Risk Management Framework & System Development Guidelines

Table of Contents

1. Risk Management Framework and System development guidelines ..... 3~~2~~
1.1. Introduction ..... 3~~2~~
1.2. Common Minimum Risk Management Structure ..... 4~~3~~
2. Risk Management Principles ..... 4~~3~~
2.1. Introduction ..... 4~~3~~
2.2. Risk Management Principles ..... 4~~3~~
3. Risk Management Framework ..... 5~~4~~
3.1. Introduction ..... 5~~4~~
3.2. Essential components of the framework ..... 5~~4~~
3.3. Risk Management Architecture ..... 6~~5~~
3.3.1. Risk Management Committee ..... 6~~5~~
3.3.2. Risk Management Strategy ..... 8~~7~~
3.3.3. Risk Management Protocols ..... 13~~12~~

1. Risk Management Framework and System development guidelines

1.1. Introduction

The purpose of these guidelines is to establish a common understanding of risk management and provide a step by step guidance to organizations to support them developing their own risk management processes, including a system, strategy and policy.

These guidelines set out a basic common structure for risk management process, system, strategy and policy, to support the organization in understanding the process to develop these products, followed by guidance notes to achieve them.

In these guidelines:

- The term **standard** refers to international standards[1];
- The term **common** refers to commonly and widely used **criteria** in risk management by a number of international NGOs, UN system members, donors and publicly available in the technical reports and guides;
- The term **basic** refers to commonly and widely used norm for basic **condition** in risk management;
- The term **minimum** refers to the **lowest acceptable level** of in risk management;
  Unless otherwise stated, the term **committee** refers to a risk management committee, subcommittee or working group;
- For the purposes of risk management, the term **quality of delivery** refers to **a holistic process approach** to ensure the quality of humanitarian assistance and service provided to affected people in Syria. The working definition for quality of delivery is the extent to which the assistance services provided to affected people improve the desired outcomes. To achieve this, the assistance services provided must be **safe, effective, timely, efficient, equitable** and **people-centered**, and in a manner, which considers the preferences and aspirations of individual service users and the culture of their community.

The holistic nature of the approach as indicated by the term quality of delivery is such that the risk analysis seeks to enable management of internal and external risks. For example, internal risk management to ensure quality of delivery enables humanitarian staff to be trained, capacitated, and safe in terms of their professional well-being to provide quality support to the affected population when serving their needs. External risk management seeks to enable the management of risks in the operational environment, such as interference, aid diversion, or security threats.

[1] ISO31000, 31004, 31010 – Risk Management Standards, publicly available, and widely used by several international NGOs and UN system agencies.

1.2. Common Minimum Risk Management Structure

The basic common minimum risk management structure comprises three main elements:

I. **Risk Management Principles** is a set of eight basic common minimum principles which guide the risk management activities;
II. **Risk Management Framework** is an overall structure and operation of risk management across the organization; and
III. **Risk Management Process** defines how risks are identified, analyzed, and treated.

All these three elements are detailed separately in the following sections.

2. Risk Management Principles

2.1. Introduction

The purpose of risk management is to identify possible risks, their likelihood and impact on resources. The objective of the risk management process is to create a system and processes to protect people and humanitarian resources of value. The risk management process does not focus upon risk avoidance but on the identification and management of an acceptable level of risk to strengthen the project management through adequate forward planning of potential risks. The best system aims to mitigate and prevent the impact.

A best practice approach to risk management is to embed it within the daily operation and functions of any organization, from strategy formulation through to policy, planning, and implementation. Through understanding risks, organisations decision-makers are better able to evaluate the impact of a particular; 'decision' or 'action' on the achievement of the organization's objectives.

Hence, risk management principles aim to provide guidance on the characteristics of effective and efficient risk management, communicating its value and explaining its intention and purpose. Therefore, risk management principles must influence the design and implementation of organization's risk management framework and process.

2.2. Risk Management Principles

There are eight principles set out in international standard to provide guidance on the characteristics of effective and efficient risk management. The first five principles provide guidance on how a risk management process must be designed, and principles six, seven and eight relate to the operation of the risk management process. These principles are:

I. Risk management framework and processes must be customized and proportionate, tailored to create and protect value.
II. Appropriate and timely involvement of stakeholders in effective risk management is necessary in order to be transparent and inclusive.
III. Risk management requires a systematic, structured, comprehensive and timely approach.
IV. Risk management is an integral part of all organizational activities as well as decision making.

V. Risk management anticipates, detects, acknowledges and responds to changes and explicitly addresses uncertainty.
VI. Risk management explicitly considers any limitations of available information and is based on the best information.
VII. Human and cultural factors influence all aspects of risk management.
VIII. Risk management is continually improved through learning and experience and facilitates continual improvement of the organization.

The principles of risk management and a risk management framework are closely related. For example, one of the principles is that risk management must be integrated and one of the components of the framework is integration. The principle outlines what must be achieved, and the framework provides information on how to achieve the required integration.

3. Risk Management Framework

3.1. Introduction

The purpose of the Risk Management Framework is to outline a Risk Management System which facilitates the effective and timely recognition and management of risk facing the organization.

The Risk Management System is the framework of policies, processes and procedures employed by the organization to ensure that it can fulfill the risk management tasks required to achieve its purpose and objectives. These objectives will cover all aspects of the organization, including strategy, governance, operations and compliance.

Furthermore, risk management framework determines how risk management is integrated with the organization's management system. Therefore, a well formalized risk management system has defined, documented processes that are intended to explicitly manage the process within the organization. These will be auditable standards developed for each activity or process. Furthermore, it includes roles and responsibilities, compliance and management of change through communication, therefore, these formalized processes are essential and important.

3.2. Essential components of the framework

The following are the essential components of the framework;

- **Risk Management Architecture** defines the roles and responsibilities of the individuals and committees/departments/units that support the risk managing process.
- **Risk Management Strategy** outlines the objectives of the risk management activities in the organization.
- **Risk Management Protocols** determines how the strategy will be implemented and risk managed.

3.3. Risk Management Architecture

The guidelines in this section are centered on leadership and commitment. The effectiveness of risk management will depend on its integration into all aspects of the organization, including decision-making. The remaining components of the framework are design, implementation, evaluation and improvement. This approach is often represented in management literature as Plan-Do-Check-Act.

Integrating risk management into organization's existing management activities will ensure that risk information is part of the management information used by senior management. This will help overcome the perception that risk management is concerned only with compiling and managing a list of risks and this can be undertaken separately from the day-to-day management of the organization and the development of strategy for the future.

The guidelines provide a narrative description of how the framework must support risk management activities in the organization. This is often referred to as the risk architecture, strategy and protocols of the organization, and the extent of leadership and commitment that is required, and the range of activities involved in designing and implementing the risk management process.

The information provided aims on how to examine both the external and internal context of the organization. There is guidance on articulating risk management commitment, assigning roles and responsibilities and allocating resources and on establishing communication and coordination.

The components of establishing the risk context are described as defining the purpose and scope of risk management activities; establishing the external, internal and risk management context; and defining the risk criteria. Defining the risk criteria involves specifying the amount and type of risk that the organization may or may not take, relative to objectives; usually referred to as the 'risk appetite' of the organization.

3.3.1. Risk Management Committee

The objective of a Risk Management Committee is to encourage a culture change throughout the organization by promoting risk management awareness and practices. It oversees organization-wide risk management process and policy of continuous risk identification and assessment, defining the risk appetite, developing risk mitigation strategy and processes, and reporting and communicating on risks. The committee ensures coordination and evaluation of the risk management process.

Overall risk governance responsibility rests with the organization's top management, risk management is coordinated and monitored by the risk management committee. The primary responsibility for identifying risks and managing them lies with management/risk owners at all levels. Responsibility for implementation of the risk management; process, strategy and system, is shared by all staff within an organization. *Risk Management is everyone's responsibility.*

The Risk Management Committee acts as an information platform on best practice in handling and/or identifying risks and discusses possible actions to prevent and mitigate risks or contain further risks from affecting the organization, particularly the major risks identified during the process.

The committee may be used as a platform for risk owners to share their experience on past or perceived future risks and to support the setting up of an organization-wide risk management strategy. As such, the committee is recommended to be a formal structure used to support risk-based decision-making and oversight across all operations across the organization.

❖ **Committee Structure and membership**

- A risk management committee must be structured to adequately represent all departments/units of the organization;
- Committee members must be the unit heads/senior managers or equivariant with appropriate decision-making authority;
- The committee's work process needs to be impartial, it must be given appropriate authority and proportionate independence to avoid any bias in decision-making.

❖ **Terms of Reference**

- The committee's terms of reference must be comprehensive and developed in a holistic way to encompass the organization's risk management requirements sufficiently, thus, enabling an effective and efficient robust risk management culture.
- Senior management is responsible to develop these terms of reference.
- Risk management culture is a combined set of individual and organizational values, attitudes, competencies and behaviors that underpin the organization's commitment to risk management.

➢ **Guidance Notes**

The following are essential contents to be included and detailed in the terms of reference;

I. *Purpose or Objective of the Committee*; this must be very specific and formulated to the organization's specific risk management needs.

II. *Composition and Structure*; includes number of members, type of membership, committees' organogram, and members' titles if any.

III. *Frequency of Meetings*; how often the committee will meet, how the proceedings of these meetings will be documented, and who will participate in the meetings. The committee may also function between meetings through correspondence and any decision(s) taken formally and ratified at the next meeting of the committee.

IV. *Roles and Responsibilities*; what will be the role and responsibility of each member of the committee, and what would be the hierarchy among the members.

V. *Standing Agenda*; the committee meetings will be conducted in accordance to an agenda which must be in line with organization's risk management policy and process.

VI. *Functioning and Responsibilities*; are the activities the committee will undertake in line with the organization's risk management policy.

VII. *Authority*; details of the authority level of committee, what the committee is authorized to do, as well as the level of decision-making this authorization entitles.

VIII. *Reporting Responsibilities*; details of committee's reporting line and frequency. Additionally, it also outlines organization's internal reporting and documentation requirements for the committee ensuring proper documentation of the committee's decisions. Furthermore, reporting responsibilities also underpin the external reporting controls for the committee.

IX. *Review of Performance*; how the committee will undertake its performance review, who will be responsible for this review and what will be the frequency for this review. This is part of risk management compliance monitoring and reporting; and act as a risk management assurance arrangement.

X. *Secretariat and Resources*: outline of how and by whom the committee will be provided the secretariat functions including needed resources both human and financial.

3.3.2. Risk Management Strategy

An organization's senior management holds overall responsibility for managing the organisation's risks; it is important for the senior management to go further and enhance the conversation with the organization's board/executive body and stakeholders. Risk management plays a strong supporting role at board/executive body level to provide robust oversight of risk management. Hence, the risk management strategy provides important information for board members to define and fulfil their risk oversight responsibilities. These considerations include governance and culture; strategy and objective-setting; performance; information, communications and reporting; and the review and revision of practices to enhance the performance of the organization.

Through enhanced risk management, senior management gains a better understanding of how the explicit consideration of risk may beneficially impact the choice of strategy. The risk management strategy must acknowledge stakeholder engagement, seeking greater transparency and accountability for managing the impact of risk, while critically evaluating leadership ability to embrace opportunities.

The strategy must support the organization and board members to be more adaptive to change, and to think strategically about how to manage the increasing volatility, uncertainty, complexity and ambiguity of the context and humanitarian landscape. A sound risk management strategy must provide the organization with a proactive approach to risk and risk management, and enable it to achieve the following four areas of improvement:

I. **Strategy**; because the risks associated with different strategic options will be fully analyzed and better strategic decisions will be reached.
II. **Tactics**; because due consideration will have been given to selection of the tactics/methodology to gain organization's objectives and the risks involved in the alternatives that are available.

III. **Operations**; because events that can cause disruption will be identified and actions taken to reduce the likelihood of these events, limit the damage and contain the cost.
IV. **Compliance**; will be enhanced because the risks associated with failure to achieve compliance with statutory and stakeholders' obligations will be recognized.

Organizations must take their responsibility to plan to mitigate or prevent foreseeable issues, such as financial loss, disruption to normal operations, damage to reputation and loss of presence in the area. Stakeholders now expect that organizations take full account of risks that may cause non-compliance with statutory obligations; disruption and inefficiency within operations; late delivery of projects; or failure to deliver promised strategy.

Integrating consideration of risk into existing management activities will ensure that risk information is part of the management information used by senior management. This helps overcome the perception that risk management is only concerned with compiling and managing a list of risks and this can be undertaken separately from the day-to-day management of the organization and the development of strategy for the future.

❖ **Risk Management Strategy**

A sound risk management strategy must:

- Provide the organization with a proactive approach to risk and risk management, and enable it to achieve; strategy, tactics, operations and compliance;
- Be proactive in terms of from incident response to risk management and must avoid the traditional call for help after something has already happened;
- Be defined as a document that contains the following minimum components;
    - A description of each risk identified, and the organization's approach to managing these risks;
    - A list of the policies and procedures dealing with risk management matters;
    - The role and responsibilities of the risk management function;
    - A description of the risk governance relationship between the board/executive body, risk management committee and senior management with respect to the risk management framework;
    - An outline of the approach to ensuring all persons have awareness of the risk management framework and for instilling an appropriate risk culture across the institution.

➢ **Guidance Notes**

Below are essential contents to be included and detailed in risk management strategies;

I. *Introduction* as a brief statement on organization's risk management approach as well as how it envisions to implement the risk management process.

II. *Objective* that is specific and formulated to capture the organization's risk management approach and is normally written by the board/executive body.

III. *Definitions* to communicate the commonly used risk terms to promote a consistent understanding within the organization. These definitions could be customized to organization's risk management policy, however must be aligned to common and widely practiced risk management standards.

IV. *Principles of Risk Management* that underpin the organization's risk management process. It could be the organization's interpretation of risk management principles, the eight basic common principles set out in international standard, and how the organization will utilize these principles in management and implementation of its day-to-day operations.

V. *Responsibilities* to define responsibility for developing the organization's approach to risk management and who will be responsible with the day-to-day management of specific risks. These different roles and their respective responsibilities, authorizations and reporting protocol must be detailed.

VI. *Process* to outlines a framework to align responsibilities for control and assurance activities for the risk management, known as three lines of defense.

A. **Execute Controls**; is a control activity. It comprises of board/executive body, senior management committees, and delegated authority. It attributes to implementation, ongoing maintenance and enhancement of the risk management framework, including identification and effective management/mitigation of risks.
B. **Monitor Controls**; is crosscutting between control and assurance. It includes risk management committee and attributes in risk management to be leveraged to benefit the whole organization. Its scope includes all risk types and categories. Furthermore, it facilitates the organization and management to understand aggregated risk positions and support in developing and advising on risk strategies.
C. **Assess Controls**; is assurance activity, an independent assurance that the risk management framework has been complied with and is operating effectively. Therefore, a periodic comprehensive review of the appropriateness, effectiveness and adequacy of the risk management framework, is included in both in the risk management strategy as well as in risk management committees' terms of references.

However, this would be organization's internal decision to follow other model of enterprise risk management[2].

[2] There are mainly three enterprise risk management models; *COSO framework on enterprise risk management (sees risk management primarily as a compliance activity), Australian/New Zealand risk management standard, AS/NZS 4360, and International Organization for Standardization (ISO) – ISO 31000, 31004 and 31010*.

VII. *Monitoring* of risks and performance against 'Appetite' is the essence of risk management and integral part of risk compliance. It is the process and approach the organization applies to the ongoing review of the risk profile including progress in implementing remedial actions where necessary.
The progress made in mitigating the risks listed in the risk register must be monitored regularly in order to determine the residual risk, which need further action(s) or acceptance.

VIII. *Risk Documentation* is one of the outputs of the risk management process and is vital part of institutional memory. The organization must maintain risk documentation properly in line with its documentation and archiving policy if any. Risk documentation must be available to all staff with information on risk management (including policy, templates, training materials, risk management committee minutes, risk register, and board/executive body documents.

IX. *Business Continuity Planning* reflects certain risks impact upon the organization's ability to maintain operations during times of change or disruption. These risks feed the business continuity planning cycle.

X. *Policy Review* is vital for effective risk management and is cross cutting to both compliance and assurance. Hence, effective risk management requires a reporting and review structure to ensure that risks are effectively identified and assessed, and that appropriate controls and responses are in place.
Regular compliance/audits must be carried out and changes in the context and the environment in which the organization operates must be identified and appropriate modifications made to systems.
The review process must provide assurance that there are appropriate controls in place and that the procedures are understood and followed. The management must ensure that the agreed control measures continue to be applied.

XI. *Terms of Reference of the Risk Management Committee*; please refer to section 3.3.1 'Terms of Reference' pp. page 7 for details.

XII. ***Risk Appetite Statement*** articulates the amount and type of risk that the organization is prepared to pursue, retain or take in pursuit of its objectives. It is informed by changing variables, such as reported results of control-mechanisms that have succeeded or failed in the past, the changing value of assets potentially to be lost, perception of stakeholders, extent of possible control, etc.
It helps to guide management and staff within the organization on the level of risk permitted and encourage consistency of approach across the organization.

The risk appetite generally expressed by a broad statement of approach, which is written by the executive body/board of the organization. The executive body/board sets the Risk Appetite for the organization. Risk appetite provides the basis to set acceptable levels of risk tolerance and thresholds and contributes to the identification and implementation of mitigation actions.

The organization's risk appetite must always be less than its risk tolerance. Strategy, financial planning and risk appetite are integrally connected. Ideally, risk appetite statements must be developed for each risk category and sub-category.

XIII. **Risk Tolerance** is the organization's attitude to risk; risk tolerance is the amount of risk the organization can withstand. The line of tolerability depends on impact and likelihood. It separates the low and medium risks an organization is willing to take from the medium and high risks it is not willing to take.

Tolerance levels may be set out in the organization's relevant policies and procedures; if not, the senior management makes the judgment.

XIV. ***Risk Assessment and Risk Classification*** is the process and approach applied to the identification of risks and opportunities facing the organization. The level of risk that is accepted in a given context based on the current values of the organization.

Once risks are identified, they are then categorized. The risk categories must reflect the nature of activities organization carries. The use of risk categories is central to making the link between risk strategy and risk appetite and provides a link between the organization's overall strategy and risk management.

The risk categories must be used to aggregate specific risks for reporting purposes. Reporting using risk categories enables a view of risk across the organization and provides a mechanism for aggregation.

XV. ***Risk Register*** aims to formulate the risks faced which can be mitigated to some degree by taking the time to develop a risk management approach to help cope with threats and maximize opportunities.

The format and contents of the risk register is the formal output of the risk management process.

The risk register is used as a risk management tool and acts as a repository for all risks identified and includes additional information about each risk such as risk category, description along with their impact and probability, risk inherent rating, risk owner, mitigation measures.

The risk register is maintained as outlined in the risk management policy and sent to the secretariat of the risk management committee accordingly.

The risk register is revised regularly to assess residual risks and update mitigation measures. Furthermore, it must lend itself to be easily maintained

and updated. By remaining current and up to date, the risk register can be a valuable tool for communications and may serve as a relevant and useful management tool.

If a risk cannot be effectively treated at operational level managing the respective risk register, this must be indicated and communicated in accordance with the risk management policy.

3.3.3. Risk Management Protocols

Risk management protocols articulate the risk management process and describe risk assessment and risk treatment as being at the center of the risk management process. Although the risk management process is often presented as sequential, in practice it is iterative. Risk assessment is described as having the three stages of risk identification, risk analysis and risk evaluation.

The successful implementation of a risk management process is an ongoing process that involves working through the following 10 activities on a continuous basis following the risk management protocols. These activities relate to the following four components: *Plan*; *Implement; Measure; and Learn;*

Plan

- Identify intended benefits of the risk management process and gain senior management's support.
- Plan the scope of the risk management process and develop common language of risk.
- Establish the risk management strategy, framework and the roles and responsibilities.

Implement

- Adopt suitable risk assessment tools and an agreed risk classification system.
- Establish risk benchmarks (risk criteria) and undertake risk assessments.
- Determine risk appetite and risk tolerance levels and evaluate the existing controls.

Measure

- Evaluate effectiveness of existing controls and introduce improvements.
- Embed risk-aware culture and align risk management with other activities in the organization.

Learn

- Monitor and review risk performance indicators to measure risk management contribution.
- Report risk performance in line with obligations and monitor improvement.

Therefore, the following are recommended as the basic minimum risk management protocols to implement risk management effectively and efficiently;

- Tools and techniques

- Risk classification system
- Risk assessment procedures
- Risk control rules and procedures
- Responding to incidents, issues and events
- Documentation and record keeping
- Training and communications
- Compliance procedures and protocols
- Reporting/disclosures