DOCUMENT TITLE:

Collaborative Risk Management (CRM) for the aid stakeholders of Somalia: Implementation Plan (Part C of A/B/C)

SPONSOR:

UNITED NATIONS
SOMALIA

Risk Management Unit of the Integrated Office of the Deputy Special Representative of the Secretary General, UN Resident Coordinator and Humanitarian Coordinator (DSRSG/RC/HC) of Somalia. Funding under Joint Programme of Enablers.

CUSTODIAN:

Multi Party Risk Working Group representing Aid Community in Somalia

AUTHOR:

International Risk and Strategy Consultant:
Tarald Jarlsen
[CMIRM, RMP/PMP, MBA, Dipl. Acc., B. Eng. Hon.]
[Operations Director at Gerald & Aldger SL (www.geraldandaldger.com)]

ATTRIBUTES:

Document Date:	30th of July 2020
Document Version/Status:	Version DRAFT
Document Page(s):	1 of 22

CONTENTS

SECTION 1 GENERAL FOR THIS DOCUMENT

About this document

This document describes a structured collaborative risk management strategy (SCRM) for the aid organisations operating in Somalia. The elements of the SCRM described within this document comes as a result of the capacity and capability assessments carried out during March 2020, and the conclusions drawn from there, documented in the report "*Collaborative Risk Management (CRM): Capacity and Capability Assessment for the aid stakeholders of Somalia*", issued on the 30-Aug-2020.

Basis for this document

This document is based on the conclusions described in the preceding part for this document – i.e. "*Collaborative Risk Management (CRM): Capacity and Capability Assessment for the aid stakeholders of Somalia*", UN-Risk Management Unit; by JARLSEN, Tarald.

About the author of this document

Tarald Jarlsen has +25 years of international experience in the areas of operational/program and organizational business risk-position analysis, risk management, implementation of risk management frameworks, and strategy development as well as implementation thereof. On a daily basis, Tarald serves as a *partner* and *principle risk and risk management advisor* in the Spain-based risk and strategy consulting firm, Gerald & Aldger SL (www.geraldandaldger.com). For any comments to this document or clarifications to it, Tarald can be reached on tarald.jarlsen@gmail.com or +34 658 439968 (or at tarald@geraldandaldger.com).

About the readers of this document

The users of this document are the Somalia aid community; covering the spheres of humanitarian, development and peacebuilding activities; which include Government of Somalia, international NGOs, local NGOs, donor organisations, donor countries (via local embassies), UN agencies, and private bodies. The main custodians, Multi-Party Risk Working Group, for collaborative risk management are an array of risk working groups (RWG) across the Somali aid community – entities such as UN RWG, SDRF pooled funds (UN/WB/AfDB) Risk Management Group, Trust Fund RWG (SDRF pooled funds). The UN´s Risk Management Unit (UN-RMU) currently has a coordination, advisory and capacity building role across the aid community.

Key Definitions

The below definitions are valid for this document´s context, only.

Abbreviations

CCA	Capacity and Capability Assessment
CRM	Collaborative Risk Management
FGS	Federal Government of Somalia
FGS	Federal Government of Somalia
HSSEQ	Heath, Safety, Security, Environment, Quality
KRA	Key Risk Areas
KRI	Key Risk Indicator
KRP	Key Risk Parameters
MPRWG	Multi-Party Risk Working Group
ORSA	Operations Readiness/Risk and Solvency Assessment
PMP	Project Management Professional
RBM	Results Based Management
RFP	Risk Focal Points
RM	Risk Management
RWG	Risk Working Group
SCRM	Structured Collaborative Risk Management
SDRF	Somalia Development and Reconstruction Facility
SOX	Sarbanes-Oxley Act
SWOT	Strength /Weakness /Opportunity /Threat
TOR	Terms of Reference
TOR	Terms of Reference
UN-RMU	UN Risk Management Unit

Terminologies

Accountability	The means through which power is used responsibly: a process of taking into account the view of, and being held accountable by, different stakeholders' interests, and primarily the people affected by authority or power.
Accountability	The means through which power is used responsibly: a process of taking into account the view of, and being held accountable by, different stakeholders' interests, and primarily the people affected by authority or power.
Collaboration	Working together to produce something
Collaboration	Working together to produce something
Collective Risk Management	A joint mechanism to better manage common risks by a more transparent and informed strategic approach, as well as to cultivate higher transparency in order to reduce corruption risks.
Effective Risk Management	Effective risk management is when the right combination of risk management principles is formed together to fulfil the *risk management purpose*.
Fund Risk Management Strategy (FRMS)	FRMS seeks to: i) accelerate delivery and increase fund impact; ii) ensure that fund operations 'do no harm'; iii) verify that funds are used for their intended purpose, iv) build risk management capacity of institutions
Governance Strategy Risk	Risks emanating from fund's ties to a broader and governed aid architecture. For example: fund allocations not aligned to strategic objectives and/or poorly prioritized fund allocations.
Opportunity Potential	The likelihood of an event with positive impact on in relation to the achievement of a stated objective.
Pooled Funds	Pooled fund is a risk sharing mechanism, enabling stakeholders to take on high fund-risk together than each individual stakeholder could take on alone.
Programmes / Operations Risk	Risk emanating from programme design and implementation. For example: weak capacity of implementing partners; diversion of funds; poorly designed fund interventions.
Risk Assessment	Establishing the impact and likelihood of a negative event, for a organisation
Risk Confidence	Level of certainty established in a risk analysis by its quality and quantity of the underlying objective evidence, supporting the risk position estimations.
Risk Context	The broader perspective to risks emanating from the wider territorial context. For example: risk of state failure, risk of return to conflict, etc.
Risk Exposure	Risk Potential at a given point of time, or period, accounted for risk manageability and risk confidence.
Risk Immediacy	A risk potential at a given point of time, or, within a given period.
Risk Manageability	The sum of favorable factors put together to manage a risk position. Such factors typically.: resources, budget, time, knowledge, information, decision taking authority, etc.
Risk Management	Risk management is designed to reduce risks to and of governments, the fund administrators, financial contributors, and recipients through a comprehensive risk-based and results-based approach.
Risk Management Purpose	The risk management principles set the foundational building blocks for the design of an organization's risk management framework and processes. Essentially, such principles seek to create and protect organisations value, to improve performances, encourage innovations, supports achievement of objectives.
Risk Potential	The likelihood of an event with negative impact on in relation to the achievement of a stated objective.
SDRF Governance Structure	Governance structure that brings together UN agencies, international financial institutions, FGS agencies and donors, as a platform for understanding of the risk context and effective mitigation measures.
Strategy	A chosen road map between a current state operation to a chosen future new

SECTION 2 ABSTRACT, BACKGROUND AND INTRODUCTION

2.1 ABSTRACT

The risk management is a central part of Somalia aid organization's strategic management – i.e. as so also for any organization – this, as it is purpose to create and protect value in organizations by managing risks, making decisions, setting, and achieving objectives and improving performance.

It is the collective and collaborative set of risk management business process and functions whereby organizations methodically address the risks related to the business activities – all aiming to reach the strategic and operational business or mission objectives. It is iterative in nature and assists these aid organizations in setting strategy, achieving objectives, and making informed decisions pertaining development and humanitarian efforts.

Further, risk management forms part of governance structure and is fundamental to how these organization are managed at all levels, and it contributes to the improvement of management systems, as well being part of all activities that includes interaction with stakeholders.

This CRM approach should:

- …be largely based on the principles, framework and processes outlined in ISO 31000 and COSO – however, fitted for own local needs – i.e. as illustrated by Figure 2.1.
- …consider both the external and internal context of these aid organization, including human behaviour and cultural factors.
- …account for the potential upside and downside of all those factors which can affect the organization. In practice, that would be to decrease likelihood and/or impact of negative events or exploit the opposite opportunity-position.
- …be a continually developing process which runs throughout the participating organization's implementation of that strategy.
- …address the internal and external risks.
- …be integrated into the culture of the organization with an effective policy and a program led by key dedicated staff – or the CRM Coordinator.
- …translate the strategy into tactical and operational objectives, assigning responsibility throughout the organization.
- …support accountability.

This CRM approach protects and adds value to the organization by supporting the organization's achievement of objectives by. How?

- *framework for a consistent and comparable CRM approach.*
- *risk knowledge, advancing planning and prioritization capabilities.*
- *reducing volatility in the essential operations.*
- *protects company operations.*
- *developing and supports people within the collaborating organization.*

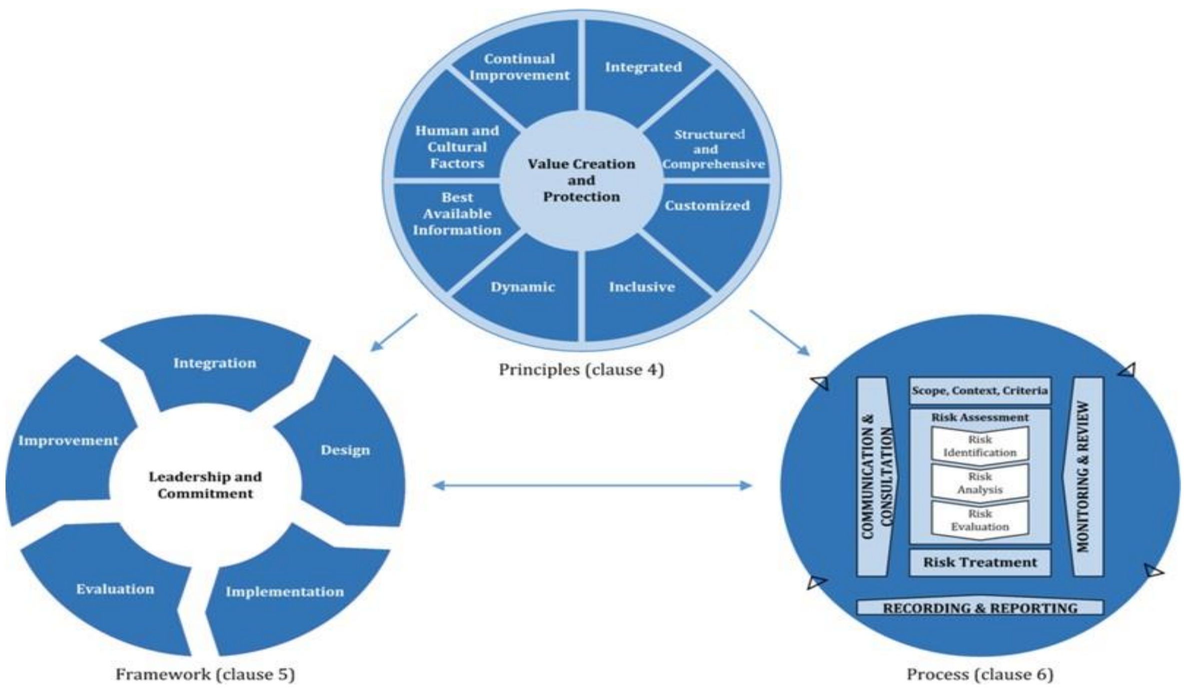

Figure 2.1 – The ISO 31000 Overall RM Framework Model

2.2 BACKGROUND

2.2.1 The Somalia risk context

The main actors of the Somalia aid community have provided humanitarian and development aid activities across the region for +20 years. The main risk stakeholders are I-NGOs, N-NGOs, donor organisation, UN agencies, Somali government bodies, and private sector and beneficiaries.

Today, from an external surface view of Somalia´s risk context, it is observable an abundant manifestations of weakness of governance, accountability, and rule of law, criminality, independent armed groups; limited access to populations in need, rampant corruption throughout the entire value chain of humanitarian and development funding cycles.

Also, today, from a viewpoint inside the aid organisations operating in Somalia they see individual RM effectiveness needs to be higher in order to combat the indeed one most challenging operation in the world.

The RM practices so far have shown that some of their applied tools and approaches have worked effectively. However, the aid community would benefit from further streamlining RM practices, strategies, systems, procedures, etc.

By default, the primary risk categories, and sequence priorities, within this community are:

i) *Contextual risks* (Somalia-on-the ground- risks).
ii) *Program risks* (Strategy execution, Governance and Control of funding of programs and/or initiatives for development, humanitarian, peacebuilding or enhancement, and the efficiency thereof;
iii) Institutional risks (corruption, fiduciary, change agenda, other).

Aid organization in Somalia have externally focused mission objectives – i.e. of aiding the vulnerable people of Somalia. Otherwise their own existence there could not be adequately justified. It follows from that the risk management functions also ought to directly support these objectives, and hence also the risk factors associated with their mission objectives.

This study also reveals that the actual predominant way of prioritising risk management activities is in the reversed order of: *i) institutional risks, ii) program risks, iii) context risks*.

2.3 INTRODUCTION

This document is based on the preceding documents, Part A: "*Collaborative Risk Management (CRM): Capacity and Capability Assessment for the aid stakeholders of Somalia*"; and Part B: "*Collaborative Risk Management (CRM): Strategy.* With reference to Figure 2.1, this document addresses the Clauses 4, 5 and 6 separately (i.e. Principles, Leadership and Process; respectively).

The overall structure of the collaborative risk management strategy implementation plan is comparable with Figure 2.2 - i.e. which was applied during the capacity and capability assessment. (Note here that Figure 2.2 is a further breakdown of Figure 2.1). This document will go through these main elements. The structure of this document will follow the main elements of Figure 2.2 – i.e. parts I, II, III, IV, and V. However, the parts I and II will only be introduced very lightly as such has already been covered by the document, Part B: CRM Strategy. The main bulk of this document will comprise of Pat III. However, part III.1 is omitted as such has been defined through all documents. Parts IV and V are also only lightly introduced as the development of such scopes is beyond the scope of this document to develop / define.

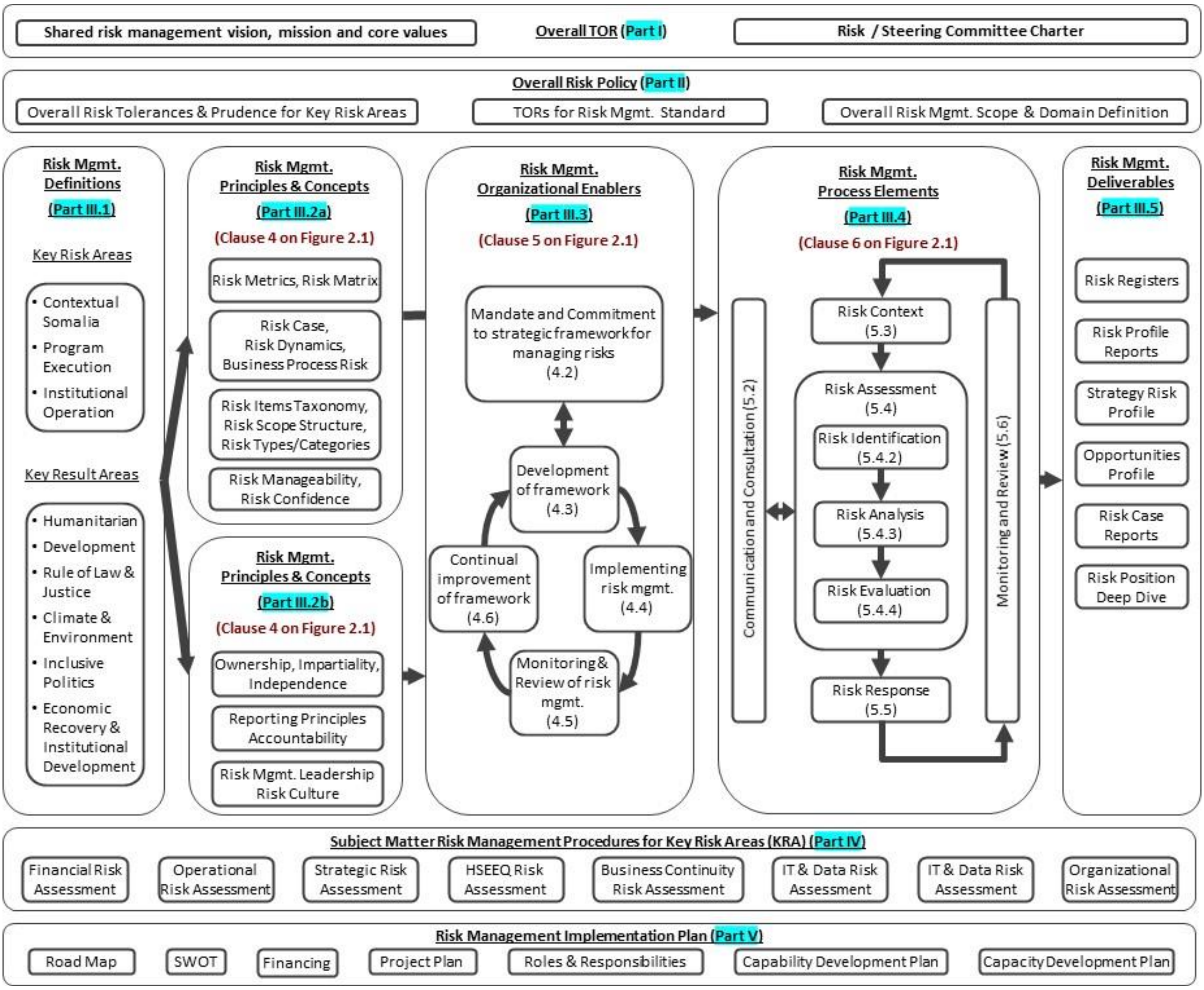

Figure 2.2 – 5 staged of risk management strategy Implementation as per IRM, UK

2.3.1 The CRM strategy implementation plan in brief overall generalised words

A general-purpose thought-model, developed by the Institute of Risk Management (UK), for the implementation of any risk management strategy based on the principles set out in both ISO 31000 and COSO is offered as per Figure 2.1. This document is structured accordingly - and the parts thereof: 0, I, II, III, IV - are briefed upon here below:

Part 0: Overall TOR

Part 0 is the implementation of the overall vision and mission - as described within the document, CRM Strategy (Part B). (Note here that, due to the premises for this CRM initiate, the "steering committee charter" is not applicable for this CRM strategy implementation plan (see subsection "Premises").

Part I: Overall Risk Policy

Part I is setting the overall premises. For this, no separate *risk policy* document has been developed for this CRM strategy implementation plan but would have to form part of the implementation works itself. For this, common scheme of risk metrics would have to be developed – including individua levels of risk tolerances, prudence's, impact categories for common key risk areas, key risk indicators, likelihood scale, risk matrix with standardised colour palette, colour code interpretation, and more.

Part II: Risk Management Framework

Part II is the technical RM process and comprise parts II.1-5. These parts form part of the implementation works and are sensitive to the individual CRM part-takers organizations. Therefore, they need to be a tailor-fit for each one the following are its sub-parts:

Part II.1: …defines the in-common risk management vocabulary (key terminologies and abbreviations.

Part II.2: …defines the in-common key risk management concepts and principles.

Part II.3: …defines the organisational empowerment enablers (roles, responsibilities, demarcations, accountabilities, risk ownerships, etc.)

Part II.4: …risk management process elements (risk identification, risk analysis, risk responses, etc.)

Part II.5: …defines the deliverables from the risk management strategy and framework.

Part III:

Part III comprises multiple sub-parts which typically matches with the number of Key Risk Areas (KRA) - i.e. such refers to subject matter specific risk analysis procedures – i.e. as such are highly different and specific in terms of applied methodologies (financial, safety, security, IT, operational, strategy, etc.). However, the development of such document items is beyond the scope of this study to provide. Anyway, for clarity, examples are:

Risk Assessment category for KRA	Typical applicable risk assessment standard to be fitted for individual KRA
Financial	SOX, ORSA, COSO
Health and Safety	ISO 45000
Environment	ISO 14000
IT Security	ISO 27001/5
Risk Based Quality Mgmt.	ISO 9001/5 / ISO 10005
Project and Program Execution	ISO 21500, Prince2, PMP
Strategy execution	ISO 26500
Risk Based Compliance	ISO 19600
Crisis	ISO 11200
Continuity and Resilience	ISO 22300
Risk in Supply Chain Mgmt.	ISO 28000

Part IV:

Part IV normally refers to detailed standardised organisational implementation guidelines and is beyond the scope of this study to provide. This section has been replaced by the “Discussion and Recommendation” section based on the capacity and capability assessments (Part A).

SECTION 3 THE CRM STRATEGY IMPLEMENTATION PLAN

The below content of this sub-section refers to Figure 2.1, Part III.3, portion "Implementing Risk Management (4.4)"

3.1 PART III.2: KEY PRINCIPLES AND CONCEPTS ("CLAUSE 4")

As illustrated by Figure 3.1, the CRM adopted thirteen principles for the CRM strategy implementation that are aimed at enhancing value creation and protection (Clause 4).

Eight of these are based on the ISO 31000 and another five are added to adapt it to the local needs, based COSO and IRM (the blue fonts).

This sub-section describes the elements of Figure 3.1.

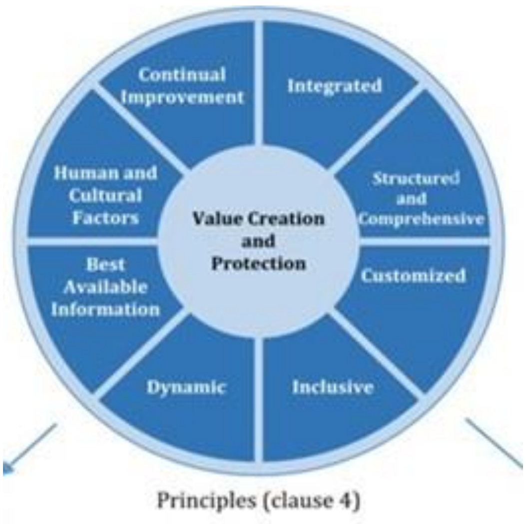

Figure 3.1 – RM Key Principles

1 *Aligned:* The RM process activities need to be aligned with the other activities in the organization.

2 *Available Information:* The RM process inputs to risk management are based on historical and current information, as well as on future expectations. Risk management explicitly considers any limitations and uncertainties associated with such information and expectations. Information should be timely, clear, and available to relevant stakeholders.

3 *Collaborative:* The RM process activities ensure that all risk stakeholder´s perspectives are included.

4 *Comprehensive:* The RM process is needs to be scaled up sufficiently to be effective and to covering the wider spectre risk exposures.

5 *Continual Improving:* The RM process is designed to in a cyclic sequenced and iterative manner remove efficiency obstacles and qualitative defects or degradations.

6 *Cultural adapted:* The RM process is designed to take into account human behaviours that significantly influences risk management activities and its outcome and quality.

7 *Customized:* The RM process is tailor fitted to the organization's external and internal context, as well as proportionally related to its business objectives.

8 *Dynamic:* The RM process recognises that risks can emerge, change, or disappear as the risk context changes. A dynamic RM process anticipates, detects, acknowledges, and responds to those changes and events as and when needed.

9 *Embedded:* The RM process activities need to be embedded within the individual participating organization´s own systems, for which the collective CRM approach is complementary and supportive.

10 *Inclusive:* The RM process ensures appropriate and timely involvement of other risk stakeholders, as well as gathers their knowledge, views, and perceptions to be considered also.

11 *Integrated:* The RM process supports several organizational functions by the same *risk management principles*, framework, and activities.

12 *Proportionate:* The RM process activities are proportionate to the level of risk faced by the organization.

13 *Structured:* The RM process is being consistent and produce comparable results to previous.

3.2 Part III.3: Organizational Empowerment Enablers ("Clause 5")

As illustrated by Figure 3.2, the CRM adopted five main elements for the CRM strategy implementation that are aimed at enhancing the leadership and commitment to the RM framework (Clause 5).

This sub-section describes the elements of Figure 3.2.

Figure 3.2 – RM Overall strategy and governing structure

3.2.1 Leadership and commitment

The participants of CRM Forum demonstrate leadership and commitment for the risk management practices within their own organisation to the best extent possible or needed by aligning with this commonly agreed CRM strategy. In doing so, ensure that:

- ✓ an adequate risk policy is defined and implemented – including accurate risk metrics and risk tolerances – including that of the other risk stakeholders.
- ✓ risk culture regime is adequately understood.
- ✓ key commitments are adequately followed up.
- ✓ the risk exposure is communicated to the organization and its stakeholders.
- ✓ the risk management framework remains appropriate for the risk context.

Integration of RM into organisation

Integrating risk management into the organizations relies on understanding the organizational structures and context, which typically differs depending on the organization's purpose, strategy, and complexity. In principle, all employees have a responsibility for managing risk at some level. Risk assessments must me evaluated against the organization´s objectives and goals at both strategic and operational levels.

Design

The design of the risk management framework must be based on the understanding of the external and internal risk context.

Considering the external factors as typically:

- ✓ social, cultural, political, legal, financial, technological, economic, environmental.
- ✓ trends affecting the organizational objectives.
- ✓ external stakeholders' relationships – including perceptions, values, needs and expectations.
- ✓ contractual commitments.
- ✓ networks and dependencies.

Considering the internal factors as typically:

- ✓ vision, mission, values, and beliefs.
- ✓ governance structure, roles, and accountabilities.
- ✓ strategy, objectives, and policies.
- ✓ organizational risk culture and RM maturity.
- ✓ contractual relationships and commitments.
- ✓ interdependencies and interconnections.

Evaluation of RM effectiveness

The effectiveness of the CRM should be periodically measured against its purpose. Key performance indicators should be developed for the implementation plans – including metrics for expected behaviour and desired risk culture.

Improvement

The CRM Forum should at regular review and re-adapt the CRM framework and strategy in order to address the changes in external and internal risk context. The CRM Forum should continually identify relevant areas of improvement – including sharing such within a lesson learned register.

3.2.2 Roles, Responsibilities and Accountabilities

The CRM Forum´s participating organisations´ own Risk Management Function

The CRM participating organisations are accountable for determining their own strategic direction of the organization, which includes obtaining and storing on-going knowledge of their own risk exposures, as well as that of their key stakeholders. They are accountable for creating the needed environment, governing structures and adequately empowered organization to meet the on-coming risk management challenges in an effective way. This includes that risks can be assessed and reported in an impartial way, to the top management. Therefore, independent forum needs to be established for this. Such may be through an executive group, a non-executive committee, an audit committee, or such other function that suits the organization's way of operating. The CRM participating organisations are responsible for – within their ow n organization: a) set risk policies and risk management objectives; b) conduct risk management meetings and on a fixed regularity basis; c) managing own risks on a day-to-day basis; d) building a risk aware culture within their operations; e) designing and reviewing processes for risk management; f) coordinate various risk management activities; g) developing risk responses - including business continuity programs; h) report on risk-positions to the risk stakeholders, i) auditing the risk management processes across an organization; j) support the risk management processes – including assist in facilitating risk identification/assessments and design of risk controls; and k) on an as-needed basis, positively assist the internal audit function in their independent risk based auditing activities.

The CRM Forum

The CRM Forum cannot hold much of fixed responsibilities and accountabilities itself as it operates without a formal charter and since its participants' level of commitment to the CRM Forum is non-binding. Hence, this document set out some expectations to the CRM Forum. The following are therefore proposed for it as a first phase scheme:

a Promote the participation into collaborative risk assessment sessions and risk management meetings. A fixed regular schedule for such is the best. Proposed is 2-monthly.

b Promote the sharing of risk related information among the CRM stakeholders.

c Promote risk policies and assist in the development risk management objectives for the Somalia aid stakeholders – including quantified ones.

d Promote and assist the development of risk culture development programs, aiming to reach alignment on practices.

e Promote the CRM Forum as a hub to channel risk management consulting services the Somalia aid community.

f Strive towards developing a service portfolio that could benefit the aid community (3dr party risk assessment, training, framework development, culture advisor, etc.).

g Reach consensus of what risk focuses areas to be focused on. Among the CRM Participants, promote the role of CRM Forum Risk Champions as focal point for specific Key Risk Areas (KRA) – i.e. for each member to actively contribute to the build of risk intelligences for the KRAs focused on.

Deliverables from the CRM Forum

The CRM Forum shall deliver exchange of relevant risk related information to the CRM participants by participating in regular CRM coordination meetings. Expectations to such deliverables will be defined by those meetings.

The CRM Forum Coordinator

The CRM Forum Coordinator is the only actively working person within and for the forum – this on a sponsored basis by its own organisation of employment. Hence, this role comes along with duties, as follows:

a Chair the regular CRM Forum meetings – including coordinating and preparing the agenda for it.

b Preparing the meeting agenda and the minutes of these meetings.

c Ensure the re-election of the CRM Forum Coordinator role on an annual basis.

d Ensure that the elected CRM Forum Coordinator has granted approval from the employee´s parent organisation for the spending of up to 20% of the person´s nominal working time, for the CRM Forum works.

e Drive the CRM Forum´s stated business objectives.

Deliverables from the CRM Forum Coordinator

The CRM Forum Coordinator shall deliver on meeting coordination and preparation, as well as meeting chairmanship – including writing minutes of meeting of these meetings.

3.3 Part BIII.4: Risk management Process Elements (“Clause 6”)

As illustrated by Figure 3.3, the CRM adopted five main elements for the CRM strategy implementation - aimed at enhancing the leadership and commitment to the RM framework (Clause 5).

This sub-section describes the elements of Figure 3.3.

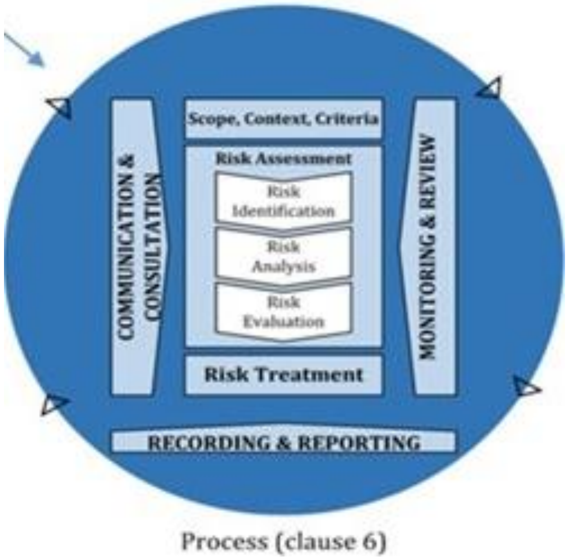

Figure 3.3 – RM Process Elements

3.3.1 Establishing the risk context, scope and overall criteria

Risk Context
Establishing the risk context is not only the first and a crucial step of the risk assessment process, but also a typically a neglected step. Establishing the risk context comprises correctly describing the risk stakeholders, risk environment, ownership, assumptions, domain, and the key attributes.

Risk Management Scope
Defining the risk scope is also an often-misunderstood step of the RM process. It entails defining the boundary around the analysis scope. It is important part of system-analysis and especially so when multiple risk objects are modeled into one risk case analysis.

Risk assessment criteria
Again, an often-underestimated step of the process. Important to understand is that the assumptions and premises of the risk assessment steps needs to be correctly understood. Also, the impact scale often needs to be adjusted to the risk ranking policy matrix.

Planning for consistent risk assessment
It is typically useful to make use of risk assessment template for recording of all the risk related information and be viewed in structured format, as illustrated by Table 3.3.

3.3.2 Risk Assessment

Risk Identification

The Risk Assessor is responsible for identifying the risk position by identifying the information as stipulated by Table 3.4, in which these data may vary greatly depending on the type of risk. Depending on the nature of the risk (context, type, information availability, etc.), the Risk Assessor shall chose the most appropriate assessment methodology (workshop, checklist, questionnaire, data estimation, inspection, audit, flowchart, dependability analysis, SWOT, PESTLE, Fault-tree, Cause & Effect, Bow-tie, HAZID/HAZOP, FMECA, Monte-Carlo simulation, Bayesian Network, etc.

Risk Analysis

Having identified suitable identification method and risk policy, the organization’s willingness to take risk can be better understood as well as the capacity to hold onto that risk-position. Thereafter, the risk owner determines the overall exposure to the risk item. The Risk Assessor needs obtain/gather an intimate knowledge of the subject matter of the risk-position (organizational environment, legal, social, political, operational, cultural, strategical, etc.) - including the critical factors to threats versus opportunities and related such to the achievement of these objectives. The risk identification process should be approached in a methodical and structured way to ensure that all significant activities within the organization have been considered in a consistent manner.

Risk Name	Short Name • Long Name • Risk Identification Code
Risk Owner	Name of person accountable for the risk item • Job Role
Risk Stakeholders	Name of other entities who/which are affected by the risk-position and their expectations.
Risk Environment	Name of main Key Risk Area
Risk Domain Area	Qualitative description of the dimension of the risk in case of being impacted.
Risk Dependability	Qualitative description of other dependability relations to other risks items or events.
Risk Scope	Qualitative description of the events, their size, type, number, and dependencies.
Risk Category	Qualitative description of category belongingness
Risk Type	Qualitative description of type belongingness
Risk Object	Qualitative of the object the risk-position pertains to.
Risk Subject	Qualitative of the subject the risk-position pertains to.
Risk Impact Category	Strategic • Operational • Financial • Knowledge • Compliance • Data • Health • Safety • Security • Environment • Quality • Credibility • Technology • Other
Risk-position	Qualitative and quantitative description of the risk-position – including functional failure modes, events, what-if scenarios, etc.
Risk Driver	Qualitative and quantitative description of the risk-position´s root-causes
Impact Level	Qualitative and quantitative description of the impact risk-position, if exhausted.
Likelihood	Qualitative and quantitative description of the likelihood for the risk-position to occur.
Risk Potential	Level of negative impact X Likelihood
Risk Controls	Qualitative and quantitative description of the in-place procedures, functions limiting the risk items level of impact or likelihood – including how much of the risk-position if already mitigated.
Residual Risk	Qualitative and quantitative description of the remaining risk-position given the in-place risk controls (= unmitigated risks)
Risk Immediacy	Qualitative and quantitative description of the time-domain for the risk-position (= Risk Protection as a function of time) – including change receptiveness, maturity to evolve as well as any volatility.
Risk Confidence	Qualitative and quantitative description of the underlying basis for the estimations of impact, likelihood, and immediacy – including how much knowledge is acquired for it and Levels of confidence in existing controls.
Risk Manageability	Qualitative and quantitative description of the underlying basis for the estimations of impact, likelihood, and immediacy – including: i) how much knowledge is acquired for it, ii) available resource to mitigate, iii) available authority to instill changes, iv) available knowledge, information and competency to act upon the risk, v) available budget, vi) available time-window of opportunity, etc. (= level of uncertainty).
Risk Exposure	The total net risk-position – including value at risk - given the risk potential, risk immediacy, risk confidence and risk manageability
Opportunity-position	Qualitative and quantitative description of the opposite risk-position (Level of positive impact X Likelihood)
Risk Capacity	Qualitative and/or quantitative description of the total possible absorbable risk.
Risk Taking Policy	Qualitative and/or quantitative description of the maximum willingness to take on a given risk-position (= Risk Appetite = Risk Prudence)
Risk Tolerance	For risk monitoring purposes, level of fractional change in risk position that the risk owner is willing to accept without intervening.
Risk Transfer Strategy	Sharing / Pooled Funds • Mitigation • Controls • Acceptance • Spreading • Modification • Insurance • Diversification • Manage out • other
Risk Life Cycle	New/Old: emerging • New evolving • New dissolving

Table 3.4 – Risk Assessment Recording Template

Risk Evaluation

Estimation of *value-at-risk* can be quantitative, semi-quantitative or qualitative. To maintain a consistent analysis process, a standardized assessment template needs to be applied, as shown by Table 3.3.

Risk Potential Ranking Matrix and Risk Policy

Therefore, it is important to apply one and the same / standard *risk potential* ranking matrix for all risk rankings performed. It is important that people can memorize the color palette so they can easily and correctly interpret the given risk policy at hand. That is, the interpretation of the color codes must me equally understood by all people. For example, in city traffic: red light means, “stop the car”. Such set rules must be interpreted the same for all people. The commonly used configuration is the 5-by-5 matrix, but it may very well be any other combination such as: 6-by-6, 5-by-6, 10-by-10, or 4-by-5, etc. The commonly used number of color codes are either 3 of 4. Further, it is important to apply one and the same likelihood scale along the risk ranking matrix for all assessment. What needs to be a variable is the impact scale. Obviously because the impacts differ for every risk assessment. Also, across different organizations, the level of tolerance to impacts differs greatly. So, the impact scale needs to be curve fitted to the given risk policy´s or risk matrix color palette. However, when applying percentage (%) scale for impacts – i.e. %-impact on the objectives being considered – then the impact scale can possibly be largely standardized as well. For this, firstly a generic version risk ranking policy needs to be the starting point, as proposed by Figure 3.4/5. Note here that a common mistake is to set the likelihood scale from 0 to 100%. This paper argues that already at a 25% probability level, the risk becomes “very high”. Hence, no higher value needed to be enough for “very high”. Importantly, and influencing the above two scales, is the interpretation of the chosen color scheme. This paper proposes a short, sharp, simple, and clear color coding, as below:

Red	**Intolerable** – immediate counter actions needed. Not allowed to keep staying on red.
Amber	**Tolerable for while** – if and only if, immediately counter actions needed. Immediate monitoring needed.
Yellow	**Tolerable** – to be monitored.
Green	**No actions needed.** Its inter-dependability **to** be re-considered on a regular basis.

Figure 3.4 – Generic Risk Ranking Scale / Risk Policy on Color Coding

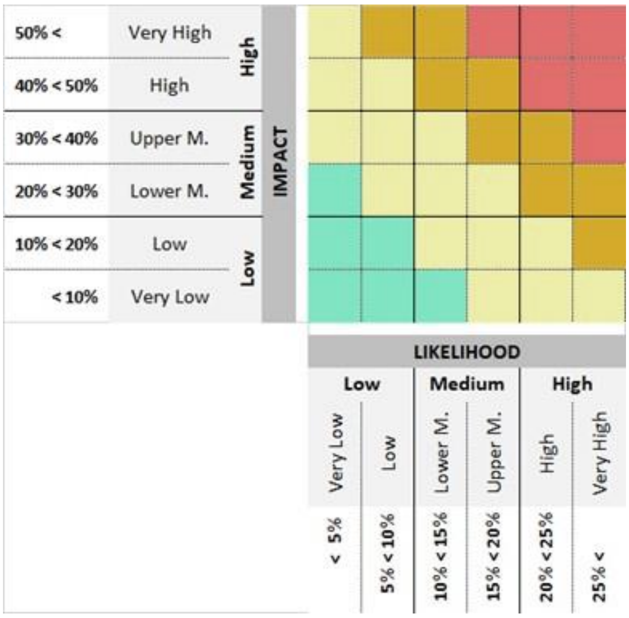

Figure 3.5 – Generic Risk Ranking Matrix / Risk Policy on Impact and Likelihood levels

Curve-fitting of generic risk matrix policy to own organization´s needs

The CRM Forum needs to operate on a common for all risk ranking matrix – i.e. to be considered the one proposed by Figure 3.4/5. However, each CRM participating organization need to curve-fit the risk potential matrix to own level of “pain points”. That is to state what level of impact (“hurt”) will correspond to / be classified as “red”, “amber”, “yellow”, “green”. It follows from this that the elements of risk relates to an individual´s ownership of it, which is also theoretically true. If further follows from that, the elements of risk need to be also considered from an impartial perspective to it. When the risk evaluation has been completed, the estimated risk-positions are compared with the risk criteria which the organization has established for the various impact categories (strategy, financial, operational, heath, safety, security, environment, quality, knowledge, credibility, legal compliance, etc., technology, market position, etc.).

Opportunities

Opportunities are to be ranked in the same manner as risks. The only difference is that the impact scale is of positive outcomes instead of negative ones. Important to understand is that, by default, for every risk item, there is in theory an opposite positive outcome possible, and very often that is also the case in practice. By considering both of these two opposing positions, the analysis results usually get better.

Impartiality in Risk Evaluation

From common humanistic knowledge: people have tendency to reason and draw conclusion in line what is best with own agenda. Therefore, due to the element of risk ownership, to ensure minimum level of objectivity and impartiality for the risk analysis process, it can often be advantageous to separate the impact assessment process with that one for the likelihood. The method and tool(s) need to evaluate these parameters objectively are typically quite different and may well be necessary to deploy different people for it.

Risk Immediacy

Risk Manageability

As *risk exposure* is a function of time and any risk evaluation is only valid for a certain period of time. Depending on the nature of the risk-position, some needs frequent re-consideration and some not so. However, without understanding of the time horizon for the risk exposure it is difficult to relate to it, and consequently manage it effectively. This paper proposes the schemes for risk Immediacy as described by Table 3.6.

Now	Immediate consideration needed
Fast approaching	Immediate consideration needed
Slow approaching	Can be put on hold
In the long future	Can be put on hold

Table 3.5 –Risk Immediacy Levels

Risk Exposure

As *net risk exposure*, as concept is illustrated by Figure 3.6, is also a function of the in-place *risk manageability* and *risk confidence*, it is key to understand this aspect. Many risk estimations are flawed due to not adequately taking such into account within the analysis steps.

Risk Exposure	**Risk Immediacy**	**Risk Potential**	**Impact of Event MULTIPLY Likelihood of Event**
	Urgency of Event		
Manageability of the Risk Exposure AND Confidence in Risk Analysis			

Table 3.6 – Concept of Risk Exposure versus Risk Potential

As shown by Figure 3.7, risk manageability is the amount of key factors within the risk owners control domain available to adequately manage the risk position within the given time window (budget, resources, information, knowledge, time-window of opportunity, authority, effectiveness of in-place risk controls, do-ability, etc.). This document proposes the following scheme for risk manageability:

	Level of accountability to continue risk ownership	Level of effort needed
High manageability	The designated risk owner is fully accountable to manage the risk positions within own domain. Do not need to be reported upwards.	Well within the risk owner´s disposal.
Medium-high manageability	The designated risk owner is fully accountable to manage the risk positions within own domain. Need some support to fully in control of it.	Medium-low effort needed to management risk-position.
Medium-low manageability	Risk ownership can possible be upheld, if and only if, risk manageability. If not, risk ownership most be moved to improve to other with higher risk manageability.	Medium-high effort needed to management risk-position.
Low manageability	Risk ownership needs to be moved to other or elevated to higher management.	High effort needed to management risk-position.

Table 3.7 –Risk Manageability Levels

Risk Confidence

As shown by Figure 3.8, risk confidence is another aspect of manageability but is considered separately as it relates to the amount of objective evidence the risk analysis and estimations is based upon (– i.e. qualitative guessing, quantitative guessing, quantitative fact-based calculation, available sample space, etc.). This document proposes the following scheme for risk manageability:

High confidence	High knowledge of the risk position
Medium-high confidence	High knowledge of the risk position
Medium-low confidence	Little certainty about the risk-position
Low confidence	Risk-position is fully uncertain

Table 3.8 –Risk Manageability Levels

Risk Manageability Matrix

Figure 3.9 illustrates the risk manageability matrix applied to the risk register discussed in the document part A, CRM Capacity and Capability Assessment, where *risk manageability* and *risk* *confidence* were imparted onto these 22 recorded risk items. This result indicates that only three risk items are within the *white swan* area (i.e. 8, 18, 22), the rest of them are outside of their normal envelope of effective manageability. That is, outside of their own control domain due to lack of information, lack of authority, lack of resources to mitigate, lack of window of opportunity, etc. The white swan area is those the organisation would be morally obliged to act upon as they have the necessary capacity and capability in place to counter-act the risk high position – i.e. into an as low as reasonably acceptable position. If knowingly not choosing to do so could produce a new high risk of legal impact. Contrary, if the risk items are within the *black swan* area, i.e. when the organisation, or dedicated risk owner, have limited or no data, intelligence, data, tools, etc. to establish sufficient *risk confidence* in the risk analysis, and, where the organisation insufficient capacity (resources, authority, time, opportunity, controls, etc) to establish effective *risk manageability* for it, then, they could be legally and morally somehow excused. However, it does not mean that risk position is not there. Indeed, it is, and these are more dangerous risk items since they are generally unknown or outside of the given domain to manage them. Risk manageability assessments needs to form part of the standard risk assessment step-process. As commonly known, the standard version is that risk is defined as the product of impact and likelihood, which is not untrue, but only true for that snapshot in time when the assessment was done. But relevant risks are typically highly time-invariant in nature. The more interdependent and complex they are, the more dynamics are introduced. Hence, risk-position may quickly change. Therefore, as risks are a function of time, its *risk immediacy* needs to be assessed.

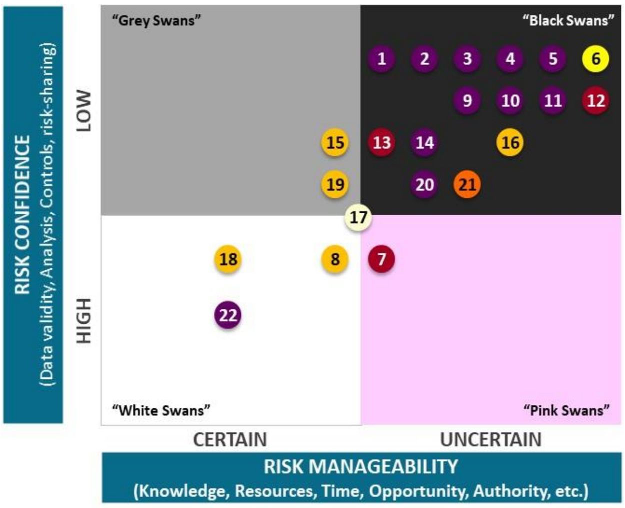

Figure 3.9 - Risk Manageability Matrix (1 of 2)

Figure 3.10 shows the risk exposure matrix – i.e. taking into account all the three aspects: risk potential, risk immediacy and risk manageability. Table 3.11 give a more precise view of the net risk-position exposure. The same 22 risk items as for Figure 3.10 have been used. The diameter of the bubbles represents the level of effort needed to management risk position – i.e. high effort needed indicates low level of manageability, and vice versa. The degree of opacity of the bubbles represent the risk immediacy.

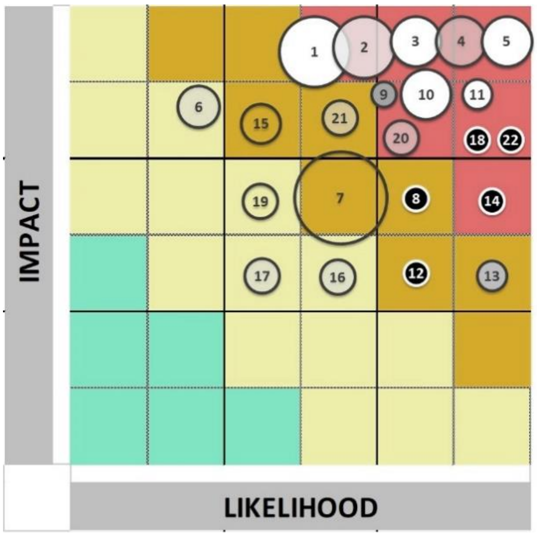

Figure 3.10 - Risk Exposure Matrix (2 of 2)

By Figure 3.12, this document proposes the following scheme for risk immediacy:

Fully solid black	In front of us right now
Semi-transparent grey	In the near future
Semi-transparent white	In the future
Fully transparent	Far into the distant future

Table 3.11 - Risk Immediacy Levels

Risk Ownership

The risk exposure´s risk manageability, as illustrated by Figure 3.10-11, shall be used as a tool to ensure that the ownership of the risk items is being adequately allocated – i.e. to most appropriate person or entity. In this way, the risk level can be further and better controlled.

3.3.3 Risk Treatment (Risk Responses and Recovery Options)

Risk Treatment Process

The process of risk treatment involves an iterative process of: i) selecting risk response options or risk controls; ii) implementing the controls; iii) assessing its effectiveness; iv) deciding whether residual risk is remains within the acceptable limits, and if not, perform a risk manageability study.

Risk response options

Risk response options are the following:

- removing the risk source: eliminate the element that gives rise to the risk.
- avoiding the risk: discontinue the activity.
- accepting the risk: continue without action or with added monitoring or risk controls.
- exploiting the risk: increasing the risk in order to pursue the opposite opportunity-position.
- altering the risk exposure: by modifying the likelihood.
- altering the risk exposure: by modifying the impact.
- sharing the risk: by buying insurance, by outsourcing, by diving among several stakeholders.
- containing the risk: by informed decision.
- delaying the risk: by delaying the risk immediacy.
- Managing out the risk: by altering the risk manageability.

If there are no good responsible options available, the risk should be recorded and kept under on-going review.

Implementing risk response plans

The process of risk response planning is to be prepared for the possible exhaustion of a risk scenario. It involves an iterative process of: i) establishing the various risk scenarios; ii) designing adequate risk barriers; iii) assessing its effectiveness; iv) implement scenario preparedness plan (i.e. e.g. business continuity plans; contingency plans, resilience plans; emergency response plans, crisis management plan, and similar).

For each risk response plan, the cost benefit of shall be positive. Knowing this, all risk response plans must be viewed in the context of the degree of risk immediacy and manageability.

Risk Recovery Options / Preparedness Planning

From general philosophy of common good, we all are accountable for what we know. Hence, considering Figure 3.9, when operating within the “white swan” area – i.e. the risk items are fully understood, as well as having the knowledge of how to management them – then the risk management function is responsible for advising on the given risk exposure profile so that the risk response and recovery options can be maximized. It follows from that, that is inadequate to develop contingency plans, business continuity plans, resilience plans, emergency preparedness plans, and crisis management plans – without having based such upon the given risk profile. That is, by first having gained prior knowledge of the risk potential scenarios.

3.3.4 Risk Communication and Consultations

The result of the risk analysis shall be used to produce, specific risk-position reports, general risk profile report for selected key risk areas. In this context, the key risk areas ought to map the key results areas for the business operation. It is critical that the CRM risk stakeholders correctly understands the various risk position´s severity, complexity and intendencies to other risk-positions. Therefore, the CRM Forum should drive risk awareness and obtaining feedback and information to support decision-making. Such should take place within and throughout all steps of the risk management process. The CRM Forum ought to coordinate different areas of expertise together for each step of the risk management process; ensure that different views are appropriately considered when defining risk criteria; provide sufficient information to facilitate risk based decision-making; aim at building a sense of ownership to the CRM process.

Risk Based Stakeholder Management

As illustrated by Figure 3.13, regularly review to what extent the various CRM stakeholders’ scope of risk management is appropriate and adequately defined. This included reviewing how the various CRM participants can contribute to higher understanding and risk intelligence of the various Key Risk Areas (KRA). The figure illustrates a risk life cycles – i.e. from it originates with an KRA and how it is being progresses if the risk is not managed. The figure also illustrates differing risk stakeholders through these life cycles. A mapping of risk stakeholders could be very useful in terms of risk-based stakeholder management – i.e. when it comes to collaborative approaches.

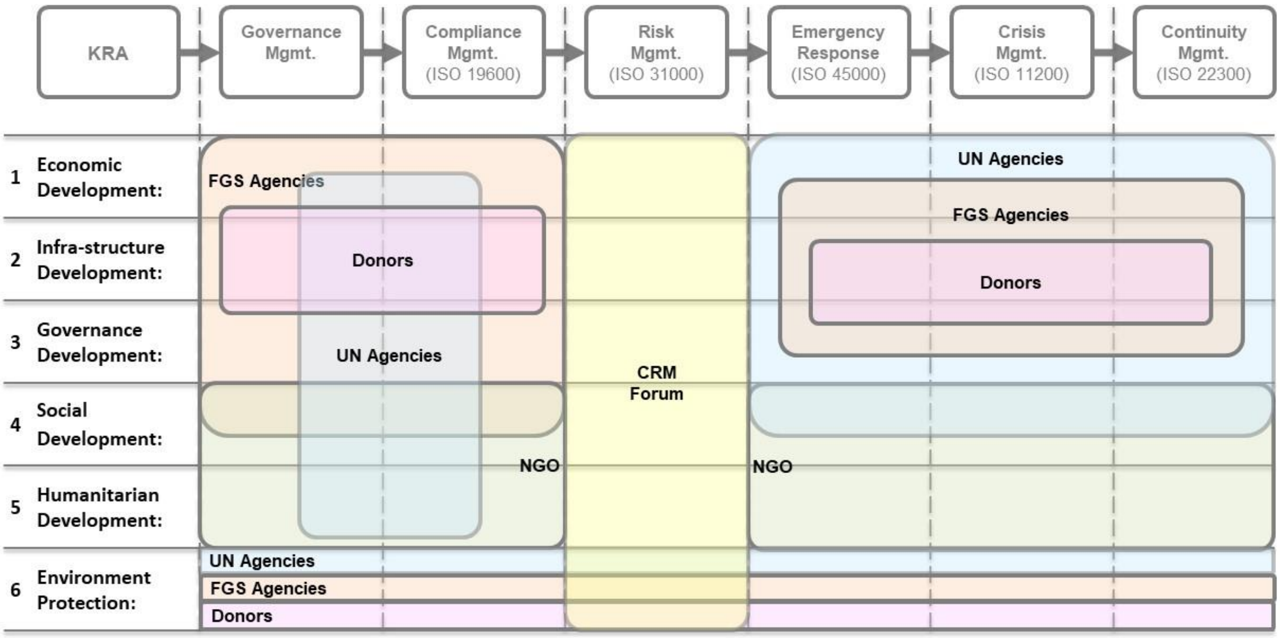

Figure 3.13 – CRM Scope Monitoring of Key risk Areas (KRA)

3.3.5 Risk Recording and Reporting

Risk Managers/Coordinators/Focal Points should:

- know the most significant risks facing the Somalia and aid operators
- know the possible effects on the aid organizations mission objectives
- ensure appropriate levels of awareness throughout the organization
- know how the organization will manage a crisis
- know how the prepares for the various risk recovery options
- know how the risk-position affects CRM stakeholder
- know how to communicate the risk-positions effectively
- be assured that the risk management process is working effectively and understand how such can enable continuous improvement
- publish a clear risk management policy covering risk management philosophy and responsibilities

CRM stakeholders should:

- know the risks that pertains to their area of responsibility, as well as the possible impacts these may have on other key risk areas and stakeholders
- monitor key risk indicators allowing to monitor risk tolerances relative to the mission objectives
- report specific risk cases and general risk profile on the most significant risks to senior management

Individuals should:

- understand their accountability to risk
- understand that risk management and risk awareness are a key part of their own organization’s culture
- report systematically and promptly to senior management any perceived new risks or failures of existing control measures

The risk management process and its outcomes should be documented and reported through appropriate mechanisms. Recording and reporting aims to: — communicate risk management activities and outcomes across the organization; — provide information for decision-making; — improve risk management activities; — assist interaction with stakeholders, including those with responsibility and accountability for risk management activities.

Decisions concerning the creation, retention and handling of documented information should take into account, but not be limited to: their use, information sensitivity and the external and internal context. Reporting is an integral part of the organization’s governance and should enhance the quality of dialogue with stakeholders and support top management and oversight bodies in meeting their responsibilities. Factors to consider for reporting include but are not limited to: — differing stakeholders and their specific information needs and requirements; — cost, frequency and timeliness of reporting; — method of reporting; — relevance of information to organizational objectives and decision-making.

3.3.6 Risk Monitoring and Review

<u>The CRM stakeholder's organization should</u>

- on a regular review its risk management policies and the effectiveness in achieving its objectives.
- Make arrangements for the formal reporting of risks senior management. The formal reporting should at least address: i) risk accountabilities; ii) i) in-place risk controls; iii) risks identifications and its processes; iv) risk mitigations; and v) risk monitoring and reviews.
- Advocate that good corporate governance requires that companies adopt a CRM approach to the common risk positions.
- Advocate that effective risk management requires that reporting and review structures in place and that appropriate controls are in place.
- Advocate that organizations´ risk-positions are dynamic and that changes within own or other stakeholders' organization, or environment, entails changes to the given risk case(s).
- Ensure that the monitoring and review process provides risk assurance – i.e. that there are appropriate controls in place.
- Ensure that the monitoring and reviews opinions to what extent: i) measures adopted resulted in what was intended, ii) procedures adopted were appropriate; and iii) what new knowledge would have helped to reach better decisions.

SECTION 4 PART D: DISCUSSIONS AND RECOMMENDATIONS

4.1 DISCUSSIONS [D]

Several discussion items are produced – serving as a basis introduction for the recommendations produced - for the CRM strategy implementation and are described under the separate document, CRM Capacity and Capability Assessment (Part A of A/B/C).

4.2 RECOMMENDATIONS [R]

4.2.1 *R1 – Severe, complex, and inter-dependent risk positions need high risk manageability*:

Premise: Somalia and Somalia aid actors are exposed to highly severe, complex, and multi-party inter-dependent risk positions

Most risks need to not be viewed as singular risk items but rather as a network/web of interacting risk factors forming degree of dynamics, variable.

Action 1: Apply the principle of risk case modelling of capturing the multiplicity and dynamics nature of risk positions.

Action 2: Apply the principle of risk manageability for severe, complex, and inter-dependent risk positions – as part of the standard assessments - in order to more effectively and accurately understand the risk exposures.

4.2.2 *R2 - Information sharing*:

Premise: Somalia and the Somalia aid actors are inhibited by lack of information sharing among the multitude of risk stakeholders. Lack of accessibility to key risk related data and information is prevailing and inhibits any effective update to the real risk dynamics which is highly multi-variate / interdependent on multiple factors that are changing

Lack of sharing information with others is very prevailing. The interviewees were either unable or unwilling to share their own formally recorded risk registers with the consultant, except one of them on the condition of not revealing its source/owner. Some were willing to share their general views of a generalised risk profile applicable for them. Also, only a few of the interviewed were able to share their own risk management procedure / standard / framework with the consultant – also due to being unable or unwilling. The main reasons for such were confirmed across the aid community´s interviews:

- **i** lack of mutual trust combined driven by fierce competition for funding and survival, among the aid organisations.
- **ii** lack of availability of useful data driven by lack of effective formal platforms to shore such information, or the lack of effective handing of relevant data sets.
- **iii** lack of the systematic collection and structured analysis of risk related data and information, producing data driven key risk indicators.

Action 3: Unite around a single common collaborative risk management forum that delivers overall coordination of the fostering activities of common risk management practices. Let this forum work interactively with multiple thematic risk forums, covering a defined set of Key Risk Areas, which again reflects the risk profiles of the overall key results areas. Let the thematic risk working groups establish risk case models for their own key risk areas. Also, let the CRM forum commonly agree on what information ought to be shared, and what not so. Then, collected such information systematically and allow the thematic risk working groups to formulate proper risk case studies. (More details on this will be in the Part C, CRM Implementation Plan).

Action 4: Establish risk culture transformation program across the Somalia aid community, aiming to foster higher risk culture – including the advancing of information sharing. (More details on this will be in the Part C, CRM Implementation Plan)

Key is to ensure efficient and effective use collaborative meeting forums and platforms were useful discussions can take place, reaching consensus among the CRM organisations.

Action 5: The most obvious starting point for this would be a hybrid of the two, UN´s RMU´s lead Multi-Party Risk Working Group and (UN MPRWG) and the Somalia NGO Consortium´s RWG.

Somalia risks are typically highly dynamic and multi-variable in nature. This is so as they are project / program executed. They are data driven. Clearly, the need for a common IT platform is obvious. Data and information need to be shared, quality assured, re-formatted, re-communicated, re-parameterised, etc. to re-generate added value / useful risk related information. Also, a common set of risk metrics needs to be adopted and adapted to own use– i.e. so that users can understand the risks in the same way. A common way of assessing and analysis risk needs to be put in place. In this context, risk tolerances and appetites need to be aligned for each CRM part-taker.

Action 6: Establish a collaborative risk repository.

Action 7: Establish a collaborative IT platform for information sharing.

Action 8: Establish a collaborative risk metrics.

4.2.3 *R3* - Risk culture and risk management maturity:

Premise: Somalia and the Somalia aid actors are inhibited by lack of information sharing among the multitude of risk stakeholders. Lack of accessibility to key risk related data and information is prevailing and inhibits any effective update to the real risk dynamics which is highly multi-variate / interdependent on multiple factors that are changing

This study, as well as the earlier works of reveals a risk culture that is fragmented and lack of effective networking in terms of information as well as practising the complementary risk management principles. Typically, risks are viewed as something that always needs to be mitigated, whist not much considerations given to the various options (opportunities) in exploiting the risk positions – i.e. to take risks by better understanding them, and then be rewarded for it. The level of risk maturity appears as filled with processes that are politicised, squeezed by budgets, lack of advanced tools and operates within a command-control-hierarchy to maintain status quo. Catalyst for change initiatives comes due to the outside ambience only. TI´s report [36] serve as an example: i) Barriers to collaboration and cooperation is embedded into these organization´s cultures. NGO Consortium's report [48] serves as another: The aid community has typically unpredictable or unstable funding, causing and inhibitor for long term stable strategic efforts, as well as even unstable HR policies for many.

Action 5: In-common risk-position needs to be commonly understood as well as consensus on how to manage such in a collaborative and effective way. It follows that "to collaborate" needs a have a shared expectation to it, as well as shared values attached to it.

Action 6: Alignment of risk management principles, practices, processes, methodologies, tools, policies, framework, etc. (More details on this will be in the Part C, CRM Implementation Plan).

Action 7: Ensure that the CRM approach is collaboratively clearly understood as the given the risk-positions´ level of complexity, and the barriers for success that needs to be broken down, CRM is the way forward. However, a sustained, persistent, and highly competent effort over long time would here be needed. A key question is how to do it right.

Action 8: As the CRM initiative is highly intensive in terms of varied experience, knowledge, competency, skills, management and leadership pertaining to all aspects of general risk management as well as strategy implementation. Hence, needed is a very clear guidance, close coordination, and cooperation of all stakeholders and users. Therefore, the CRM approach must be highly knowledge based, involving data research using effective tools, and guided by highly experienced and competent resources.

Action 9: Instil and integrated *risk culture* and *risk management maturity* enhancement program that ensures alignment to the CRM partakers long-term strategic objectives.

4.2.4 *R4* – Develop Risk Policy for the CRM participants:

Premise: Across the Somalia there are variable understanding and interpretation of the real risk exposures, as well as variable risk tolerance among the CR participants.

A starting point of the implementation of all risk management systems is to develop a risk policy. Such will describe how much risks are the risk managers willing to take / not to take.

Action 10: As a preceding step before the main bulk of the CRM implementation, establish a commonly agreed risk policy.

4.2.5 *R5* – Capacity and Capability Developments:

Premise: Across the Somalia there are variable use of RM tools and approaches.

Effectiveness in terms of risk management very much depends on what RM tools, procedures and skills sets are being deployed, as well as level of collaborative coordination.

Action 11: Develop a CRM risk register for risk items that are in common among the CRM participant. This is an important step, as the typically "the devil is in the details". It is important to get some common understanding of the technicalities.

Action 12: In doing so (Action 11), it automatically follows on the requirements for defining the principles for common risk acceptance criterions, risk tolerances, risk metrics and matrix. All these parameters can be standardised and the same for all participants except that the impact scale would be different for each participating organisation as well as different for each type of risk category (or KRA, KRI, and possibly also KRP).

Action 13: In doing so (Action 12), it automatically follows on the need for defining the principles for common criterions for *risk manageability*, *risk confidence* and *risk immediacy*.

Action 14: In doing so (Action 11, 12, 13), it automatically follows on the need for implementing a common web-based solution to facilitate the exchange of risk related information, contain the risk registers, etc. – including risk reporting and communications – i.e. a risk management and analysis tool environment. Such tool environment would be instrumental in terms of advancing common practices, methodologies and principles.

Action 14: The need for implementing a common mobile solution to better capture risk related information and data in the field for various territories – including auto-synchronising (if possible).

Action 15: Develop modular standards risk management training programs that are adapted for this Somalia CRM purposes.

Action 16: Develop modular risk culture awareness and enhancement programs.

Action 17: Develop risk-case study and analysis capabilities (e.g. Bayesian network modelling) in order to build more advanced risk case models that incorporate multiple factors and outcomes, as well as dynamically updating of the risk-model. Consider building overall risk models for major risk areas, or, aligned with the KPIs and/or common strategic objectives.

Action 18: Consider developing specific detailed risk analysis procedures for specific areas. Recommended is to start with one selected area as a pilot in terms of agreeing on a common methodology. Which risk are to start with needs to be discussed within the CRM Forum.