Risk Analysis Tool

HANDBOOK WITH FREQUENTLY ASKED QUESTIONS

Table of Contents

Introduction

This handbook provides you with detailed information and instructions on using the risk analysis tool. This tool was developed with considerable inputs drawing from and key interlocutors. The 39 evaluative elements represent those items most critical in the effective risk analysis and subsequently developing a functional risk strategy.

Your organisation's senior management may select risk areas for review that are critical in determining the organizational strategic priorities or programmatic priorities for a particular response. For instance, if there will be substantial procurement or outsourcing and contracting associated with a program, an extensive procurement policies and systems check is vital. Organization are encouraged to prioritize the risk areas of their requirements for more in-depth review, in order to risk management strategy to more closely align to their needs.

This tool aims to facilitate a systematic and functional risk management and inform determination of an effective and robust risk mitigation strategy. It can be used to identify, assess and analyze any ad hoc risk situation in a limited and constraint environment.

Tools to support functional and effective Risk Management

The following three tools are designed to support a functional and effective risk management as well as to promote a collective and standardized risk management approach to the cross-border response. The organization may amend them as appropriate for their local context.

1. **Risk Analysis Tool**: Used for systematic identification, assessment, analysis and management of a risk or risk situation and to develop a robust and functional risk mitigation strategy accordingly and periodically repeated to review and show progress and subsequent priorities.
2. **Risk Management Guidelines**: Guide to determine and initiate a standard risk management function in an organization, as well as whether any special conditions may be required.
3. **Risk Management Minimum Standards**: A set of minimum standards for risk management recommended for a facilitated, collective and standardized approach to risk management of cross-border response, adapted to the operating context and take account of the capacities, operational areas and risk-appetite of the various organizations.

As noted above, these tools are complementary and designed to facilitate the different purposes, stages and time periods, and functions of risk management.

Purpose of Risk Analysis Tool

The risk analysis tool is a hybrid combining the three fundamental functions of risk management; analysis, mitigation and management. Starting from risk identification and ending at the performance review and periodic checks of risk mitigation and management process, the tool provides a step by step facilitated assessment and recording of information that leads to analyzing the risk, determining inherent risk rating, plotting the risk on heat map, developing a mitigation strategy and monitoring and reviewing its performance.

As noted above, the purpose of the tool is to facilitate a systematic identification, assessment, analysis and management of a risk or risk situation and support to develop a robust and functional risk mitigation strategy accordingly and periodically repeated to review and show progress and subsequent priorities.

The tool helps to determine whether the organization's systems, processes and controls put in place are adequate to manage, control, account for, and report on the risk or risk situation and its potential impacts, thus protecting both or the organizational and stakeholders' interests equally.

It provides the management with the information needed to evaluate the ability of the organization to adequately fulfill the terms of proposed risk mitigation strategy and serves as a tool in the selection of controls needed to deter the strategy gaps to impact negatively. The tool is not to be used in making a responsibility determination of risk appetite.

Getting Started

Getting to Know the Tool

The figure 1 below explains the overall setup of the tool as well as information flow.

Figure 1 – Risk Analysis Tool

About the Interface

Button/Data Field	Function
Macros	The tool is a macro-enabled file, therefore, prior to enter any data the macro should be enabled. By default, the tool is opened in a macro disabled mode. ➢ The yellow earning bar shows that macros have been disabled.
Enable Content	This button enables the Macros. Please see 'Running Macros' for detailed instructions. ▪ Press to enable the Macros.

Button/Data Field	Function
Record Index	The tool assigns a number to each risk entered. This number is called 'Index'.
Creation Date/Time	The tool saves the date and time when the data is entered, and/or new entry is generated.
Previous	This tool maintains the database of risks which can be viewed at any stage. The 'Previous' and 'Next' buttons are to scroll between entered data/entries. Press to view the 'previous' entry(s).
Next	Press to view the 'next' entry(s).
New Entry	The tool treats each risk as an individual data entry. This button enables the tool to accept a new entry. ▪ Press to enter a new risk. ▪ Press to generate a new entry.
Edit	The tool, when started, opens the interface in 'Read Only' mode. The 'Edit' button open an existing record/entry for editing.
Inherent Risk Rating	The tool automatically calculates the inherent risk rating of the entered risk (rate range from 1~25). The inherent risk rating is based on the assigned likelihood and impact of the risk. The number in this field represent this rating, the tool also plots a '**BLUE**' dot on the 'Heat Map' at the right bottom corner of the tool.
Residual Risk Rating	If the risk is having a residual risk, the tool automatically calculates the residual risk rating too (rate range from 1~25). Similarly, the residual risk rating is also based on the assigned likelihood and impact of the residual risk. The number in this field represent this rating, the tool also plots a '**RED**' dot on the 'Heat Map' at the right bottom corner of the tool.
Heat Map	The heat map is data visualization, on a 5x5 two-dimensional matrix, of entered risk. It plots the both ratings of the risk i.e. inherent and residual. The heat map also known as a risk heat map, is a data visualization tool for communicating specific risks an organization faces. Heat map is a way of representing the resulting qualitative and quantitative evaluations of the probability of risk occurrence and the impact on the organization when a particular risk is experienced. It helps organization to identify and prioritize the risks associated with its area of work, by presenting the results of a risk assessment process visually and in a meaningful and concise way.
Section A	This section contains the following general profile information; ➢ A1. Data Entry ID – open text field ➢ A2. Organization Type – dropdown list Please see 'General Profile' for detailed instructions.
Section B	The section deals with the risk profiling and risk identification and contains the following data fields: ▪ *Risk Profile*; ➢ B1. Risk ID – open text field ➢ B2. Risk Type – dropdown list ▪ *Risk Identification*; ➢ B3. Risk Category – dropdown list ➢ B4. Risk Sub-Category – dropdown list ➢ B5. Risk Sub-Category Type – dropdown list Please see 'Risk Profiling and Risk Identification' for detailed instructions.

Button/Data Field	Function
Section C	This section focuses on the risk's effects, if any, on clusters and cluster activities and contains the following data fields; ➤ C1. Cluster Affected – dropdown list ➤ C2. Cluster Activity – dropdown list Please see 'Affected Cluster' for detailed instructions.
Section D	This section deals in detail with the risk assessment and analysis, and contains the following data fields; ➤ D1. Risk Description – open text field ➤ D2. Impact – dropdown list ➤ D3. Likelihood – dropdown list ➤ D4. Risk Driver – dropdown list ➤ D5. Inherent Risk Rating – automatically populated locked field Please see 'Risk Assessment and Analysis' for detailed instructions.
Section E	This section focuses on risk mitigation, risk management, as well as performance review of the risk mitigation and management process. The hyperlink given in this section takes the user to 'Risk Mitigation Strategy' tool which facilitate, and support user through step by step guidance, to develop the risk mitigation strategy. At the end of the tool, another hyper link is given, which brings the user back to Risk Analysis Tool, i.e. the main interface. *The tool will not process further until this section is completed. The user needs to fill this section completely to proceed further with the risk analysis tool.* Then risk mitigation strategy contains the following data fields; ➤ E1. Risk Context Established – open text field ➤ E2. Risk Analyzed – open text field ➤ E3. Risk Evaluation – open text field ➤ E4. Risk Mitigation Approach – Button (locked field for data entry) ➤ E5. Risk Mitigation Measures – open text field ➤ E5.1 Resources Needed – open text field ➤ E5.2 Gaps – open text field ➤ E5.3 Controls – open text field ➤ E5.4 Strategy Owner – open text field ➤ E6. Monitoring and Review – open text field ➤ E7. Communication and Coordination – open text field ➤ E8. Next Review Date – Date in DD/MM/YY format (locked field for data entry) Please see 'Risk Mitigation and Management' for detailed instructions.
Section F	This section reviews and monitor the risk mitigation and management performance, and contains the following data fields; ➤ F1. Mitigation Outcomes – open text field ➤ F2. Follow-up Notes – open text field ➤ F3. Next Review Date – automatically populated field locked for entry Please see 'Performance Monitoring' for detailed instructions.
Section G	This section is dedicated to residual risk, and contains the following data fields; ➤ G1. Residual Risk – dropdown list ➤ G2. Impact – dropdown list ➤ G3. Likelihood – dropdown list ➤ G4. Residual Risk Rating – automatically populated locked field

Button/Data Field	Function
	Please see 'Residual Risk' for detailed instructions.
Export the Report as PDF	Once complete data is entered, the tool can generate the risk report. • Press the button to generate report. Please see 'Generating Reports' for detailed instructions.

Essential Information

The following are brief explanations of each essential component of the tool.

Software

The tool is designed and programmed as Macro-Enabled workbook in Excel for Office 365 version and is compatible with; Excel for the web, Excel 2019, 2016, 2013, 2010 and 2007 versions. The risk analysis tool is backward-compatible to Office 2007 version.

Layout and Formatting

As, noted above, the tool is a macro-enabled file and is password protected. This means that only certain fields are open to enter the data, either via dropdown lists or through open text, with the pre-defined parameters. These parameters show up with the dropdown lists, and the details are explained under each field in the data entry protocols section below.

The tool is divided into the following three sections:

1. Risk Analysis Tool

The risk analysis tool is the main interface of the tool where most data is entered. This section is formatted with the dropdown lists to facilitate the data entry, and each dropdown list have the 'other' option. When 'other' option is selected a new data entry field appears parallelly.

All the data fields are linked and automatically synchronized among the three sections of the entire tool, hence any data entered in the risk analysis tool automatically populate the respective field in the risk register as well.

This interlinkage and synchronization are based on the logical sequencing and thus follows a strict cascading and constraint by default. Any in correct data entry is marked red with an error message. Due to this logical sequencing the sub-sections within a section follows a predefined logical script defining the cascading and constraint and the dropdown list displays only valid options for this section with option of 'other'.

The risk analysis tool is further sub-divided into the following sections:

- **Section A**: contains the general profile information.
- **Section B**: deals with the risk profiling and risk identification.
- **Section C**: focuses on the risk's effects, if any, on 'Clusters' and cluster activities.
- **Section D**: deals in detail with the risk assessment and analysis.
- **Section E**: focuses on risk mitigation and management.
- **Section F**: reviews and monitor the risk mitigation and management performance.
- **Section G**: is dedicated to residual risk.
- **Risk Heat Map**: provides the visual representation of risk's inherent and residual rating.

2. Risk Register

The risk register records the detailed information of the risk in a matrix form and reads the data from both the risk management and risk mitigation tool. It serves as the main database of risks. Each risk entered/reported is saved in a separate row.

3. Risk Mitigation Strategy

The risk mitigation strategy is a tool focused on to develop a robust and effective risk mitigation strategy for the reported risk and therefore provides a step-by-step guidance to facilitate the process. This tool also contains sections for risk management as well as to review and monitor the mitigation performance.

Running Macros

As already mentioned, the tool is a macro-enabled file, therefore, prior to enter any data the macro should be enabled. However, the existing data in all the three sheets of tool can be reviewed without using/enabling macros.

A macro is a series of commands that allows user to automate a repeated task and can be run to perform the task.

To Enable macros when the Message Bar appears, use the following instructions;

- ➢ When the tool is opened, the yellow message bar appears with a shield icon and the **Enable Content** button.
- ➢ On the **Message Bar**, click **Enable Content**.
- ➢ Please refer to the figure 2 below;

Figure 2 – Running Macros
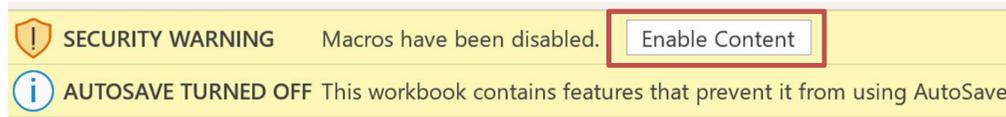
Enabling Auto Save

AutoSave is a feature of Microsoft Office 365 that saves the file automatically, every few seconds, as you work. AutoSave is enabled by default in Office 365 when a file is stored on OneDrive, OneDrive for Business, or SharePoint Online.

To enable the auto save in other version, use the following instructions;

- ➢ Go to **File** > **Options** > **Advanced**.
- ➢ Scroll down to the **Save** section on the right-side pane.
- ➢ Make sure the '**Allow background saves**' box is selected.
- ➢ Click '**OK**' to save changes.

Starting Up

It is recommended that when information is being entered into the risk analysis tool, that the information is factual, timely, and as complete as possible to inform the risk rating outcome. Any

information that is not available during data entry, should be noted in the risk description area. This will allow you to refer to this in the later risk mitigation and the risk management approach.

Before you begin to enter the data to the risk analysis tool, it is important to review all the necessary documentation, data and information you have in advance. This will allow you to identify gaps or lack of information before you begin analyzing any risk. A best practice approach recommended, is to make note of any of these missing pieces of information which will allow you to record them in the risk description to properly explain what has not been uncovered in your risk analysis.

With the tool opened and enabled the macros (please refer to section 'running macros'), the first step is to click on new entry button. Please see below the figure 3;

Figure 3 – New Entry
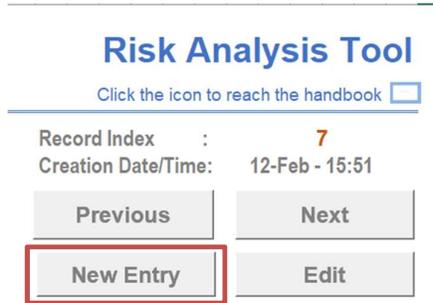
Once new entry is selected the tool automatically assigns a record **index** and saves the time and date of the data entry as well.

➢ The same record **index** is used as the file name, when after complete data entry the report is generated. For details, please see the section 'Generating Report'.
➢ The tool reads the date and time from the system's main clock.
➢ The figure 4 below illustrates the new entry details;

Figure 4 – Record Index
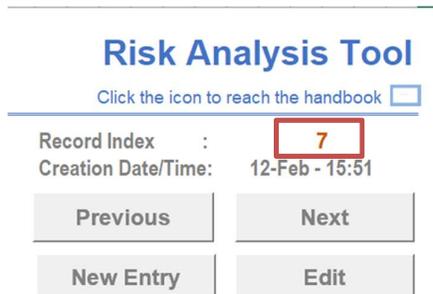
➢ Each dropdown list provides the option of '**Other**', when other is selected, an additional field appears next to it. Please see the figure 5 below.

Figure 5 – Other
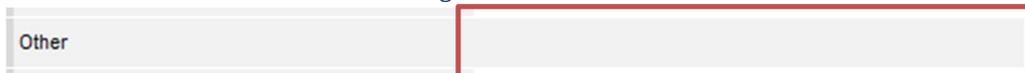
Data Entry and Data Protocols

The following section explains the details on how to enter the data in each field, along with the protocols and constraints. There are basically two type of data fields in the tool; the dropdown list and the open text field. The dropdown lists are cascaded and conditioned with the response/choice to their predecessor, the details are explained under their respective sections. The open text fields have character limit which is displayed when the data entered in the field.

➢ There is also a brief explanation included for each field. This brief description can be retrieved by clicking on the title of the field. The figure 6 below, a screenshot of B2, illustrates the brief description which appears once B2 is clicked;

Figure 6 – Brief Description

➢ Each data entry field also provides a brief '**Instructions**' on the data entry and an error message '**Incorrect Entry!**' incase the data protocol is violated. The figure 7 and figure 8, below illustrate the instructions and error message;

Figure 7 – Instructions

Figure 8 – Error Message
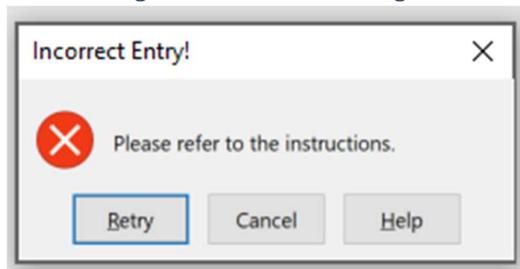
➢ Any incorrect entry is marked in **RED** and the background of text field also changes to light RED. Please see below figure 9 – Incorrect Entry.

Figure 9 – Incorrect Entry
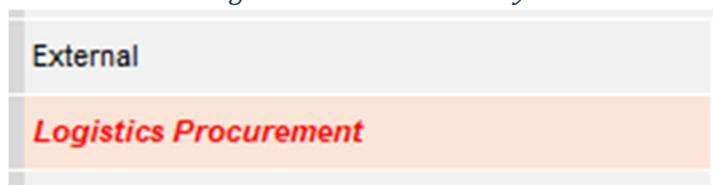
> Please note, because of the logical constraints and cascading, each data field with dropdown list need to have a value selected from dropdown, otherwise, the proceeding data fields will remain empty/blank. This will result in malfunction of the tool.

General Profile Information

Section 'A', deals with the general profile information, and contains the following fields:

A1. Data Entry ID

This field is designated to identify the data enterer. The purpose of this field is to record the identity of the data enterer for the future references made for this particular risk, as well as for the internal communication among different departments of the organization.

The suggested format for this ID is alphanumeric and the following protocol is recommended for this field;

> **PIN/Dept-Office/Year**
- PIN (Personal Identification Number); A three-digit number assigned by the organization to its staff member.
- Dept; Department Abbreviation
- Office; Office Code e.g. CO for Country Office, and FO for Field Office
- Year; last two digits of the year i.e. 19 for 2019, 20 for 2020

The following examples are for the illustration purposes only;

- 123/FN-CO/19 (a finance staff with staff ID#123 from country office entered the data during 2019)
- 046/PG-FO/20 (a program staff with staff ID#046 from field office entered the data during 2020)
- 012/SM-CO/18 (a senior management team member with staff ID#046 from country office entered the data during 2018)

A2. Organization Type

This field identifies the organization type. It is basically introduced for a broader level analysis at hub and/or country response level, where the risks and their emerging trends needs to be classified in various categories and among them one classification is based on the organization type.

> A2 field is a dropdown list, with single selection option.
> The table A2 below show the organization types;

Table A2 – Organization Type

A2. Organization Type:
Coordination Body (Network, Forum, Platform, Cluster)

Donor
International Non-Government Organization
National or local Non-Government Organization
Red Cross/Red Crescent Movement
UN System Agency
Other

Risk Profiling and Risk Identification

Section 'B' deals with risk profiling and identification and contains the following fields:

B1. Risk ID

This field is designed to assign a unique identity to the risk entered. The objective is to identify and record each entered risk separately. The risk ID also serve as a reference number for any future references made for this particular risk, as well as for the internal communication among different departments of the organization and external communication with wider audience.

The suggested format for this ID is alphanumeric and the following protocol is recommended for this field;

- ➢ **PIN/RT/Year**
- ▪ PIN (Personal Identification Number); A three-digit number assigned by the organization to its staff member.
- ▪ RT; Risk Type
- ▪ Year; last two digits of the year i.e. 19 for 2019, 20 for 2020

The following examples are for the illustration purposes only;

- 013/EX/19 (an external risk with risk log entry reference #013 entered during 2019)
- 002/IN/20 (an internal risk with risk log entry reference #002 entered during 2020)
- 089/SG/20 (a strategic risk with risk log entry reference #089 entered during 2020)

B2. Risk Type

The first step in creating an effective risk-management system is to understand the qualitative distinctions among the types of risks that organizations face.

The following is one possible classification system:

Internal Risk; risks linked to the internal environment and/or arising from within the organization e.g. operational risks in running a project or activity, or organization's internal context which includes governance, culture, standards and rules, capabilities, existing contracts, staff expectations, information systems, etc.

These risks are controllable and will largely be within the sphere of influence of the organization and need to be proactively managed.

External Risk; risks arise from events outside the organization and are beyond its influence or control. Sources of these risks include natural, political and man-made disasters, major macroeconomic shifts in market conditions, regulatory environment and stakeholders' expectations.

These risks are largely outside the sphere of influence of the organization and may require robust contingency planning. Because organizations cannot prevent such events from occurring, their management must focus on identification (they tend to be obvious in hindsight) and mitigation of their impact.

Strategic Risk; risks linked to the interface between one or more risk types (internal and external risks), departments and/or organizations. Strategic risks are quite different from preventable risks because they are not inherently undesirable extract. An organization voluntarily accepts some risk in order to generate superior returns from its strategy.

Managing the risks related to strategic choices require close cooperation with stakeholders, partner organizations and authorities, and organization need to anchor these discussions in their strategy formulation and implementation processes. Organizations can identify and prepare for nonpreventable risks that arise externally to their strategy and operations, thus, strategy risks cannot be managed through a rules-based control model. Instead, a risk-management system designed to reduce the probability that the assumed risks actually materialize and to improve the organization's ability to manage or contain the risk events should they occur. Such a system would not stop organizations from undertaking risky ventures; to the contrary, it would enable organizations to take on higher-risk, higher-reward projects than could competitors with less effective risk management.

➢ These three major types of risk i.e. internal, external and strategic are listed in the drop-down list.
➢ B2 is a dropdown list, with single selection option.
➢ If the risk to be reported can't be comfortably classified in these types, then please select 'Other' and give descriptive details in the next box.

B3. Risk Category

Several types and sources of risks – either internal or external to the activity, or strategy related – may affect a project. Some risks may be unpredictable and linked to large-scale structural causes beyond a specific activity (for instance, financial risks). Others may have existed for a long time or may be foreseen to occur in the future. Thus, to achieve a structured and manageable overview of all risks facing an organization, it helps to classify them in categories and subcategories.

Additionally, categorization of risk allows management to decide which risks can be managed through which risk management model and which require alternative approaches. The risks faced by an organization should be categorized according to the organization's needs.

➢ The three major types of risk i.e. internal, external and strategic, are further categorized into their specific categories adapted to suit the contextual needs of the cross-border response. The table B3 – Risk Category, lists all the categories under each listed risk.
➢ B3 data field is a drop-down list, with single selection option.
➢ The B3 dropdown list is conditioned with the response to **B2**, therefore, the data is cascaded respectively.
➢ If the risk to be reported can't be comfortably categorized in these types, then please select 'Other' and give descriptive details in the next box.

Table B3 – Risk Category

External:
Access
Aid Diversion
Quality, Accountability and AAP (Accountability to Affected Population)
Safety & Security
Environment
Other

Internal:
Administrative
Financial
Human Resources
Logistics Procurement
Operational
Programmatic
Other

Strategic:
Change in Government Policy(s)
Demographic Change(s)
Duty of Care
Fluctuation of Exchange Rates
GBV
Human Rights Violations
Laws/Regulations Imposed Requirements
Major Macroeconomic Shifts
Major Shift in Power
Manmade Disasters/Crisis
Natural Disasters
Obsolescence of Current Systems
Political Disaster/Crisis
Political Instability
PSEA
Sudden Onset of Large-Scale Emergency
Under Engagement with Government due to Lack of Understanding of the Cross-border Operation
Other

B4. Risk Sub-Category

The sub-categorization of risks is 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. Therefore, sub-categorization of risks must reflect the nature of activities organization carries.

The use of risk sub-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.

➢ Each risk category is further sub-categorized into its specific sub-categories adapted to suit the contextual needs of the cross-border response.

➢ B4 data field is a drop-down list, with single selection option.
➢ B4 dropdown list is conditioned with the response to **B3**, therefore, the data is cascaded respectively.
➢ **Annex 1** – Table B4 – Risk Sub-Category, lists all the categories under each risk category.
➢ If the risk to be reported can't be comfortably sub-categorized in these types, then please select 'Other' and give descriptive details in the next box.

B5. Sub-Category Type

This is an additional layer in _external risk classification_, specifically introduced to accommodate the contextual versatility and volatility of Syria crisis, and aims to further facilitate the management, for an effective and efficient risk management.

➢ B5 data field is a drop-down list, with single selection option.
➢ B5 dropdown list is conditioned with the response to **B4**, therefore, the data is cascaded respectively.
➢ **Annex 2** – Table B5 – Sub-Category Type, lists all the categories under each risk category.
➢ If the risk to be reported can't be comfortably sub-categorized in these types, then please select 'Other' and give descriptive details in the next box.

Section C focuses on the risk's effects, if any, on 'Clusters' and cluster activities.

C1. Cluster (affected)

Some types and sources of risks – either internal or external to the activity – faced by an organization may influence a specific cluster or clusters and some particular activity(s), therefore, it is crucial to factor these in while analyzing a risk.

➢ C1 data field is a drop-down list with single selection option.
➢ Table C1 – Cluster (affected), lists all the active clusters of cross-border response.
➢ If the risk to be reported may influence more than one clusters, then please select 'Multi-Cluster' and give descriptive details in the next box.

Table C1 – Cluster (affected)

C1. Cluster (affected):
Camp Coordination Management - CCCM
Coordination Common Services – CCS
Early Recovery
Education
Emergency Shelter NFI
Food Security Livelihoods FSL
Health
Logistics
Nutrition
Protection
Protection - Housing Land Property
Protection - Child Protection
Protection - Gender Based Violence
Protection - Mine Action
Refugee Multi Sector – RMS

Return Reintegration Recovery – RRR
Water Sanitation & Hygiene – WASH
Multi-Cluster - *please specify*

C2. Cluster Activity

This field provides the option to select the cluster activities to be/might be affected by the risk reported. Therefore, it is equally important to deliberate this during analyzing the risk.

- ➢ C2 data field is a drop-down list, with single selection option.
- ➢ C2 dropdown list is conditioned with the response to **C1**, therefore, the data is cascaded respectively.
- ➢ **Annex 3** – Table C2 – Cluster Activity, lists all major activities according to the logical framework of each cluster.
- ➢ As this list of dropdown depends on each cluster's logical framework, therefore, _it is highly recommended_ that this list needs to be kept updated and aligned with the clusters' logical framework, and whenever, any new activity is introduced in the cluster logical framework, this should be updated in this list as well.

Risk Assessment and Analysis

This section deals in detail with the risk assessment and analysis. Whether conducted as part of a broad-based enterprise risk management process or more narrowly focused internal control process, risk assessment is a critical step in risk management.

D1. Risk Description

This field is to describe the important details of the risk to be reported. Therefore, please describe the risk in detail in order to facilitate the risk-management system designed to reduce the probability that the assumed risk actually materialize and to improve the organization's ability to manage or contain the risk events should they occur.

- ➢ D1 data field is an open text field with character limitation.
- ➢ Once the data is entered the character limit is displayed.

D2. Impact

In risk management terms, the effect of a risk relative to the achievement of the objective.

- ➢ A five-stage impact scale is used in accordance with ISO31000, 31004, 31010 – Risk Management Standards.
- ➢ The following are five stages of impact scale;
  1. Very Low
  2. Low
  3. Medium
  4. High
  5. Very High
- ➢ D2 is a dropdown list, with single selection option.

D3. Likelihood

In risk management terms, the possibility and/or probability that a risk will occur.

➢ A five-stage probability scale is used in accordance with ISO31000, 31004, 31010 – Risk Management Standards.
➢ The following are five stages of probability scale;
   6. Very Unlikely
   7. Unlikely
   8. Moderately Likely
   9. Likely
   10. Very Likely
➢ D3 is a dropdown list, with single selection option.

D4. Inherent Risk Rating

Inherent risk is the risk without considering the application of any mitigating measures or any controls. The comparison between inherent and residual risk helps to identify the effectiveness of risk control.

➢ Inherent Risk rating is the product of risk impact and likelihood and is expressed as a whole number ranging between 1~25.
➢ D4 is a locked field with automatic calculation enabled.
➢ Once the inherent risk rating is calculated the tool plots it as a '**Blue**' dot on the heat map at the right bottom corner of the tool.

D5. Risk Driver

The existing factors in the environment where organization is working, that leads the risk analysis to believe that a particular risk would occur, or the factors/forces/authorities influence the context in favor of a risk to occur.

➢ D5 data field is a drop-down list, with single selection option.
➢ The dropdown list of D5 is based on the current available data according to the Access Monitoring and Reporting Framework, which may need to be updated parodically.
➢ The Table D5 – Risk Driver, below lists most of the major risk drivers currently have an influence in the cross-border response.

Table D5 – Risk Driver

D5. Risk Driver:
Border Management at Bab Al Hawa - Syrian Side
Border Management at Bab Alsalam - Syrian Side
Clusters
Contractors/Vendors
Donors
Government of Syria
Hayat Tahrir Al Sham
ICCG
IDPs Affairs Committee
Implementing Partner(s)
Local Camp Management
Local Council
National Army – FSA
National Liberation Front

NGOs Affairs Office
Syrian Interim Government
Syrian Salvation Government
Turkish Entities
Unknown
Other

Risk Mitigation and Management

The section E focuses on risk mitigation and management.

E1. Mitigation Strategies

A systematic management of risk at all levels of the organization and at each stage of programming cycle improves planning efficiency and service delivery and allows better and more reliable decision-making, as well as strengthen the overall governance and accountability. Therefore, a sound and practical approach-based risk management strategy is an integral part of strategic planning and results-based management.

➢ E1 data field is an open text field with character limitation.
➢ Once the data is entered the character limit is displayed.
➢ There is also a hyperlink 'Please click here to develop Risk Mitigation Strategy', which take the user to Risk Mitigation Strategy development tool.
➢ This tool provides a step-by-step guidance to facilitate the process.
➢ Once the strategy is developed using the strategy development tool, there is hyperlink 'Please click here to go back to Risk Analysis Tool' which brings the user back to the main interface of the risk analysis tool.
➢ The figure 10 below illustrates both hyperlinks;

Figure 10 – Hyperlinks

E2. Gaps

Based on the context, a very sound mitigation strategy may have some external or internal factors, that beyond its control. These gaps require special attention and specific control to be introduced and put in to place to facilitate the smooth implantation of the strategy.

➢ E2 data field is an open text field with character limitation.
➢ Once the data is entered the character limit is displayed.

E3. Controls

What measures and controls need to put in place to overcome the mitigation gaps?

➢ E3 data field is an open text field with character limitation.
➢ Once the data is entered the character limit is displayed.
➢ Use this field to list the controls needed to address the gaps mentioned in E2.

E4. Strategy Owner(s)

Strategy and risk ownership; once a risk identified, should be assigned to an owner who has responsibility for ensuring that the risk is managed and monitored over time. The owner must have sufficient authority to manage the risk sufficiently.

A risk owner is a person or department that has been given the authority to manage a particular risk and is accountable for doing so.

- ➢ E4 data field is an open text field with character limitation.
- ➢ Once the data is entered the character limit is displayed.

E5. Coordination Needs

To effectively and efficiently implement the mitigation strategy and the process, the organization may need to coordinate with different stakeholders, particularly for external risks.

- ➢ E5 data field is an open text field with character limitation.
- ➢ Once the data is entered the character limit is displayed.
- ➢ Use this field to list the stakeholders to be coordinated as well as what type of coordination is needed.

Performance Monitoring

This section is dedicated to review and monitor the risk mitigation and management performance.

F1. Mitigation Outcomes

Based on the given monitoring details and review frequency decided in the mitigation strategy, the management convene to review the performance and outcomes of risk management to decide the next steps. This section is used to record these notes and action points if any.

- ➢ F1 data field is an open text field with character limitation.
- ➢ Once the data is entered the character limit is displayed.
- ➢ Use this field to record the notes on mitigation outcomes.

F2. Follow-up Notes/Next Review Date

This section is used to record the follow-up notes, action points and to assign the next review date to review the performance of the mitigation and management of the reported risk.

- ➢ F2 data field is an open text field with character limitation.
- ➢ Once the data is entered the character limit is displayed.
- ➢ Use this field to record the notes, action point and next review date.

Residual Risk

This section is assigned to residual risk analysis.

G1. Residual Risk

Residual risk is a risk remaining after risk mitigation measures have been implemented.

- ➢ G1 is a dropdown list with only two options i.e. 'Yes' and 'No'.
- ➢ The data fields of **G2**, **G3** and **G4** are only activated when 'Yes' is selected in the G1.

G2. Impact

As noted above in the section 'D', impact is the effect of residual risk relative to the achievement of the objective.

- ➢ A five-stage impact scale is used in accordance with ISO31000, 31004, 31010 – Risk Management Standards.
- ➢ The following are five stages of impact scale;
    1. Very Low
    2. Low
    3. Medium
    4. High
    5. Very High
- ➢ G2 only becomes active if response in **G1** is positive.
- ➢ G2 is a dropdown list, with single selection option.

G3. Likelihood

As noted above in the section 'D', likelihood of the residual risk is the possibility and/or probability that the residual risk will occur.

- ➢ A five-stage probability scale is used in accordance with ISO31000, 31004, 31010 – Risk Management Standards.
- ➢ The following are five stages of probability scale;
    1. Very Unlikely
    2. Unlikely
    3. Moderately Likely
    4. Likely
    5. Very Likely
- ➢ G3 only becomes active if response in **G1** is positive.
- ➢ G3 is a dropdown list, with single selection option.

G4. Residual Risk Rating

Residual risk is a risk remaining after risk mitigation measures have been implemented. The comparison between residual and inherent risk rating helps to identify the effectiveness of risk control.

- ➢ Residual Risk rating is the product of risk impact and likelihood and is expressed as a whole number ranging between 1~25.
- ➢ G4 is a locked field with automatic calculation enabled.
- ➢ G4 only becomes active if response in **G1** is positive.
- ➢ Once the inherent risk rating is calculated the tool plots it as a '**RED**' dot on the heat map at the right bottom corner of the tool.

Generating Report

Once the complete data is entered for the risk to be reported, the tool automatically generates the risk report, and saves it as a pdf format document on the desktop of the user's computer.

To generate the report, click on the button 'Generate Report', as shown in the figure 11 below;

Figure 11 – Generate Report

Export the Report as PDF

➢ Once the 'Generate Report' button is clicked, the tool automatically generates the report.
➢ The report is generated in pdf format.
➢ By default, the generated report is named with the record **index** number i.e. **Risk Report - Index7.pdf**
➢ The report is saved on the desktop of the user's computer.
➢ The report can easily be copied to any other device and can be renamed as well as.

Frequently asked questions

When to use this tool?

There is not prescribed frequency, or time to use this tool. It depends on the management and the decision makers' needs and discretion whenever they deem it appropriate to use this tool. However, 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, organizations decision-makers are better able to evaluate the impact of a particular; 'decision' or 'action' on the achievement of the organization's objectives.

For further details, please refer to risk management guidelines section 2.1 (Introduction pp. 4)

How frequently the tool should be used?

As already noted above, there is not any prescribed timeline to repeat this tool, however, the repeated use of this tool will be subjected to the following:

➢ The frequency set in the performance review of a reported risk.
➢ Whenever the management or decision makers deem it necessary to use.

Pre-preparations before using the tool?

It is recommended that the data in the tool should be entered based on a collective decision of the team, and hence, should reflect the holistic and agreed parameters and factual figures, than personal opinions.

How to share the data from the tool?

There the following two ways to share the data from this tool;

➢ In pdf format as the report that the tool generates.
➢ As a matrix copied from the risk register.

How can I update the lists for the dropdowns?

As noted earlier, the tool is password protected, because of the heavy scripting running in the background of the tool enabling it to perform its functions properly. Therefore, it is not possible for an end user to update the list by him/herself.

To update any list in the drop down, please coordinate with Information Management Unit of UNOCHA Turkey office.

Can I customize the tool to best suit my organizational needs?

The tool is adaptable and compatible to customization.

However, as stated above, due to the advance programming, an end user might not able to customize the tool properly. Therefore, it is recommended to consult Information Management Unit of UNOCHA Turkey office, for your customization needs.

Annex 1 – Table B4 – Risk Sub-Category

1. **External**: Access; Aid Diversion; Quality, Accountability and AAP; Safety & Security; Environment; Other.

Access
Denial of Access
Poor Infrastructure
Restriction of Movement
Other
Aid Diversion
Diversion of Aid
Denial of Humanitarian Needs
Interference in Implementation
Other
Quality, Accountability and AAP
Accountability to Affected Populations
Coordination Partnership
Quality of Service Delivery
Accountability System and Practices
Other
Safety & Security
Safety and Security of Affected Populations
Safety Security of NGOs Personnel Assets Infrastructure Facilities
Other
Environment
Environmental Constraint
Climatic Conditions
Other

2. **Internal**; Administrative; Financial; Human Resources; Logistics Procurement; Operational; Programmatic; Other.

Administrative
Absence of Code of Conduct
Lack of Proper and/or Insufficient Policies/Systems
Lack of Proper Reporting and Documentation Systems
Lack of Proper and/or Insufficient Standard Operating Procedures
Poor Administrative Efficiency including Resource Management
Poor Inventory Handling
Quality, Accountability and AAP
Other
Financial
Absence of/Improper Segregation of Duties
Audit Quality of Reports Not Optimal and to Expected Standards
Delays of Disbursement/Liquidation of Funds due to poor/improper Internal Payment Procedures
Donor Fatigue and Lack of Interest in Funding
Fraud/Corruption, and Theft or Diversion of Goods/Services
Lack of Proper and/or Insufficient Internal Controls

Poor and/or Insufficient Financial Controlling and Reporting Mechanisms
Poor Financial Information and Data Quality
Poor Financial Management
Quality, Accountability and AAP
Significant Delay in Compilation of Financial Report or Refunding Unspent Balances
Other
Human Resources
Absence of Code of Conduct
Duty of Care
Ghost Employees
Lack of Proper and/or Insufficient Policies/Systems
Lack of Proper and/or Insufficient Standard Operating Procedures
Obscure Hiring System
Poor Administrative Efficiency of Human Resource Management
Quality, Accountability and AAP
Other
Logistics Procurement
Absence of Code of Conduct
Donors' Strict Adherence to 'Zero Tolerance' and Compliance Policies
Improper Management of Storage Facilities and/or Warehousing
Insufficient Understanding of OFAC General License
Lack of Proper and/or Insufficient Policies/Systems
Lack of Proper and/or Insufficient Standard Operating Procedures
Obscure System for Outsourcing and/or Contracting
Obscure System for Vendors' Vetting and Selection
Quality, Accountability and AAP
Other
Operational
Absence of Code of Conduct
Excessive use of cash transactions at the operational level
Lack of interest for Support Staff Capacity Building
Lack of Proper and/or Insufficient Policies/Systems
Lack of Proper and/or Insufficient Standard Operating Procedures
Poor Capacity of Support Staff on Safety & Security Management
Quality, Accountability and AAP
Other
Programmatic
Insufficient Coherence Between Identification, prioritization of needs and Program Design
Lack Humanitarian Program Cycle and/or Project Management Cycle
Lack of Appropriate Compliance to Donor Policies/Requirements
Lack of Appropriate Reporting to the Relevant Bodies/Donors
Lack of Effectiveness of the Humanitarian Coordination System
Lack of Proper Risk Management System
Poor Information and Data Quality and/or Poor Needs Assessment
Poor or Insufficient Capacity on Program Design and Development
Poor or Insufficient Monitoring, Reporting and Documentation of both Program and Financial Resources and Controlling Mechanisms
Poor Program Management

Quality, Accountability and AAP
Other

Annex 2 – Table B5 – Sub-Category Type

Denial of Access
Affected Populations' Access to Humanitarian Services/Assistance
Denial of Population Movement to Location of Assistance
Denied of Assistance to Certain Population Groups
Forced Movement of Population Away from Location of Assistance
General Restriction on Population Movement
Humanitarian Workers' Access to Affected Area
Humanitarian Workers' Access to Affected Communities
Humanitarian Workers' Access to Affected Infrastructure
Humanitarian Workers' Access to Government Officials
Humanitarian Workers' Access to Information/Data/Reports
Manipulating Community's Perceptions Regarding their Actual Needs
Prevention of Use of Services/Assistance
Other
Poor Infrastructure
Non-Functional State of Infrastructure
Other
Restriction of Movement
Bureaucratic Impediments from Local Civilian Authorities e.g. MoU
Checkpoints Prohibiting/Affecting Movement
Curfew(s) Imposed by Government or Local Civilian Authorities
Delay/Denial for Staff Crossing List at Border Crossings
Delay/Denial in Official Registration of a Humanitarian Organization in Turkey
Delay/Denial of Permission to Operate in NW Syria
Demonstrations by Local Communities
Fear of/Presence of IEDs/UXOs/Mines in the area
Military Operations
New Regulation for Vehicle Registration
Ongoing Hostilies
Restriction of Movement (Cross Border)
Restriction of Movement (within NW Syria)
Restriction on Movement of Female Staff, and Access to Affected Females in the Population
Other
Diversion of Aid
Asking a Portion or %age of Humanitarian Assistance
Diverting Assistance to Certain Community
Diverting Assistance to Certain Geographic Area
Diverting Assistance to Certain Thematic Area
Other
Denial of Humanitarian Needs
Affected Communities' Entitlement to Humanitarian Assistance
Anticipated Humanitarian Needs (Due to Sudden Displacement)
Cultural Challenges, such as Language Issues or Belief Systems that Inhibit Receiving Aid

Data Collection for Assessments
Existing Humanitarian Needs
Influence to Change/Manipulate the Needs of Affected Communities
People Involuntarily Forced/Encouraged Into an Area in Order to Receive Assistance
Other
Interference in Implementation
Information Sharing and Reporting
Contracting and Outsourcing
Delay/Denial for Import of Goods through Border Crossing
Inappropriate Taxation on Humanitarian Goods or Services
Lack of Documentation Preventing People from Receiving Assistance (ID Cards)
Manipulation of Beneficiaries' List (Directly or Indirectly)
Organization's Internal Operations/Processes
Procurement/Logistics Processes
Prohibition of Utilization of Certain Electronic Equipment e.g. Notepads/Tablets for Assessments and M&E
Project/program planned implementation
Publicizing/Claiming NGO Activities through Social Media
Staff Recruitment Process
Other
Accountability to Affected Populations
AAP Commitments
Other
Coordination Partnership
Coordination with Donors
Coordination with Line Ministries
Coordination with Local Authorities
Coordination with NGO Network(s)
Coordination with other INGOs
Coordination with other NGOs
Coordination with UN System Agencies
Partnership with Donors
Partnership with other INGOs
Partnership with other NGOs
Partnership with UN System Agencies
Other
Safety and Security of Affected Populations
Involuntary Return to Place of Origin
People Involuntarily Forced/Encouraged into an Area in Order to Receive Assistance
Presence of IEDs/UXOs/Mines in the Area
Other
Safety Security of NGOs Personnel Assets Infrastructure Facilities
Confiscation/Theft/Looting of Goods
Detention or Arrest of Humanitarian Staff
IED Attacks Against Infrastructure and Staff
Intimidation of/or Threats to Staff
Kidnapping/Detention of Staff or their Family Members
Killing or Physical Injury of Staff

Occupation of Humanitarian Facilities
Post-distribution Looting or Confiscation of Aid/Relief Items
Requesting Staff List and Demands to share Personal Details (Contact Details, Salary etc.)
Violence Against Personnel, Assets and Facilities
Other
Environmental Constraint
Improper Waste Disposal
Poor Water Safety Planning
Other
Climatic Conditions
Extreme Climatic Conditions
Flooding
Other

Annex 3 – Table C2 – Cluster Activity

Camp Coordination Management - CCCM
Closure of IDP Sites, Particularly Collective Centers that were Schools
IDP Tracking
Livelihood Activities
Multi-Sector Response in IDP Site
Needs Assessment in Camps
Promotion of Equal Access to Services
Promotion of Participatory Management Structures
Site Renovations/Infrastructure Improvements
Train Emergency Responders and IDP Committees
Training on Camp Governance or Protection Mainstreaming
Other
Coordination Common Services CCS
Capacity Building on Coordination/Humanitarian System
Coordination of Humanitarian Response
General/Inter-Sector Needs Assessments and Information Gathering
Provision of Security Services for Humanitarians
Strengthening/Establishment of PSEA Mechanisms
Tracking of IDPs
Other
Early Recovery
Basic Housing Repair
Basic Needs Support
Capacity and Equipment Support to Public Service Providers
Cash Assistance
Civic Engagement Initiatives
Creation of Short-Term Work
IDP Integration
Entrepreneurship Support
Rehabilitation of Basic Utilities
Rehabilitation of Education/Health Facilities or other Social Infrastructure
Rehabilitation/Repair of Economic Infrastructure

Removal of Debris and Waste
Support to Access to Regular Employment
Support to Community Initiatives
Support to Local Public Service Delivery Initiatives
Support to Small Farmers, Livestock Owners, and Fisherfolk
Vocational Skills Training
Other
Education
Establishment, Expansion or Rehabilitation of Classrooms
Incentives for Education Personnel
Non-Formal Education Programs
Provision of Learning Materials
Training of Education Personnel
Other
Emergency Shelter - NFI
Advice or Referral in Relation to HLP and Shelter
NFI Distribution
Rehabilitation of Shelter
Shelter Provision
Voucher Provision
Other
Food Security Livelihoods - FSL
Distribution of Agricultural Inputs
Early Warning/DDR Systems
Emergency Livestock Treatment/Training for Veterinary Services
Food Distribution
Rehabilitation of Economic Infrastructure
Supplementary Food Assistance
Support to Asset Building/Protection
Support to Bakeries
Support to Income-Generating Activities such as Vocational Training
Support to Small Scale Food Production
Other
Health
Capacity Building of Health Care Providers and Community Health Workers
Immunization
Mental Health Services
Mobile Medical Units
Provision of Medicine and Medical Supplies
Provision of Primary and Secondary Health Care Services
Rehabilitation of Health Facilities
Trauma Management and Disability and Rehabilitation Services
Other
Logistics
Maintain Common Logistics Services
Trainings on Logistics
Transshipment
Other

Capacity Building of Partners
Capacity Building of Public Health Staff on Reporting and Rapid/SMART Assessments
Capacity Development on Nutrition-Sensitive Agriculture
Facility and Community-Based Counselling and Awareness Raising on IYCF-E and Maternal Nutrition
Implementation of SOPs for Breast Milk Substitutes
IYCF Strategy Development
Provision of Micro-Nutrient or Vitamin A Supplementation
Provision of Specialized Nutritious Food for Children for Prevention of Malnutrition Promotion of Dietary Diversity
Rapid/SMART Assessments
Screening for Acute Malnutrition
Strengthening/Establishing Nutrition Surveillance System
Treatment of Acute Malnutrition
Other
Protection
Advocacy with Stakeholders
Capacity Building of Humanitarians or Local Authorities
Integrated Protection Services
Legal Advice/Counselling/Representation on Civil Documentation/HLP
Protection Monitoring and/or Needs/Risk Identification
Other
Protection Housing Land Property
Ownership and Legal Status of Agreements of Land Donated for Infrastructure
Other
Protection - Child Protection
Capacity Building on Child Protection
Community-Based Child Protection
Specialized Child Protection Services such as Case Management
Other
Protection - Gender Based Violence
GBV Prevention
GBV Risk Mitigation in Humanitarian Response
GBV Services including Case Management etc.
Other
Protection - Mine Action
Mine Risk Education
Survey and/or Removal of Explosive Hazards
Victim Assistance
Other
Refugee Multi Sector - RMS
RMS Coordination
Other
Return Reintegration Recovery - RRR
RRR Coordination
Other
Water Sanitation Hygiene - WASH
Cash Assistance for WASH Services

Distribution of WASH NFIs
Establishment of Water Safety Plans
Operation and Maintenance of Water Facilities
Repair/Rehabilitation of Water Systems
Support to Sewage and Solid Waste Management Systems
Other