10.3 Definitions 40
10.4 Risk identification 40
10.5 Risk analysis 42
10.6 Risk Evaluation. 44
10.7 Review Questions 45
Session 11:The Risk Management Process – Risk Register and Treatment Plans . . 47
11.1 Introduction 47
11.2 Session Objectives 47
11.3 Definitions 47
11.4 Developing the LGA's Risk Register 47
11.5 Preparing the Risk Treatment Action Plans 50
11.6 Review Questions 52
12 Monitoring, Evaluation and Reporting of LGA Risk Management 53
12.1 Introduction 53
12.2 Session Objectives 53
12.3 Preparing Risk Treatment Implementation Reports 53
12.4 Monitoring and Evaluation of the Risk Management Framework 56
12.5 Review Questions 57
Bibliography 58

List of Tables

Table 1: Different definitions of risks from standard setting institutions . . 10
Table 2: Examples of risks in different categories 11
Table 3: List of most common risk management standards. 16
Table 4: Risk management roles and responsibilities in the LGA 31
Table 5: Sources of risk 41
Table 6: Example of risk identification by considering the causes and consequences 41
Table 7: Meaning of rates on impact and likelihood of risks 42
Table 8: Risk ratings, color expression and responses 44
Table 9: Risk Assessment Form 45
Table 10: Example of a completed Risk Register 48
Table 11: Example of Risk Treatment Action Plan 50
Table 12: Risk Treatment Quarterly Report Form 54

List of Figures

Figure 1: Risk Management Process 12

Figure 2: Risk management process based on ISO 31000:2009 17

Figure 3: Risk management process based on COSO 18

Figure 4: Linking risk management with the planning process 21

Figure 5: Components of a risk management framework 24

Figure 6: Sample of a risk management policy of an LGA 27

Figure 7: Example of a risk management governance structure: 30

Figure 8: Choice of risk management procedures as per ISO 31000 or COSO ERM (2004) 35

Figure 9: Different levels of looking at risks and their assessment. 38

Figure 10: Example of a plotted risk heat map 49

List of Abbreviations

BS	British Standards
CAG	Controller and Auditor General
CCHP	Comprehensive Council Health Plan
CHMT	Council Health Management Team
CLFO	City Livestock & Fisheries Officer
CMO(H)	County Medical Officers (of Health)
COSO	Committee of Sponsoring Organizations
CRSA	Control Risk Self-Assessment
DC	District Council
ERM	Enterprise Risk Management
FERMA	Federation of European Risk Management Standards
GIZ	Gesellschaft für Internationale Zusammenarbeit
HoD	Head of Department
IA	Internal Audit
IAG	Internal Auditor General
IAGD	Internal Auditor General's Division
IAU	Internal Audit Unit
IIA	Institute of Internal Auditors
IMS	Information Management System
IRM	Institute of Risk Management
IRMI	International Risk Management Institute
ISO	International Organization for Standardization
IT	Information technology
LGA	Local Government Authority
MDAs	Ministries, Departments and Agencies
MTEF	Medium-term Expenditure Framework
PSOs	Public Sector Organizations
RAS	Regional Administrative Secretary
RMGS	Risk Management Governance Structure
RS	Regional Secretariat
SULGO	Support to Local Governance Processes
TZS	Tanzanian Shilling

Introduction to the Handbook

Background Information

This Participant's Handbook on Risk Management has been developed as part of the Project "Strengthening internal controls at sub-national level" under the GIZ Programme "Support to Local Governance Processes" (SULGO). The project's objective is: "The internal control mechanisms at selected LGA level in the two partner regions of the programme, Mtwara and Tanga, are reinforced". The project supports the Tanzanian Local Government Reform Programme as one of the major national strategies promoting the decentralization process.

The project covers four (4) key thematic areas: (1) risk management; (2) accounting and administrative controls; (3) internal audit techniques and (4) functioning of the audit committees. Each thematic area has its own coaching materials in form of participants' and facilitators' handbook. The coaching curriculum for each of the thematic area was developed based on the coaching needs assessment of beneficiaries, documentary review on CAG audit reports, management letters and on the study "Priority Entry Points to Strengthen Accountability and Internal Auditing at District level" from 2012.

Use of the Participants' Handbook

This handbook was first used as a coaching aid when coaching sessions were conducted to officials in the four pilot LGAs, i.e. in Handeni District, Tanga City, Mtwara District and Mtwara Municipal Council. Further coaching sessions were conducted for selected participants of the Tanga and Mtwara Regional Secretariats (RS).

After the coaching has ended, the handbook can be further used as reference and guidance document, e.g. for clear definitions of technical terms, for step-by-step explanations of processes, for checklists or for the correct use of templates and reporting formats.

In addition to the coaching participants, the handbook was also developed for staff members of other RS and LGAs as a self-learning kit.

Overview of Session Layout and Design

The Participants' Handbook covers 12 main coaching sessions. The layout of the session is composed of an introduction, learning objectives, definitions if appropriate, the session content, some hints and review questions. On successful completion of the 12 sessions, participants will be able to perform clearly their roles and responsibilities with regard to risk management.

The coaching sessions may have a duration ranging from forty five minutes up to two hours, with the average being one hour. They will be delivered in the form of one-on-one sessions, focus group discussions and peer-to-peer learning sessions.

Session 1

1 Introduction to Risk Management

1.1 Introduction

Risk management has become a core management principle. Organisations both private and public face a number of risks that originate from various sources and pose uncertainty on the achievement of objectives. This session presents the basics of risk management which will set a building block for the remaining parts of the handbook.

1.2 Learning Objectives

To give the participants a broad perspective of the meaning of the terms ‘risk’ and ‘risk management’, and its advantages such that, at the end of the session, the participants will be able to:

- Explain the meaning of risk;
- Understand the concept of risk management;
- Appreciate the relevance and benefits of managing risks in their LGAs.

1.3 Definitions of Risk

Risk is defined differently by different organisations. However, the most common definition of risk is:

> “Risk is defined as the uncertainty/possibility of an event occurring that will have an impact on the achievement of objectives. Risk is measured in terms of impact and likelihood”.
>
> Institute of Internal Auditors (IIA)

This definition is also used in the Guideline for Institutional Risk Management Framework in the Public Sector in Tanzania, which forms the basis of risk management in the LGAs.

Table 1 below gives a collection of other definitions of risk as provided by different standard setting institutions.

Table 1: Different definitions of risks from standard setting institutions (Source: Hopkins, 2010)

Organization	Definition of risk
ISO Guide 73 ISO 31000	Effect of uncertainty on objectives. Note that an effect may be positive, negative, or a deviation from the expected. Also, risk is often described by an event, a change in circumstances or a consequence.
Institute of Risk Management (IRM)	Risk is the combination of the probability of an event and its consequence. Consequences can range from positive to negative.
"Orange Book" from Treasury (UK)	Uncertainty of outcome, within a range of exposure, arising from a combination of the impact and the probability of potential events.
Institute of Internal Auditors	The uncertainty of an event occurring that could have an impact on achievement of the objectives. Risk is measured in terms of consequences and likelihood.
Alternative Definition by the author	Event with the ability to impact (inhibit, enhance or cause doubt about) the mission, strategy, projects, routine operations, objectives, core processes, key dependencies and/or the delivery of stakeholder expectations.

From the definitions above the following are the key points to consider:

- Risk is a consequence of pursuing an OBJECTIVE.
- Risk is something (event, situation, circumstances) that is UNCERTAIN.
- Risk has an IMPACT on the objective, and a LIKELIHOOD of occurring.

1.4 Confusion between an existing Problem and a Risk

It should be noted that there is often confusion between the term risk and the term problem:

- The main feature for an event to be termed as a risk is UNCERTAINTY (i.e. the possibility of future events, which may happen or not). Risks must be managed.
- A problem is an event that is CERTAIN or sometimes is termed as an ISSUE (i.e. has or is happening or known for sure to happen. Hence one does not need to prepare for it but to solve it). Problems are often viewed as challenges or issues that are known and must be solved/encountered.

1.5 Types and Categories of Risks

Risks can be grouped into different categories according to their nature and effect. The following are the most common types and categories of risks:

i. Strategic risks:

   Risks to the entity's direction, external environment and to the achievement of its plans e.g. changes in government policies, political changes etc.

ii. Compliance/Commercial/Legal risks:

   Risks of commercial relationships/meeting regulatory obligations, such as breach of contract, non-compliance with accounting standards or environmental regulations.

iii. Operational risks:

   Operational activities such as inadequate human resources, poor service levels, physical damage to assets or threats to physical safety.

iv. Technical risks:

Risks of managing assets such as equipment failure, IT risks like virus incidents, computer crash etc.

v. Financial and systems risks:

Risks in financial controls and systems, such as fraud, theft or misappropriation of funds, inadequate funding, delayed procurement, delayed reports etc.

Table 2: Examples of risks in different categories (Risk Management Guideline, 2012)

Strategic	Financial	Operational	Knowledge and System
Loss of customers to private sector companies	Incorrect valuation of capital assets	Absenteeism	Inadequate system security/Confidential information not adequately protected
Political change	Capital assets not maintained/deterioration	Inability to attract and retain staff/Staff turnover	IT systems not integrated
Inaccurate forecasting	Equipment obsolescence	Poor service provided by staff	Network failure/network unavailability
Unethical business practices	Customer revenue/collections targets not met	Strikes and workplace unrest	Unauthorized system access/IT security breach or failure
Strategic plan not implemented	Unauthorized and irregular expenditure	Wrongful termination	IT system/software obsolescence
Business Continuity Planning inadequate/or not developed	Wasteful or unproductive expenditure	Uncompetitive remuneration	Ineffective Disaster Recovery Plan
Poor community relationships	Changes in funding allocations	Job roles/accountabilities unclear	Poor choice of software/IT solution/IT solution does not support business requirements
Negative/hostile/inaccurate press coverage	Over/under spending budget allocations	Workplace injury: Burns, falls, food poisoning, car accident etc.	System not scalable/cannot meet increased capacity requirements
Ineffective communication strategy/plans	Inaccurate revenue forecasting	Pandemic and Infectious Disease Outbreak	Loss of data/information
Failure to meet sustainability targets	Inaccurate expenditure forecasting	Failure of/No fire suppression system	
Water shortages	Financial reporting requirements not understood	Sexual harassment/violence	
Fuel shortages	Reporting deadlines not met	Equipment obsolescence	
Contamination of water supply	Errors/omissions in financial statements	Failure to maintain/repair assets	
Damage to/development of protected sensitive natural habitats	Reporting not in correct format	Unauthorized use/Misuse of fleet vehicles	
Air or water pollution	Fraud	Failure to maintain assets/equipment	
		Theft	

1.6 What is Risk Management?

Risk management is defined as:

> "A process for identifying, assessing, managing, and controlling potential events or situations to provide reasonable assurance regarding the achievement of organisation's objectives".
>
> Institute of Internal Auditors (IIA)

Based on the definition above, risk management can be seen as a PROCESS, which consists of the aspects depicted in figure 1 below:

Figure 1: Risk Management Process

1.7 Benefits of Managing Risks in LGAs

The following are the potential benefits for managing risks in LGAs:

- Establishment of a reliable basis for decision making and planning (strategic and operational planning);
- Assurance on the achievement of LGA's objectives and performance targets through the awareness and management of potential events/and situations that work against the objectives;
- Enhanced communication across all levels of management within the LGA;
- Effective use of resources to minimize operational surprises and shocks;
- Management grasping new opportunities in a timely manner.
- Facilitation of compliance with relevant legal and regulatory requirements and international norms;
- Enhanced health and safety performance as well as environmental protection;
- Improved stakeholders' confidence and trust.

> !
>
> Always consider risk in both negative and positive aspects.
>
> In English language the term risk means "a chance or possibility of danger, loss, injury or other adverse consequences".
>
> In risk management, however, risk is considered to be either positive or negative where:
>
> - Positive risks are the opportunities that push us to exceed our objectives.
> - Negative risks are the threats that hinder the achievement of objectives.

1.8 Review Questions

1. What is a risk? Can you find different definitions of a risk?
2. Which among the definitions suits your LGA? Why?
3. What are possible risks that your LGA is likely to face in the pursuit of its objectives?
4. Do you agree with the concept of positive risks? Why (not)? Provide examples of positive risks.

Session 2

2 Government Policy and Legal Context of Risk Management

2.1 Introduction

The Government of Tanzania, through the Internal Auditor General's Division of the Ministry of Finance, has made it mandatory for all public sector organisations to adopt and implement risk management practices. These requirements are specifically issued in the Treasury Circular No. 12 of 2013 which requires all Accounting Officers to establish and implement risk management processes in their organisations.

2.2 Session Objectives

At the end of this session, it is expected that the participants will be able to:

- List all the government documents with regard to risk management;
- Understand the general legal context surrounding risk management in the Tanzanian public sector (i.e. MDAs and LGAs);
- Understand the government policy and implementation requirements with regard to risk management.

2.3 Legal Context of Risk Management

Risk management is a legal requirement in Tanzanian public sector. This means that all MDAs and LGAs are required to adopt and implement risk management practices.

The following are the documents in which risk management is stipulated:

- The Public Finances Act (2001) as amended in 2010 – the act establishes the Internal Auditor General's Division of the Ministry of Finance, who is charged with the responsibility to issue guidelines and to conduct reviews and assessments of the quality and effectiveness of risk management practices across MDAs and LGAs.
- The Guidelines for Developing and Implementing Institutional Risk Management Framework in the Public Sector, which provide a step-by-step instruction on how to implement risk management – issued on December, 2012 by the Internal Auditor General's Division of the Ministry of Finance.
- Treasury Circular No. 12 of 2013 on the Guidelines for Developing and Implementing Institutional Risk Management Framework in the Public Sector – requiring all Accounting Officers to Implement the Guidelines on Risk Management.

2.4 Government Policy on Risk Management

The government of Tanzania has expressed its commitment on implementing risk management throughout the public sector. This commitment has been written in the guidelines that have been issued to all MDAs and LGAs.

In the Guidelines it is stated that:

- "The Government of Tanzania recognizes that risk is inherent in each objective of all public sector organizations.
- The Government therefore considers the management of risk as an integral part of sound public sector governance because it provides assurance to the achievement of government's objectives across different sectors, which in turn leads to the effectiveness and efficiency in government performance towards providing services to the citizens and increased stakeholders' confidence.
- To this end, the Government of Tanzania is committed to ensuring that enterprise risk management is adopted, implemented and enhance across the Tanzanian public sector.
- The Government, through the Ministry of Finance – Treasury, takes an active role in providing and setting broad guidance and support on the development, implementation and enhancement of risk management practices across the Tanzanian public sector."

In the same Guideline, the Accounting Officers are given the responsibility to implement risk management:

- "Accounting Officers of all PSOs are charged with the responsibilities of adopting and implementing effective risk management practices in their organizations".

(Source: IAG Division, 2012 – Guidelines on Risk Management Framework)

2.5 Implementation of Requirements for LGAs

Each Ministry, Department, Agency (MDA), Parastatal Organization, Regional Secretariat (RS), Local Government Authority (LGA) is required to develop, implement and enhance a risk management framework which ensures that:

- There is a policy, culture and structure that facilitates how the organisation will identify record and monitor risks, including procedures for reporting risks information to the Accounting Officers and other oversight organs;
- There is a risk management process which is in line with international standards for risk management (e.g. ISO 31000 or COSO etc.);
- The risk management process is part of the strategic, operational and annual business planning activities of the organisation;
- There is a risk register that is used to record, rate, monitor and report risks;
- There is an established process for monitoring, reviewing and enhancing risk management and governance systems.

(Source: IAG Division, 2012 – Guidelines on Risk Management Framework)

2.6 Review Questions

1. What is the role of the Internal Auditor General in relation to risk management in the public sector?
2. What are the potential challenges your LGA may face in its attempt to implement the requirements as stated in the Treasury Circular No. 12 of 2013 with regard to risk management?
3. What do you propose to be done in order to curb all the challenges against the implementation of risk management at your LGA?

Session 3

3 Principles and Standards on Risk Management

3.1 Introduction

Risk management is based on established principles and international standards. The Guidelines for risk management requires LGA to formulate their risk management framework based on internationally recognised risk management standards.

It should be noted that, there is no single international standard on risk management. This session will present two of the most common risk management standards/models (i.e. the ISO 31000 of 2009 and the COSO of 2004).

3.2 Session Objectives

This session gives the participants a broad overview of the basic principles/standards for managing risks in LGAs.

By the end of the session, participants should be able to:

- Understand what is meant by the term ”international standards and principles”;
- Understand the main principles for risk management;
- Obtain an overview of the ISO 31000: 2009 standards and COSO ERM on risk management;
- Discuss the opportunities and challenges of adopting international standards in risk management in LGAs.

3.3 Definitions

What is a standard? What are international standards?

> “A standard is a level of quality or attainment, or used or accepted as normal or average, or model in a comparative evaluation”.
>
> “International standards are standards developed by international organisations. International standards are available for consideration and use worldwide”.
>
> Source: http://en.wikipedia.org/international_standard

What is a principle?

> “A principle is a fundamental truth or proposition that serves as the foundation for a system”.

3.4 Principles of Risk Management

In risk management, one can divide between two main groups of principles (Hopkins, 2010):

- Those outlining HOW risk management SHOULD BE in the LGA.
- Those outlining WHAT risk management SHOULD DELIVER to the LGA.

3.4.1 How should Risk Management be in the LGA?

Hopkins (2010) suggests that risk management initiatives in the LGA should be based on the following principles:

- Proportionate to the level of risk within the LGA;
- Aligned with other activities/operations in the LGA;
- Comprehensive, systematic and structured;
- Embedded within business processes (this will be discussed in a separate topic ahead);
- Dynamic and responsive to change.

The above principles are summarized in the acronym PACED and provide the foundation of a successful approach to risk management within any organization.

3.4.2 What should Risk Management deliver in the LGA?

A well embedded risk management should deliver the following to the LGA:

- Compliance with laws and regulations;
- Assurance regarding the management of significant risks;
- Decisions that pay full regard to risk considerations;
- Efficiency, effectiveness and efficacy in operations, projects and strategy.

3.5 International standards on Risk Management

There are a number of standards and models for risk management, which are proposed by different institutions. Table 3 below provides a list of the most common risk management standards/models and their specific emphasis:

Table 3: List of most common risk management standards

Standard/model	Name of Document
ISO 31000:2009	Risk Management – Practice and Guidelines
BS 31000:2008	Code of Practice for Risk Management
COSO:2004	Enterprise Risk Management – Integrated Framework
FERMA:2002	A Risk Management Standard
Solvency II:2012	Risk Management for the Insurance Industry

Due to the availability of many international standards, the Tanzanian Government has allowed LGAs to choose any of the standards to adopt. The only condition is that the standard must be internationally recognised as stated in the Government's Guidelines for Risk Management:

"PSOs are not restricted to align their risk management practices with ISO 31000. They are rather required to observe that their risk management frameworks are in line with internationally recognized Risk Management Standards (e.g. COSO or ISO 31000 etc.)". (Source: IAG Division, 2012 – Guidelines on Risk Management Framework)

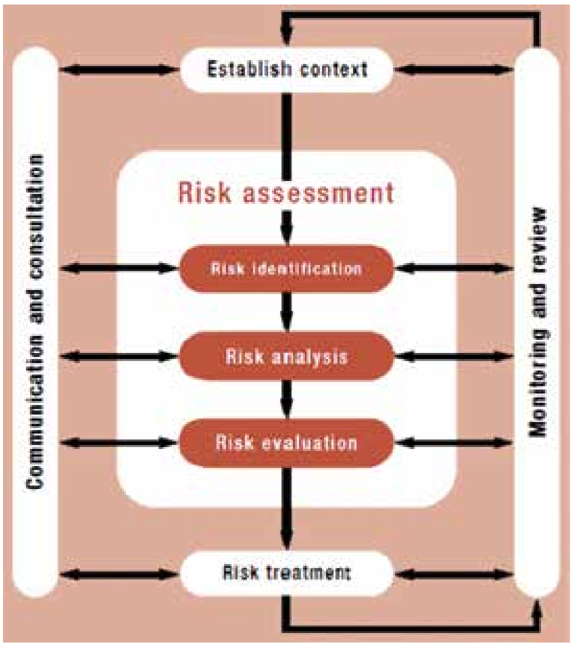
In the next sections two of these standards are given more attention i.e.:

- The ISO 31000:2000 Risk management – Practices and Guidelines;
- The COSO 2004 – Enterprise Risk Management Integrated Framework.

3.5.1 ISO 31000: 2009 – Risk Management Practices and Guidelines

According to ISO 31000: 2009, the risk management process should consist of 6 components or steps as shown in Figure 2 below:

Figure 2: Risk management process based on ISO 31000:2009 (Source: IRM, 2010)



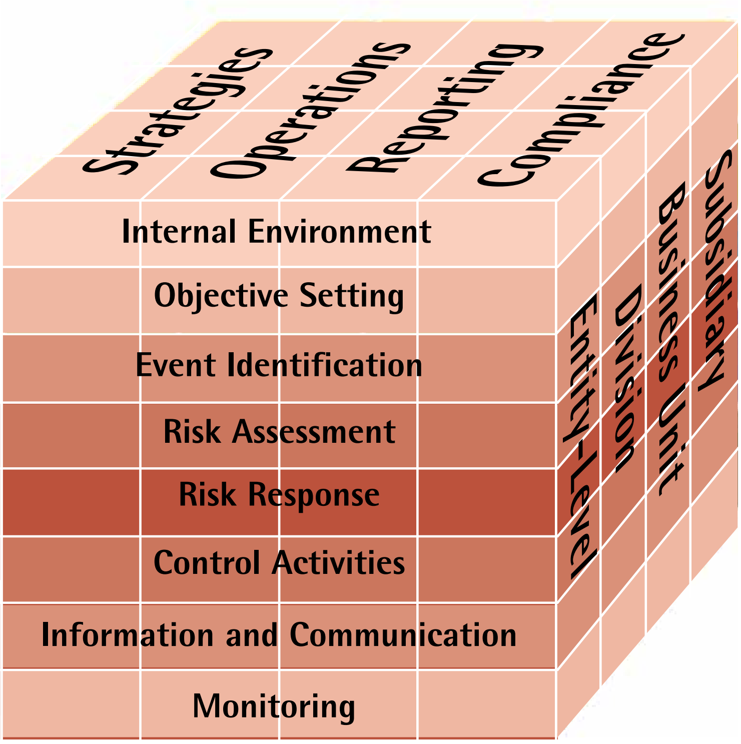
This approach consists of the following components or steps:

- Establish the context: Context could be viewed in terms of external (political, legal, technological, economic, social and environmental) and in terms of the internal environment of the LGA.
- Identify risks: The identification of what, why and how events arise as basis for further analysis.
- Analyse and evaluate risks: The determination of existing controls and the analysis of risks in terms of consequence and likelihood in the context of those controls.
- Treat risk: To develop and implement specific risk management plans including funding considerations.
- Monitor and Review: The oversight and review of the risk management system and any changes that might affect it.
- Communication and Consultation: Appropriate communication and consultation with internal and external stakeholders should occur at each stage of the risk management process.

3.5.2 COSO 2004 – Enterprise Risk Management Framework

The COSO (2004) approach to risk management is depicted in Figure 3 below:

Figure 3: Risk management process based on COSO (Source: COSO, 2004)



According to the COSO (2004)–model, risk management is geared to achieving an entity's objectives based on four categories:

- Strategic – high-level goals, aligned with and supporting its mission;
- Operations – effective and efficient use of its resources;
- Reporting – reliability of reporting;
- Compliance – compliance with applicable laws and regulations.

This categorization of entity objectives allows focusing on separate aspects of risk management. Similar to the ISO 31000, COSO views risk management as a process consisting of eight interrelated components:

- Internal Environment – the internal environment encompasses the tone of an organization, and sets the basis for how risk is viewed and addressed by an entity's employees;
- Objective Setting – objectives must exist before management can identify potential events affecting their achievement;
- Event Identification – internal and external events affecting achievement of the LGA's objectives must be identified, distinguishing between risks and opportunities;
- Risk Assessment – risks are analysed, considering likelihood and impact, as a basis for determining how they should be managed;
- Risk Response – management selects risk responses – avoiding, accepting, reducing, or sharing risk – developing a set of actions to align risks with the LGA'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;
- Monitoring – the entire enterprise risk management is monitored and modifications are made as necessary.

! The choice of an international standard for risk management of your LGA should be based on:

- The compatibility/or adoptability of the standard with the LGA's or public sector settings;
- Its popularity among other LGAs or MDAs or similar organizations.

3.6 Review Questions

1. What is the main difference between a standard and a principle?
2. Why do you think it is important to base your LGA's risk management approach to an international standard?
3. Compare and contrast the two standards (i.e. COSO 2004 and ISO 31000:2009). What are their main similarities? What are their main differences? Do you think they focus on achieving the same results? Why (not)?

Session 4

4 Embedding Risk Management in the LGA's Activities

4.1 Introduction

Risk management is a relatively new concept in LGA governance. It therefore needs a careful approach of integrating it within the existing cultures, systems and activities of the LGA. The main focus when adopting risk management, especially at early stages, is to avoid the mistake of making risk management to be seen as a separate activity which may bring about mismatch and potential conflict or resistance from stakeholders.

Integration is usually termed as embedding, which is used to refer to the efforts of making risk management as part of the daily activities of the LGA.

4.2 Session Objectives

It is expected that at the end of the session, participants should be able to:

- Understand the meaning and importance of embedding risk management in LGA's culture and activities;
- Know the features of a well embedded risk management framework;
- Understand how to integrate risk management into LGA planning and budgeting processes;
- Appreciate the need to allocate sufficient resources to risk management activities.

4.3 Definitions

What is embedding risk management?

> To embed risk management means to integrate risk management so that it becomes part of the daily activities. It is not to be seen as something separate added to the existing systems and activities of the organisation, i.e. risk management to be real, natural, convenient, and effective.
>
> International Risk Management Institute - IRMI (2004)

In the context of risk management, this means to make the organisation become RISK-BASED in its activities.

4.4 Embedding Risk Management Culture in the LGA

Embedding risk management culture in the LGA involves the creation of an environment that can demonstrate the following:

- Leadership from the LGA senior management and the support from the full council and political leaders;
- Involvement of staff at all levels;

- A culture of learning from experience;
- Appropriate accountability for actions (without developing an automatic blame culture);
- Good communication on risk issues.

Achieving a culture of risk awareness is ensured by:

- Establishing an appropriate risk management framework (i.e. risk architecture, strategy and protocols which are the main components), and
- Running awareness and capacity building campaigns to key stakeholders within the LGA.

4.5 Features of an Embedded Risk Management System in the LGA

The following features are expected to be present when risk management is fully embedded in the LGA:

- There is a risk management policy that is approved and sponsored by the full council (i.e. policy, structure and procedures – discussed in Session 5 and 6);
- There is buy-in from staff members, which is a results of awareness campaigns (this will help to deal with resistance and change of culture);
- Responsibilities are assigned (to the Risk Management Coordinator, risk owners etc. – included in the risk management structure – discussed in Session 5 and 7);
- Risk assessment is conducted to create a RISK REGISTER (as part of implementing the risk management process – discussed in Session 10 and 11);
- MITIGATION measures are proposed/planned and IMPLEMENTED (discussed in Session 12);
- Risk Management REPORTS are prepared and acted upon (discussed in Session 13);
- There is continuous review and improvement on the risk management framework (discussed in Session 14).

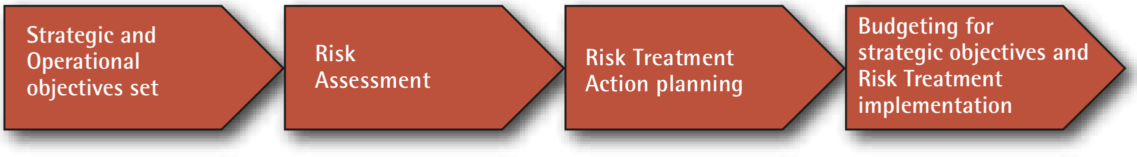
4.6 Integrating Risk Management Activities in the LGA Planning Process

Most organisations in the public sector have experienced problems in linking their risk management activities with other activities, especially when implementing their strategic plans.

The source of this problem originates from the lack of connection between the LGA planning and budgeting process with the risk management process, hence leading to limited attention and no resources committed to risk treatments.

The following figure 4 demonstrates the approach of linking risk management with the planning process and ensuring that risk management activities are implemented along other activities within the LGA:

Figure 4: Linking risk management with the planning process


Strategic and Operational objectives set
Risk Assessment
Risk Treatment Action planning
Budgeting for strategic objectives and Risk Treatment implementation

- The LGA sets strategic and operational objectives and their respective implementing activities.
- The assessment of risks against those strategic objectives or targets is conducted and leads to the preparation of a risk register.
- Risk treatment plans/controls are formulated and incorporated in activities in the strategic plan according to their respective strategic objectives.
- In a final step, the budget is prepared to include both the activities for implementing the strategic objectives and risk treatment actions.

4.7 Allocating Resources for Risk Management Activities

The LGA budgeting should consider setting aside financial resources for risk management activities like:

- Training on risk management to LGA staff (internally and externally);
- Conducting risk assessment activities (e.g. Control-Risk Self-Assessment (CRSA) workshops and surveys);
- Holding meetings relating to risk management issues;
- Implementing risk treatment activities as suggested in the risk register (because most of the risk treatment activities have budget implications).

4.8 Review Questions

1. What does embedding risk management means?
2. Why is it important to create a risk management culture among LGA staff?
3. Using the experience in your LGA, what needs to be done to make personnel be risk aware?
4. Suggest possible ways in which the LGA can link its risk management process with the planning and budgeting process, so as to ensure that risk treatment activities are implemented alongside other activities with the same available financial resources.

Session 5

5 The Risk Management Framework – Main Components of a Framework

5.1 Introduction

The previous session provided a highlight of the risk management process as viewed by different standard setting institutions (i.e. COSO 2004 and ISO 31000). However, before a LGA starts to implement the risk management process, best practice requires the development of a risk management framework, which is defined below and forms the foundation for the risk management process.

5.2 Session Objectives

The session aims at enabling the participants to understand the meaning of a Risk Management Framework (in relation to risk management process) and its main components.

By the end of the session, participants should be able to:

- Explain the meaning of the risk management framework (in relation to the risk management process);
- Understand the main components of the risk management framework;
- Appreciate the need for developing a risk management framework before implementing a risk management process in a LGA.

5.3 Definitions

What is a framework?

> "A framework is defined as an essential supporting or underlying structure."
>
> (Concise Oxford Dictionary)

What is a risk management framework?

> "A risk management framework is a set of components that provides a structure that will facilitate the use of a consistent risk management process."
>
> Source: IRM, 2010
>
> "A risk management framework is a set of components that support and sustain risk management throughout an organisation"
>
> Source: ISO 31000: 2009 Risk Management Dictionary

What is a risk management process?

> "A risk management process is a process for identifying, assessing, managing, and controlling potential events or situations to provide reasonable assurance regarding the achievement of organisation's objectives."
>
> Source: Institute of Internal Auditors

Considering the two definitions above, the following points should be noted:

- The risk management framework supports the risk management process;
- Therefore, a risk management framework must first be established before starting to conduct the risk management process.

5.4 Components of the Risk Management Framework

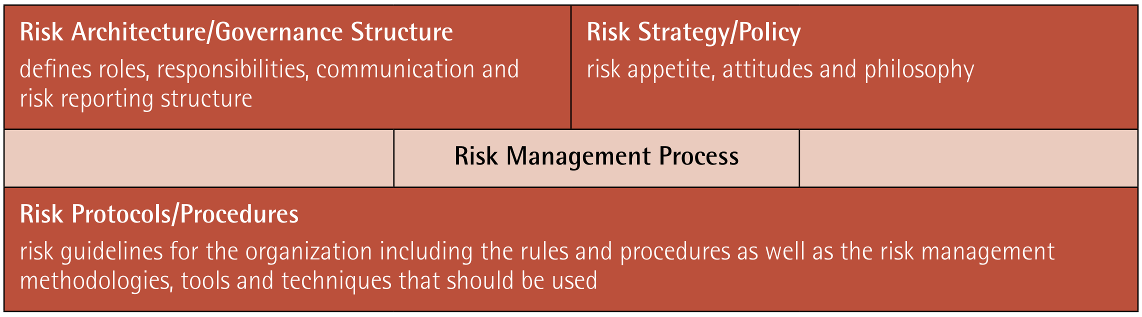
As defined above, a risk management framework is composed of different sets of components. Following the IRM approach (Hopkins, 2010), there are three components which are abbreviated as RASP i.e.:

- Risk architecture (or governance structure);
- Risk strategy (or policy),
- Risk protocols (or procedures).

For simplicity, in the following sessions, the terms risk management governance structure, policy and procedures will be used alternatively to mean risk architecture, strategy and protocols respectively as they are synonyms.

The three components and their interrelation are presented in Figure 4 below, developed by the Institute of Risk Management (IRM).

Figure 5: Components of a risk management framework (Source: Hopkin, 2010)



Risk Architecture/Governance Structure
defines roles, responsibilities, communication and risk reporting structure

Risk Strategy/Policy
risk appetite, attitudes and philosophy

Risk Management Process

Risk Protocols/Procedures
risk guidelines for the organization including the rules and procedures as well as the risk management methodologies, tools and techniques that should be used

From the figure it can be noted that the three outer components (i.e. architecture, strategy and protocols) support the middle component (i.e. the risk management process)

5.5 Developing a Risk Management Framework

The Guideline for Developing an Institutional Risk Management Framework shows that a LGA must:

- Formulate a risk management policy (to indicate its attitudes and commitment to risk management);
- Design the risk management governance structure (to show the roles and responsibilities of different officials and the reporting lines);

- Develop risk management procedures (to provide internal guidelines of how to go about when implementing risk management processes).

The following sessions will discuss on how to develop and document each of these components.

!

- Be aware that in many places the terms “risk management framework” and “risk management policy” are used interchangeably.
- In some places the risk management policy may include all the components that are the components of a risk management framework.

5.6 Review Questions

1. What is a risk management framework?
2. How does a risk management framework differ from a risk management process? What is the relationship between the two?
3. Does your LGA have a documented risk management framework? If yes, what are the main components in your LGA’s framework?

Session 6

6 The Risk Management Framework – Risk Management Policy

6.1 Introduction

A risk management policy is among the three main components of the risk management framework. An LGA with intentions to adopt and implement risk management practices must have a specific policy that addresses risk management.

6.2 Session Objectives

This session provides an understanding of what is involved in the process of developing a risk management policy.

By the end of the session, the participants should be able to:

- Understand the meaning and need for a risk management policy (as a component of the framework);
- Develop a risk management policy statement that fits with their LGA's environment.

6.3 Definitions

What is a risk management policy statement?

> "A risk management policy is a statement of the overall intentions and direction of an organization related to risk management."
>
> Source: ISO 31000:2009

6.4 Purpose of a Risk Policy Statement

Any policy statement (whether for risk management or for other areas) is intended to:

- Define the policy of the organisation;
- Describe how a policy is administered and define the particulars of the policy;
- Protect the organization from misunderstandings that might lead to unauthorized behaviour.

A risk management policy statement is likewise serving the above purposes, but more specifically, it is aimed at:

- Setting out the LGA's risk management objective and strategy to achieve this objective.
- Documenting the LGA's overall philosophy, commitment, appetite, attitudes, intentions, and direction related to risk management.

All these need to be documented, approved by the LGA and communicated to the LGA's staff and key stakeholders.

6.5 Formulating Risk Management Policy Statements

Risk management policy statements should be formulated to reflect what the LGA management wants to communicate about its philosophy, commitment and attitude about managing risks. There is no single way of writing a policy statement, except for the need to customise the statement to the needs of the LGA management.

As exemplified in Figure 5 below, it is expected that a risk management policy will have the following sections:

- The purpose: for adopting risk management in the LGA;
- Policy statements: to highlight the LGA's philosophy, attitudes and commitment towards risk management;
- Risk management principles: standards and models which the LGA adopts in implementing risk management (e.g. the ISO 31000:2009 added with some specific principles so as to align with the LGA's context).

Figure 6: Sample of a risk management policy of an LGA

KWETU DISTRICT COUNCIL
RISK MANAGEMENT POLICY

1.0 Purpose

The purpose of KWETU DC Risk Management Policy is to formalize and communicate the KWETU DC commitment and principles towards the management of risks across the Council. Specifically, the Risk Management Policy serves the following purposes:

i. To ensure that all the current and future material risk exposures of the KWETU DC are identified, assessed, quantified, appropriately mitigated and managed;

ii. To establish a framework for KWETU DC's risk management process and ensure entity-wide implementation;

iii. To ensure systematic and uniform assessment of risks related with quality education assessment and certification;

iv. To enable compliance with appropriate regulations, wherever applicable, through the adoption of best practices; and

v. To assure growth of KWETU DC's operations.

2.0 Policy Statements

It is hereby specified that KWETU DC:

i. Recognizes that risk is inherent in its mission, objectives, and activities.

ii. Recognizes that the management of risk is a key element of sound governance and an important strategy for the achievement of its mission, vision and supporting objectives.

iii. Is committed to embedding risk management principles and practices into its organizational culture, decision-making processes, business information systems, strategic and operational planning of programmes and activities.

iv. Will pro-actively identify, analyse and manage its risks and opportunities at all levels of the Council.

v. Ensures that all risk identification, analysis, evaluation and treatment are to be reported and updated within its Risk Register.

vi. Will promote continuous improvement and review of risk management through regular training, monitoring, audit and reporting processes.

vii. Will update its Risk Management Framework after every five years to align with its Five Years Rolling Strategic Plan cycle. However, the Framework may be reviewed at any given time to accommodate substantive changes which may make the existing Framework, or any of its sections, redundant.

viii. Will update its Risk Register annually to align with its planning and budgeting cycle.

3.0 Principles

The KWETU DC'S risk management approach is established in accordance with ISO 31000:2009 Risk Management – Principles and Guidelines on implementation.

6.6 Review Questions

What is the purpose for developing a risk management policy statement?

What are the key sections of a risk management policy?

In your groups, try to develop a policy statement with sentences that communicate your LGA's objective, recognition, intentions and commitment towards risk management.

Session 7

7 The Risk Management Framework – Risk Architecture

7.1 Introduction

A risk management framework must include the structure on how officials and organs in the LGA relate to each other on risk management activities. The risk management roles and responsibilities must be assigned to organs, officials and all staff and contractors working with the LGA. This will facilitate the smooth operation of risk management activities, establish clear reporting lines and risk information transfer as well as avoid conflicts.

7.2 Session Objectives

It is expected that at the end of this session the participants will be able to:

- Define the term risk architecture/governance structure;
- Design their LGA's risk architecture/governance structures that are aligned with the environment of their LGA.

7.3 Definitions

What is risk architecture/governance structure?

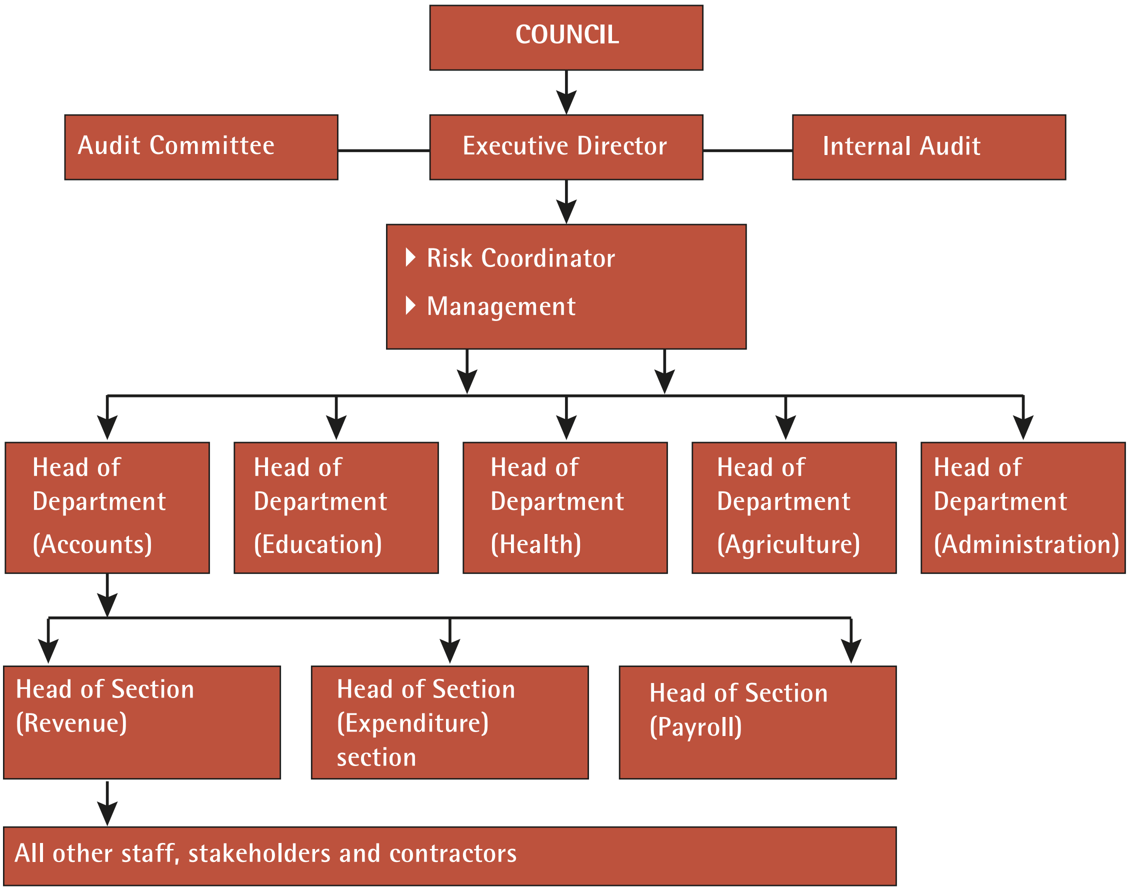
> "Risk architecture/governance structure defines roles, responsibilities, communication and risk reporting structure"
>
> Hopkins (2010)

Expanding from the definition above the LGA's risk architecture:

- Is the overall risk governance structure, which provides the arrangement and the roles and responsibilities among officials and committees;
- Outlines reporting lines among LGA officials and organs with regard to risk management.

Similar to the LGA organisation structure, the governance structure can be represented diagrammatically as in Figure 7 below:

Figure 7: Example of a risk management governance structure:
ABC District Council
Risk Management Governance Structure


COUNCIL
Audit Committee
Executive Director
Internal Audit
Risk Coordinator
Management
Head of Department (Accounts)
Head of Department (Education)
Head of Department (Health)
Head of Department (Agriculture)
Head of Department (Administration)
Head of Section (Revenue)
Head of Section (Expenditure) section
Head of Section (Payroll)
All other staff, stakeholders and contractors

7.4 Purpose of Risk Architecture

It is important for everyone to be aware of individuals and collective risk management responsibilities as it facilitates the smooth operation and reporting of risk management activities. The risk architecture is therefore a useful tool to summarize the responsibilities in risk management of each council member.

7.5 Formulating Roles and Responsibilities for Risk Management

A description of roles and responsibilities of each key party to who risk management duties have been delegated need to be stipulated.

To avoid conflicting roles and responsibilities among officials in the LGA, it is important that the risk governance structure be designed to align with the LGA organisation structure.

The Guideline for Developing and Implementing Risk Management Framework has provided some indicative roles and responsibilities for LGAs. These are summarised in Table 4 below:

Table 4: Risk management roles and responsibilities in the LGA

Position	Risk Management Responsibilities
The Council	Provides an overall direction and oversight of risk management across the LGA.
Executive Director	He/she has the responsibility of setting the tone and promoting a strong risk management culture by providing firm and visible support and ensuring risk management processes are implemented at lower levels.
Audit Committee	The primary objective of the audit/risk committee is to assist the Executive Director in discharging his/her responsibilities with regard to risk management by making risk management as their standing agenda.
Risk Management Coordinator	This is the Chief Risk Officer who has the responsibility to coordinate the development, enhancement, implementation and monitoring of risk management policies, procedures and systems at the LGA.
Internal Audit	To provide assurance that the risk management framework is effective as intended. This is done by evaluating the risk management process and focusing their audit activities on key risks. In some case, internal audit acts as the risk coordinator, especially on initial stages of developing the LGA's risk management framework. However, care must be observed when risk management activities are coordinated by the internal auditor, since there are some potential for conflict of interest when the internal auditor decides to audit the system of which he/she was responsible for designing.
Heads of Units and Departments	These are also known as "risk owners". They are the functional specialists who assume responsibility for designing, implementing, and/or monitoring and reporting on treatment of risks that fall within their areas of responsibilities.
Risk Champions	▸ Promote risk management across the LGA, or specifically within a particular department, unit, function or project; ▸ Assist to embed risk management into the LGA other systems and processes; ▸ Ensure that functional and project areas are using the LGA's risk management processes consistently; ▸ Acting as point of contact for risk management enquiries from their own departments; ▸ Facilitating dissemination of risk information to all levels of the department; ▸ Regularly updating HoDs regarding progress in implementing risk management programmes; ▸ Undertaking annual risk review. Champions will assist in the identification and reporting of emergent risks; ▸ Integrating risk actions into departmental plans and ensuring those actions are implemented and if not, report to HoD. Risk champions will advise HoD and colleagues on how risk management can be applicable in day today activities; ▸ Documenting and updating departmental risk register.
All Employees and Contractors	It is the responsibility of all personnel, stakeholders and contractors to apply the risk management process to their respective roles.

7.6 Review Questions

What is the risk management architecture/governance structure? Why is it important to design a risk management architecture/governance structure?

What care do you propose to be taken when internal auditors are given the responsibility for coordinating risk management initiatives?

In your groups, take an organisation structure of your LGA and design specific roles and responsibilities of the officials and committees in relation to risk management. What difference do you notice from your list compared to the one in Table 4?

Session 8

8 The Risk Management Framework – Risk Protocols

8.1 Introduction

Risk procedures are an essential component in the LGA's risk management framework. They provide the guidelines and procedures for carrying out risk management activities and reporting. It is essential that everyone in the LGA is aware of the procedures so as to assure the quality of risk management processes.

8.2 Session Objectives

The session aims at providing the participants with skills on formulating their LGA's risk management procedures within their risk management frameworks.

At the end of the session, the participants will be able to:

- Define the term risk management procedures/protocols;
- Understand the position/purpose of risk procedures/protocols in the LGA's overall risk management framework;
- Develop risk management procedures/protocols for an LGA.

8.3 Definitions

What are risk management protocols?

Risk management protocols are the stipulated guidelines and procedures for conducting different risk management activities in the LGA.

8.4 Purpose for Developing the Risk Protocols

The risk management protocols/procedures have to serve the following purposes:

- To provide rules and procedures that will guide all LGA officials in the conduct of their risk activities;
- To provide methodologies, tools and techniques that should be used at different stages of the risk management process (e.g. risk identification, assessment, treatment and reporting).

8.5 Outlining the LGA's Risk Protocols

As provided in the Guideline for Risk Management, when documenting the Risk Management protocols/procedures, the following should be included:

- Risk management definitions/language: a common risk language will produce consistent understanding of risk concepts and communication;

- Relationship and integration with other initiatives, e.g. strategic planning, budgeting and reporting;
- Description of how each step of the risk management process will be applied within the LGA's (see next section of matching procedures to either COSO ERM or ISO 31000 etc.);
- The risk reporting procedures, content, format, frequency and recipients of risk reports;
- Risk assessment criteria: agreed criteria for the assessment of risk likelihood, consequence, and overall risk rating.

It is important that the procedures developed are consistent with the way or system in which the LGA operates, i.e. there should be adherence to agreed procedures for reporting, meetings and channels of communication that do not violate existing procedures in the LGA.

8.6 Risk Assessment Protocols Based on International Standards

When developing the risk management protocols/procedures, care must be taken on stipulating the technical part for conducting the risk assessment process. The process must agree with international standards for risk management (e.g. the COSO 2004 ERM, or the ISO 31000: 2009).

The specific procedures that should be followed in carrying out risk management activities must be written down as shown in figure 7 below.

However, there are occasions where you need to customize/or reformulate some of the procedures so as to fit with your LGA's environment.

Example of steps in the ISO 31000: 2009:

i. Start by identifying the CONTEXT of you LGA (i.e. Operating environment, organization structure, internal approval processes, objectives and level to base your risk assessment);

ii. Identify RISKS (i.e. events/circumstances) that may impact the achievement of EACH OBJECTIVE;

iii. Assess the LIKELIHOOD and IMPACT of the risks;

iv. Propose "CONTROLS/MEASURES" to be taken in order to treat the RISK;

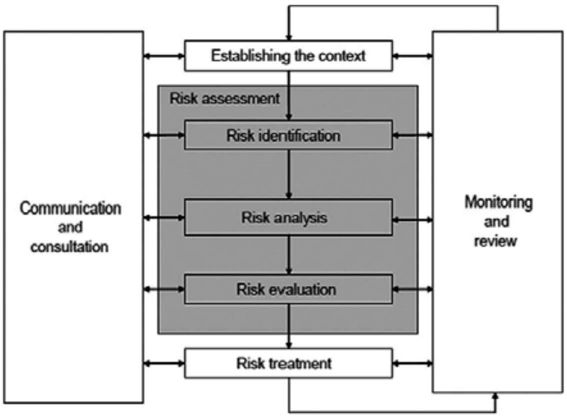
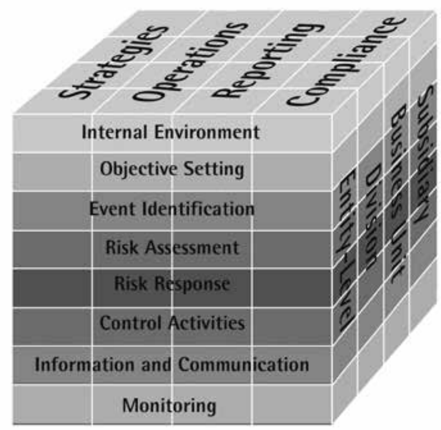
v. Assign RESPONSIBILITIES for risk management (consistent with the risk management governance structure you designed earlier);

vi. Draw ACTION PLANS for TREATMENT/RESPONSE/MITIGATION;

vii. REPORT on status (communicate, consult);

viii. REVIEW, MONITOR (monitor the management of specific risks and conduct review and evaluation of their overall framework).

Figure 8: Choice of risk management procedures as per ISO 31000 or COSO ERM (2004)

Risk Management Process by ISO 31000: 2009	Risk Management Process by COSO 2004
	

8.7 Review Questions

1. What do you understand by the term risk management protocols?
2. Outline specific procedures that should be followed in the reporting of risk management activities from heads of departments/units/sections to the risk coordinator, the executive director, the audit committee, and the full council.
3. Compare the procedures for risk assessment as given by the ISO 31000:2004 and the COSO ERM (2004) in Figure 8. (NB for detailed explanation of the models you may need to download them from the internet for free).

Session 9

9 The Risk Management Process – Preliminaries to Risk Assessment

9.1 Introduction

As defined earlier, the LGA's risk management framework (i.e. policy, structure and procedures) is designed to provide a foundation for implementing the risk management process in the LGA. It was also defined that risk management as a process involves, among others, three activities i.e. the identification, analysis and evaluation of risks, which collectively are termed as risk assessment.

This session presents the preliminary tasks and considerations to be undertaken before the LGA embarks on the implementation of the risk assessment exercise.

9.2 Session Objectives

The main objective is to give the participants the technical skills in conducting risk assessments in their LGAs.

It is expect that, at the end of this session, the participants will be able to:

- Define the term risk assessment;
- Understand the position of the risk assessment exercise in the LGA's risk management framework and risk management process;
- Choose or make decisions on the approach and levels for conducting risk assessment.

9.3 Definitions

What is risk assessment?

> "Risk assessment is a systematic process for identifying and evaluating events (i.e. possible risks and opportunities) that could affect the achievement of objectives, positively or negatively."
>
> PriceWaterHouseCoopers, 2008

9.4 Position of Risk Assessment in The Risk Management Process

Risk assessment is a key step/phase in the implementation of the LGA's risk management process. This is indicated in the ISO 31000:2009 model of risk management process in Figure 8 above (see the graph on the left side with the shaded area).

In summary, the risk assessment exercise includes three main activities:

- The identification of risks: What events or circumstances may happen to impact the objective?
- The analysis of risks: What is the impact and likelihood of the risk happening? and

- The evaluation of risks: What controls exist against the risks?

Note that, in the remaining sessions, the demonstration of the steps in the risk assessment exercise is based on the model of the risk management process by ISO 31000: 2009 (Figure 8, left side).

There could be minor differences when this is done using the COSO ERM (2004) model of the risk management process (Figure 8, right side).

9.5 Choosing the Approach to Conduct the Risk Assessment Exercise

There are several approaches or methods used to conduct the risk assessment exercise e.g.:

- Desk- top review of documentation;
- Survey using a specific questionnaire;
- One-to-one interviews with employees in the LGA;
- Group interviews (e.g. in a group of 3 staff);
- A workshop approach.

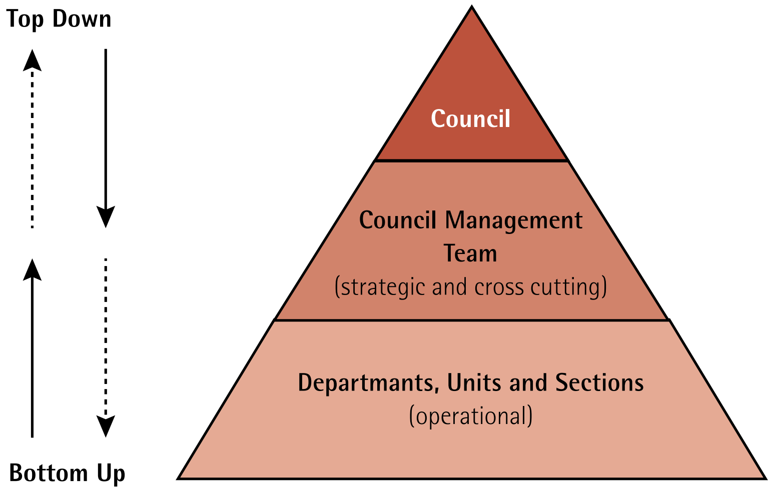
In the LGA practice, surveys and workshops have been the most widely used approaches.

- Workshop approach:
- Gathering all heads of units/departments of the LGA for two to four days;
- Staff is divided according to common objectives or departmental targets in oder to brainstorm potential risks (a special risk assessment form is used – see next session);
- Later, each group is given an opportunity to present before the whole plenary;
- All participants discuss and deliberate on the risks identified by the group.
- Survey Approach:
- A special task force or team is formed to develop the tools for risk assessment (usually a special questionnaire or a form to capture all information on risk);
- The questionnaire is distributed to all members of staff (especially heads of department/units/sections) in accordance with the LGA's objectives and targets;
- The task force later collects the completed questionnaires to summarise and prepare the risk register (see next session).

9.6 Selecting the Level for The Risk Assessment

After a choice is made on the approach for risk assessment (i.e. survey or workshop) a decision should be made on the level on which to base the risk assessment (strategic or operational level).

Figure 9: Different levels of looking at risks and their assessment


Top Down
Bottom Up
Council
Council Management Team
(strategic and cross cutting)
Departmants, Units and Sections
(operational)

The following are the implications for the choice of each of the levels:

- Strategic level – means that the risk assessment exercise will mainly focus on risks against the LGA's strategic objectives (as appearing in the strategic plan or MTEF document).
- Departmental/unit/operational level – means that the risk assessment exercise will mainly focus on risks against departmental/units targets (which usually have links to the strategic objectives of the LGA are sector-specific).

! It should be noted that the lower the level of the risk assessment, the more detailed it becomes and the more tasks will be defined. A risk assessment carried out on the operational level however also provides a very comprehensive assessment and the definition of very practical risks.

9.7 Review Questions

1. What is the difference or relationship between the following items:
   - Risk management framework
   - Risk management process
   - Risk assessment
   - Risk identification and
   - Risk evaluation?
2. What do you think are the potential advantages and disadvantages of the two risk assessment approaches namely the workshop approach and the survey approach? Which do you consider appropriate for your LGA?

Session 10

10 The Risk Management Process – Conducting the Risk Assessment

10.1 Introduction

This session is a continuation of the previous session of choosing the approach (i.e. survey or workshop) and the level of conducting the risk assessment (i.e. strategic or operational). It provides more detail by presenting the techniques for conducting the risk assessment exercise which will also lead to the preparation of the LGA's Risk Register (discussed in the next session).

10.2 Session Objectives

It is expected that, at the end of this session, the participants will be able to:

- Define the terms risk assessment and risk identification and their relationship;
- Identify, assess and document risks against their LGAs' objectives;
- Evaluate existing controls on inherent risks and propose risk mitigation measures.

10.3 Definitions

Recap: What is risk assessment?

> "Risk assessment is the overall process of risk identification, risk analysis and risk evaluation"
>
> ISO 31000:2009

What is risk identification?

> "Risk identification is the process of finding, recognizing and recording risks."
>
> ISO 31000:2009

From the definition it can be seen that risk identification is one step of the risk assessment.

10.4 Risk identification

10.4.1 Identify Relevant LGA's Objectives

Risk identification should be based on the LGA's strategic objectives or departmental targets (depending on the level chosen to base the risk assessment – see previous session).

- It is important to begin by understanding the LGA's objectives or departmental targets.
- The main source for such objectives or targets is the LGA's Strategic Plan or MTEF.

10.4.2 Identify Events that Could Affect the Achievement of the Objectives

The risk identification process includes identifying events, situations or circumstances which could have a material impact upon objectives/targets and the nature of that impact.

"Events, situations or circumstances" refers to prior and potential incidents occurring within or outside the LGA that can have an effect, either positive or negative, upon the achievement of the LGA's stated objectives.

10.4.3 Methods of Identification

There are several methods in identifying the risks including:

- Systematic team approach: A team of experts follows a systematic process to identify risks by means of a structured set of prompts or questions.
- Brainstorming session: LGA staff members grouped in terms of their sector/relationship with the objective/target and engage in brainstorming all possible events that might occur in the context of the objective/target.

10.4.4 Considerations in Risk Identification

Whatever the method of identification, the following needs to be considered when identifying risks:

- Risks should be identified based on pre-identified organizational objectives (strategic or functional);
- Both external and internal categories of risks need to be considered;
- Knowledgeable stakeholders (especially members of staff with experience/training that matches the objectives under discussion) and staff who actually work in the specific operations should be included;
- Risk identification should be a continuous process and an integral part to the organisational processes;
- Once identified, risks (along with their sources) should be clearly described and documented in a specialised risk identification form.

10.4.5 Sources of Risks

When identifying risks, the groups should consider the following possible sources of risks as shown in Table 5:

Table 5: Sources of risk

Sources of Risk	
External Sources	Internal Sources
Outsourcing to external service providers Commercial/legal changes Changes in the economic conditions Socio-political changes, like elections National and international events Behaviour of contractors/private suppliers Financial/market conditions Natural events Misinformation	New activities Disposal or cessation of current activities Personnel/human behaviour Management activities and controls Operational (the activity itself) changes Department interruption Occupational health and safety Technology/technical changes i.e. new hardware and software implementations Property/assets Security (including theft and fraud) Public/professional/product liability

10.5 Risk analysis

10.5.1 Causes and Consequences of Risks

When analysing the risks in each objective, the team should view the risk in terms of its causes and consequences i.e. situations that may lead the risk to happen and their ultimate effect on the objective/organisation.

Table 6 below presents an example of risk identification by considering both the causes and consequences:

Table 6: Example of risk identification by considering the causes and consequences

Example: 1	
Risk:	High employee turnover
Causes :	Job dissatisfaction Uncompetitive remuneration
Consequences:	Loss of corporate knowledge Delay in delivery of business objectives
Objective:	Human resource management pertaining to the organization improved

Example: 2	
Risk:	IT failure
Causes :	Power outage Software failure
Consequences:	Loss of data Delay or failure in delivery of business objectives
Objective:	Information, Communication and Technology Capacity for XYZ LGA Service Delivery enhanced

10.5.2 Assess Inherent Likelihood and Impact of Each Risk

Risks are defined as events that might occur or not with their occurrence being outside the control of the LGA. The LGA therefore has to assess two factors for each risk:

- The risk's LIKELIHOOD or probability of happening/occurring.
- The risk's IMPACT on the objective.

10.5.3 Sources of Information on Likelihood and Impact

The most relevant sources of information used in analysing impact and likelihood include:

- Past records;
- Practical and relevant experience;
- Relevant published literature;
- Market research;
- Results of public consultation, or
- Expert judgment.

10.5.4 Rating of Risks

Risks are rated using various classification band-levels:

- 5-band level: Very High = 5, High = 4, Medium = 3, Low = 2, Very Low = 1
- 4-band level: Very High = 4, High = 3, Medium = 2, Low = 1
- 3-band level: High = 3, Medium = 2, Low = 1

In this session, a 5-band level for both likelihood and impact is presented as this scheme has been adopted in the Government's Risk Management Guideline. Table 7 provides the meaning of each rate for impact and likelihood:

Table 7: Meaning of rates on impact and likelihood of risks

Number	Impact	Likelihood
5	Very High (VH) also Catastrophic	Very High (VH) also Almost Certain
4	High (H) also Major	High (H) also Likely
3	Medium (M) also Moderate	Medium (M) also Possible
2	Low (L) also Minor	Low (L) also Unlikely
1	Very Low (VL) also Insignificant	Very Low (VL) also Rare

Then Rating is made by multiplying likelihood and impact:

- The highest level of a risk is the one with a product of 25 (i.e. 5 x 5); the lowest level is 1 (i.e. 1 x 1).
- Note: The result (product) is called total risk.
- The total risk assists in indicating the priority of the risk as especially very high risks have to be dealt with.

Table 8 gives a full description on the meaning of the total risks, colour and required responses.

10.5.5 Assigning Risk Owners

Like objectives, risk fall under different areas of responsibilities. The team should make sure to assign the responsibility for risk treatment to the responsible official under whom the risk functionally falls (Department or Unit). Normally, the risk owner is assigned responsibility for the risk by the Executive Director.

A risk owner should be a person who has the ability to carry out the proposed treatment options. He/she is responsible and accountable for the risk.

10.6 Risk Evaluation

10.6.1 Evaluate the Current Controls Against the Inherent Risks

After the inherent risk rating, it is obvious that some of the risks will fall in the red, others in light brown, yellow or green colours.

The team will now need to evaluate how the LGA is controlling each of the risks i.e. by assessing the EXISTING CONTROLS (and their weakness) in order to determine the RESIDUAL RISK i.e.:

- The risk remaining even after being controlled;
- The remaining risk due to some existing weaknesses in the controls.

Questions to be addressed when assessing the current controls against each risk include:

- What are the existing controls for a particular risk?
- Are those controls capable of adequately treating the risk so that it is controlled to a level that is tolerable?
- In practice, are the controls operating in the manner intended and can they be demonstrated to be effective when required?

10.6.2 Assess the Residual Risk and Propose Mitigation Controls

The residual risk (i.e. risk after the existing controls) needs to be re-assessed to see whether it is within the LGA's TOLERABLE LEVEL.

The tolerable level of the risk is the extent up to which the LGA is ready to bear the risk after it has been treated in order to achieve council objectives. The tolerable level of risk is determined by the management and may be stipulated in the risk policy.

Again, as in the inherent risk assessment, the risk will be rated in terms of LIKELIHOOD (of happening) and IMPACT (to the objective) given the current controls.

> !
>
> It is expected that the residual risk will be lower than the inherent risks. This will happen if the existing controls are effective.
>
> If the residual risk remains above the LGA's acceptable level, more mitigation controls need to be taken to reduce the risks.

The proposed mitigation controls should be guided by the total residual risk (i.e. IMPACT x LIKELIHOOD). The last column of Table 8 below gives guidance on how to respond to each level of the total risk.

Table 8: Risk ratings, color expression and responses (Source: Risk Management Guideline, 2012)

Total Risk/Risk Status (Impact x Likelihood)	Description	Expression in Colour	Meaning and Responses
15-25	Extreme or severe	Red	Very serious concern; highest priority. Take immediate action and review regularly.
10-14	High	Light brown	Serious concern; higher priority. Take immediate action and review at least three times a year.
5-9	Moderate	Yellow	Moderate concern; steady improvement needed. Possibly review biannually
1-4	Low	Green	Low concern; occasional monitoring. Tolerate/Accept. Continue with existing measures and review annually.

10.6.3 Need for a Special Form to Record the Assessment of Each Risk

All of this information must be captured in the Risk Identification and Analysis Sheet (Refer to Template 6 in the Risk Management Guideline, 2012).

Also refer to Table 9 (at the end of this session) for a sample of a completed Risk Identifications and Analysis Sheet together with some important hints.

10.7 Review Questions

What do you understand by the terms risk assessment and risk identification?

What is the difference between assessment of inherent impact and likelihood and assessment of the residual impact and likelihood?

Pick any of your LGA's strategic objectives (as appearing in the strategic plan) and try to (in groups):

Brainstorm possible risks against the objective.

Assess the risks in terms of their inherent and residual likelihood and impact.

Evaluate the current controls against each of the risks (including their weaknesses).

Propose mitigation controls/actions to be taken to reduce the risks to a tolerable level.

Table 9: Risk Assessment Form

Risk title: Diseases Outbreak	Risk ID: 001

Overview	
Risk	Outbreak of diseases due to transmission from animal to human beings e.g. tuberculosis and rabies
Principal risk owner	City livestock and fisheries officer
Supporting owner(s)	Head of sections, and extension officers
Risk Category	Environmental
Objective/plan	Livestock diseases control

Individual responsible for the risk

Mention the objective impacted by the risk per MTEF/Strategic Plan

Details	
Causes: ▪ Lack of vaccines ▪ Lack of funds ▪ No routine vaccination ▪ Poor management	**Consequence(s):** ▪ Animal deaths ▪ Low animal productivity ▪ Low farmer income and national income ▪ Human death

Rate the risk on the assumption that current controls do not exist

Inherent risk analysis						
Inherent risk	**Impact:**	VERY HIGH √	HIGH	MODERATE	LOW	VERY LOW
	Likelihood:	VERY HIGH	HIGH	MODERATE √	LOW	VERY LOW
Risk rating	**Impact x likelihood**	15				

Controls in place to reduce the inherent risk

Key risk mitigation/controls currently in place and their weaknesses: Routine vaccination and to control livestock permit but sometimes vaccination drugs are out of stock

Remaining risk level after implementing existing controls

Residual risk analysis						
Residual risk	**Impact:**	VERY HIGH	HIGH√	MODERATE	LOW	VERY LOW
	Likelihood:	VERY HIGH	HIGH	MODERATE√	LOW	VERY LOW
Risk rating	**I X L:**	12				

Actions/mitigating controls to be taken:	
Treatment: 1. Routine vaccination 2. Farmers training on animal husbandry practices	**Resource required:** 1. Funds, vaccines and drugs 2. Transport for extension workers

Propose actions that will reduce the risk to tolerable level

Financial, physical or human resources

Session 11

11 The Risk Management Process – Risk Register and Treatment Plans

11.1 Introduction

The risk assessment process should result into the LGA's Risk Register and Risk Treatment Action plans. This session is a continuation of the risk assessment exercise and explains how the information from the risk assessment exercise will be transferred into the risk register and action plans.

11.2 Session Objectives

By the end of the session, participants should be able to:

- Define a risk register;
- Prepare the risk register and risk treatment action plans.

11.3 Definitions

What is a Risk Register?

> "A Risk register is the document used for recording the risk management process for identified risks. The purpose of the risk register is to facilitate ownership and management of each risk."
>
> ISO Guide 73

11.4 Developing the LGA's Risk Register

11.4.1 Purpose of a Risk Register

The purpose of the risk register is to:

- Form an agreed record of the significant risks that have been identified;
- The risk register will serve as a record of the control activities that are currently undertaken;
- It will also be a record of the additional actions that are proposed to improve the control of the particular risk.

11.4.2 Preparing the Risk Register

The risk register is prepared by summarizing the information collected during the risk assessment process. There are different formats for a risk register. However, the format provided by the Government Guideline for Risk Management (2012) Template 7 is recommended for use.

If a special form (e.g. Template 6 Risk Identification & Analysis Form) was used in assessing the risks, then only a selection of key information will be used to produce the register. The risk assessment forms will later be used as attachments to the register.

The following information from the risk assessment sheet will be used for preparing the register:

- The objective that is affected by the risks;
- The risk title and category (e.g. strategic, operational etc.);
- The risk identification code (each risk should be given a unique ID that connects it with the objective it affects);
- The residual risk assessment (i.e. risk by likelihood and impact with appropriate colour);
- The principle risk owner;
- The page number linking the summary to the detailed risk assessment form attached to the register;
- All of this information must be captured in the Risk Register Template (refer to Template 7 in the Risk Management Guideline, 2012);
- Refer also to Table 10 below, which shows an example of a completed Risk Register together with some important hints.

Note that the register summarises risks that fall under the same objective although these cut across departments.

Table 10: Example of a completed Risk Register

Outline the objective affected by the risk	*Transfer the risk titles appearing in identification sheet*	*As described in the Identication sheet*	*As in the identification sheet*			*Product of Impact x Likelihood*	*EXTREME, HIGH, MEDIUM or LOW*	*As in identification sheet*	*Reference to identification sheet*
Objective	**Risk title**	**Category of risk**	**Risk id**	**Residual risk assessment**		**Risk rating**	**Risk status**	**Principal risk owner**	**Page**
				Impact (I)	Likelihood (I)				
Objective C: Improve access, quality and equitable social services delivery by June 2016	Diseases Outbreak	Environmental	C:1	4	3	12	**High**	CLFO	
	Conflicts between farmers and livestock keepers	Economical	C:2	3	2	6	**Moderate**	CLFO	
	Unsustainable availability of Essential Medicines in Health Facilities	Financial	C:3	5	4	20	**Severe/ Extreme**	CMOH	
	Shortage of medical equipment, supplies and reagents in health facilities	Financial	C:4	4	3	12	**High**	CMOH	
	Prone to infectious diseases E.g. TB	Technical	C:5	2	1	2	**Low**	CMOH	

11.4.3 Drawing the Risk Heat Map

An important section of the risk register is the risk heat map (see Figure 10 below). The risk heat map presents an overview of the risks the LGA faces in one graph.

The risks from the risk register are plotted into the Heat Map. Each risk is placed in the appropriate box according to its rating.

Figure 10: Example of a plotted risk heat map (Source: Risk Management Guideline, 2012)

Likelihood	Almost Certain (5)	🟨	🟫	🟥	🟥	🟥
	Likely (4)	🟩	🟨	🟫	🟥	🟥 C.3
	Moderate (3)	🟩	🟨	🟨	🟫 C.1,C.4	🟥
	Unlikely (2)	🟩	🟩	🟨 C.2	🟨	🟫
	Rare (1)	🟩	🟩 C.5	🟩	🟩	🟨
		Low (1)	Minor (2)	Moderate (3)	Major (4)	Catastrophic (5)
		Impact				

It is obvious from a strategic point of view and with limited resources that the LGA management will be interested to see what actions are taken to deal firstly with risk C.3 (in the red region) and secondly with risks C.1 and C.4 (in the light brown region) before dealing with risks in the yellow and green regions.

The risk heat map provides a useful picture of the LGA's risk profile. It provides, at one glance, information at a high strategic level.

11.4.4 Review of the Risk Register

It is important that the risk register does not become a static document. It should be treated as a dynamic element and considered to be the risk action plan for a unit or the organization as a whole.

It is advised that the risk register should be reviewed every year. The revision of the register is usually done by undergoing the same process of risk assessment as covered earlier.

11.5 Preparing the Risk Treatment Action Plans

After preparing the risk register, it is important that risk treatment action plans are drawn. The action plan will be prepared using Template 8 in the Risk Management Guidelines, 2012.

The action plans are prepared by each of the risk owners where they are committing to implement the proposed risk mitigation measures (see an example in Table 12).

The most important information in this form, apart from those drawn from the register, is the timetable for implementation and the key indicators for risk treatment.

Table 11: Example of Risk Treatment Action Plan

As in Identification sheet

As appearing in the Action Plan

Normally will be the risk owner

Period within Financial year corresponding with the Budget for the period

Mention the means and frequency of verification

Risk title & ID	Proposed Treatment/Control Options	Person Responsible for Implementation of Treatment Options	Time-table for Implementation	How will this risk and treatment options be monitored
C:1 Diseases Outbreak	▪ Routine vaccination (3000 animals to be vaccinated)	City Livestock and Fisheries Officer	July 2013 to June 2014	Number of animals vaccinated for each villages(Monthly reports, Quarterly reports)
C:2 Conflicts between farmers and livestock keepers	▪ Livestock infrastructure to be improved e.g. Dipping tanks, Charcoal Dams and Stock routes ▪ Livestock grazing areas and Agriculture areas allocated to each ward	City Livestock and Fisheries Officer	July 2013 to June 2014	▪ Physical verification ▪ Number of infrastructure improved ▪ Livestock and Agriculture areas located
C:3 Unsustainable availability of essential medicines in Health Facilities	▪ Appointment of personnel to focus on fund returns ▪ Joint systems for requesting fund reimbursement ▪ Monthly drug audit by CHMT	City Pharmacist	July 2013 to June 2014	▪ Monthly and quarterly report ▪ Monthly audit reports
C:4 Shortage of medical equipment, supplies and reagents in health facilities	▪ Budget for procurement of medical equipment, supplies and reagents for health service care ▪ Effective management of equipment, supplies and reagents	City Medical Officer	July 2013 to June 2014	▪ Review of CCHP and procurement plan quarterly ▪ Physical verification of medical equipment, supplies and reagents. ▪ Report of inventory list
Proneness to infectious diseases	▪ Mentoring and coaching on Infection Prevention and control (IPC) ▪ IPC materials and posters to be supplied to health facilities. ▪ Adherence to Infection Prevention and control (IPC) Guideline	City Medical Officer	July 2013 to June 2014	▪ Monthly reports ▪ Physical verification of Infection Prevention and control materials (IPC) ▪ Observation of the conduct of health service providers
Compiled by: Risk Management Coordinator – Asha Rashid **Date: 19/12/2013**				

11.6 Review Questions

1. Define a risk register.
2. From your group work in the previous session, continue to develop extracts of the risk register, the heat map and risk treatment action plans.
3. From your experience, what do you perceive to be the potential challenges in your LGA in preparing and implementing the risk register and action plans?
4. Which actions can you propose to deal with the mentioned challenges?

Session 12

12 Monitoring, Evaluation and Reporting of LGA Risk Management

12.1 Introduction

The risk management framework needs to be dynamic and open for changes and improvements, especially when adopted for the first time. In this case, there is a strong need for specific efforts to monitor, review and evaluate both the risk management framework and the implementation of risk treatments which were proposed in the risk register.

12.2 Session Objectives

In this session, the risk management implementation reporting process is discussed. It is expected that the participants will be able to:

- Understand the importance of reporting in assuring the effectiveness and quality of risk management in the LGA;
- Understand the different types and arrangements in preparing risk treatment implementation reports;
- Appreciate and understand both the role and approach of internal audit in providing assurance on the effectiveness of the risk management framework;
- Prepare risk management reports.

12.3 Preparing Risk Treatment Implementation Reports

12.3.1 Types and Arrangement for Risk Management Reports

The management of risks 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.

The risk reporting should follow the requirements defined in the LGA's risk management policy and procedures/protocols, which in turn should be aligned to other reporting channels in the LGA.

A good example of a risk management reporting arrangement is given below from an LGA in the United Kingdom:

All risks on the Strategic Risk Register are monitored via quarterly reports from the clinics. Reports from these clinics are forwarded to the Executive Committee twice per year. The Strategic Risk Register is reported to full Council through its inclusion in the annual strategic plan reporting. Service-specific business risks are included within service group plans and monitored through the directorates' performance management arrangements. This includes reporting, twice per year, to relevant Council Members.

In risk management there can be different types of reporting e.g.:

- Reports based on specific priority risks;
- Reports on the status of implementing risk treatment actions plans;
- Reports on the overall effectiveness of the risk management framework (see next section).

12.3.2 Priority-based Reporting

An LGA may opt to compile reports on the treatment of identified risks based on priority, including the effectiveness of management of these risks.

This type of reporting is especially useful when aimed at both determining the frequency of reporting and hierarchy/level of the recipients of the reports in the LGA:

- "Extreme" and "High" rated risks will require immediate management attention and included in reports to audit committee or full council, and therefore will be monitored and reported on at least a quarterly basis.
- "Moderate" and "Low" rated risks may be monitored bi-annually or annually, as judged relevant, and be included in reports to middle level management and operational staff.
- All other identified risks will be monitored at least annually, and included in reports to middle level and operational staff.

12.3.3 Risk-owner Reporting

This type of reporting is also known as "stewardship reporting", where each risk owner (designated risk manager) at various levels of the LGA will have to report upwards on the status of implementation of risk treatment as proposed in the risk register. This is the type of reporting framework explained in the Guideline for Developing Risk Management Framework (2012):

- A single LGA officer (e.g. Risk Coordinator) should be given the responsibility for coordinating the reporting process.
- At the end of each quarter (if agreed to be the reporting cycle) the risk management coordinator will have to remind the risk owners about the reporting deadlines.
- Each risk owner (as mentioned in the risk register) will have to complete a risk implementation report (see Template 9 in the Risk Management Framework).

An example of a completed Risk Management Implementation Report is shown in the following table.

Table 12: Risk Treatment Quarterly Report Form

Department/Unit: HEALTH
Risk Management Quarterly Implementation Report for the Quarter Ending: December, 2013

As in Identification sheet

FromAction Plan

State whether completed, on-going, not completed

As stated in the Action Plan

As stated in the Action Plan

Risk title & ID	Proposed Treatment/Control Options	Person Responsible for Implementation of Treatment Options	Time-table for Implemen tation	How will this risk and treatment options be monitored	Status of Implemen-tation	Remarks and/or Comments
C:3 Unsustainable availability of Essential Medicines at Facility Level	▪ Appointment of personnel to focus on fund returns ▪ Joint systems for requesting fund reimbursement ▪ Monthly drug audit by CHMT	City Pharmacist	July 2013 to June 2014	▪ Monthly and quarterly report ▪ Monthly audit reports	Implemented	
C:4 Shortage of medical equipment, supplies and reagents in health facilities	▪ Budget for procurement of medical equipment, supplies and reagents for health service care ▪ Effective management of equipment, supplies and reagents	CMO	July 2013 to June 2014	▪ Review of CCHP and procurement plan quarterly. ▪ Physical verification of medical equipment, supplies and reagents ▪ Report of inventory list	Ongoing	
C:5 Proneness to infectious diseases	▪ Mentoring and coaching on Infection Prevention and control (IPC) ▪ IPC materials and posters to be supplied to health facilities. ▪ Adherence to Infection Prevention and control (IPC) Guideline	CMO	July 2013 to June 2014	▪ Monthly reports ▪ Physical verification of Infection Prevention and control materials (IPC) ▪ Observation of the conduct of health service providers	Ongoing	
Prepared by: John Jackson – (Council Medical Officer) Date: 05 December 2013						

- The Risk Management Implementation Report will require a risk owner to complete, among other items, the status of implementation of the proposed treatment, with remarks especially where the treatment is on-going, or not done.
- The risk owners will submit the completed forms to the risk management coordinator who will in turn use the forms to develop the LGA risk management report, which will include his/her findings and recommendations.

12.4 Monitoring and Evaluation of the Risk Management Framework

Relevance and usefulness of a risk management framework is largely informed by the extent to which it is continually improved.

Improvement to the risk management framework can be triggered by results of either daily monitoring activities or special reviews:

Monitoring:

- Monitoring means continual checking, supervising, critically observing the status in order to identify change from the performance level required or expected.

Reviews/Evaluations:

- Reviews are aimed at determining the suitability, adequacy and effectiveness of the risk management framework, risk management process and controls.
- This can be done by the LGA Management, Internal Audit or any external independent body (e.g. the external auditors from the CAG or risk management champions from the Internal Auditor General Division).

12.4.1 Evaluation by the LGA Management

In the Guidelines for Developing Risk Management Framework (2012), it is explained that monitoring and review at the LGA level should first be carried out by management.

This should normally be done through periodic reporting on the way risk management strategies and controls are being implemented.

It is also advised that when monitoring and reviewing are combined together, they should aim at ensuring that:

- Risks are being effectively identified and appropriately analysed;
- There is adequate and appropriate implementation of risk management strategies and controls;
- There is effective monitoring and review by management and executives to detect changes in risks and controls.

The results of such reviews should always lead to a report on the finding and recommendation for improvement.

12.4.2 Evaluation by the Internal Audit Unit

By definition of their profession, the Internal Audit Unit is providing independent assessments of risk management.

There are two ways through which Internal Audit Units achieve this role:

- Evaluating the effectiveness of the risk management framework, i.e. conducting specific assessments of the risk management process (i.e. auditing on how the LGA has identified the risks it is facing);

- Conducting risk-based audits (i.e. focusing their audit efforts on the most risky areas as indicated by the LGA management through the risk register).

In either situation, reports from internal auditors should indicate findings and recommendations on the state of the overall risk management framework, the effectiveness of controls in mitigating the risks as proposed in the register.

12.5 Review Questions

What are the objectives for risk management reports in the LGA?

In chapter 12.7.3 the reporting arrangement for UK's LGAs was outlined; briefly formulate a customised risk reporting arrangement that will align with your LGA's normal reporting channels.

In most LGAs the Internal Audit Unit is given the role of championing and coordinating risk management activities. Do you think there is any problem with this role, especially when the internal audit unit is also required to evaluate the effectiveness of the risk management activities in the LGA? What would you suggest do be the best arrangement?

Bibliography

Concise Oxford Dictionary (2011), Oxford University Press. Oxford.

COSO (2004) Enterprise Risk Management - Integrated Framework, available online at http://www.cpa2biz.com/AST/Main/CPA2BIZ_Primary/InternalControls/COSO/PRDOVR~PC-990015/PC-990015.jsp

Hopkin, P. (2010), Fundamentals of Risk Management, Understanding, Evaluating and Implementing Effective Risk Management, Kogan Page, London.

Internal Auditor General Division, Ministry of Finance (2012), Guidelines for Developing and Implementing Institutional Risk Management Framework in the Public Sector, Dar es Salaam.

International Risk Management Institute – IRMI (2004), Embedding Risk Management, Dallas.

International Standards Organization (2009), ISO 31000:2009, Risk Management Principles and Guidelines, Geneva.

International Standards Organization (2009), ISO Guide 73:2009 Risk Management Vocabulary, Geneva.

PriceWaterHouseCoopers (2008), A practical guide to risk assessment. How principles-based risk assessment enables organizations to take the right risks, London.

Public Finance Act (2001, amended 2010), Government Printers, Dar es Salaam.

Treasury Circular no.12 of 2012/13, Ministry of Finance, Dar es Salaam.

Published by
Deutsche Gesellschaft für
Internationale Zusammenarbeit (GIZ) GmbH

Support to Local Governance (SULGO) Programme
325, Isimani Road, Upanga
P.O. Box 1519
Dar es Salaam
Tanzania

T +255 22 215 0761/215 2028
F +255 22 215 3249
E sulgo-dsm@giz.de
I www.sulgo.or.tz

Photo © Andreas Korn

Design and Layout:
andreas korn visual communication, Dar es Salaam

Responsible:
Philipp Schattenmann

Dar es Salaam, April 2014