CEB

Chief Executives Board for Coordination

HIGH-LEVEL COMMITTEE ON MANAGEMENT (HLCM)

Thirty-Eighth Session, 15-16 October 2019 UN System Staff College, Turin

Reference Maturity Model for Risk Management (Final)

Table of Contents

Background	L
Pilot of the RMM for Risk Management	2
RMM for Risk Management (final)	3
Proposed decision	1
Annex I – Survey findings	•
Annex II – Reference Maturity Model for Risk Management (Final)	•
(i) Usage guidelines	•
(ii) Summary matrix	•
(iii) Evidence checklists	•
Annex III – Terms of Reference for Cross-Functional Task Force on Risk Management	•

Background

- At its 35th session, HLCM examined how United Nations system organisations have been developing and putting in place risk management tools and frameworks to reform management processes, improve efficiency and bring greater value in support of the 2030 Agenda for Sustainable Development. The Committee agreed on the need for joint, cross-functional engagement towards the system-wide harmonisation of risk management practices and endorsed the attached Terms of Reference (TOR) for a Task Force (TF)¹, to be co-chaired by WIPO and WFP.
- 2. Those TOR described the need for 'The definition of a multiple stage maturity model that exhibits the characteristics and features of an organisation deemed to be in each defined stage of organisational risk management maturity. The model may include maturity dimensions of, for example, risk culture, process and integration, policy framework, governance and organisational

¹ CEB/2018/HLCM/15

structure, system and tools, and risk capabilities. The model may serve as both a benchmarking tool to provide consistent comparison of UN system organisations' risk management maturity, and also as an implementation guide to advance risk management in the organisation.'

- 3. The TF included those organisations who responded to a call for nominations, and by October 2019 included FAO, IAEA, IFAD, ILO, IOM, OECD, UN Secretariat (including DSS and OCHA), UNAIDS, UNDP, UNEP, UNFPA, UNHCR, UNICEF, UNIDO, UNRWA, UNWOMEN, WFP, WHO and WIPO.
- 4. A survey was conducted in December 2018 with the purpose of identifying the areas of interest for the TF's work, this survey was summarized at the HLCM's 37th session.
- 5. The TF began its work on Reference Maturity Model (RMM) for Risk Management in October 2018 and at the37th session of HLCM, a Co-Chair presentation was made together with the draft RMM. At this session it was proposed to run a limited pilot with UN organisations to validate the RMM.
- 6. The report at the 37th session also noted that: 'From the outset, the model was conceived to be a management improvement initiative, to be non-prescriptive, scalable, applicable to all UN entities, and not a compliance initiative. It was recognized that the model should present indicative characteristics, and to be applicable to a broad range of operating environments and mandates, including HQ-based organisations, as well as organisations with multiple field / country office structures. It is thus anticipated that entities will in practice adapt this model to fit their mission and mandate, and their vision for how risk management contributes to improved performance and the delivery of stakeholder value.'
- 7. This report provides information to the HLCM on the finalized RMM for Risk Management, and proposes its endorsement. Organisations may choose to plan their own risk maturity assessment using the model, and subsequently develop a road map to strengthen risk management as guided by the RMM.

Pilot of the RMM for Risk Management

- 8. A sub-group was self-selected to consider the most effective questions to ask in order to validate the comprehensiveness and suitability of the RMM. A survey was developed with the intention to solicit candid and relevant feedback on the usage and output of the RMM. It was decided to ensure full anonymity of survey respondents, in order to garner honest, critical advice.
- 9. The survey was sent to all TF members on July 12, 2019 indicating a deadline for responses by September 6, 2019. In actuality, all responses provided up to and including September 13, 2019 have been included in this report. An online tool guaranteed responses remained anonymous, questions relating to the organisation type were minimal and optional. The full survey questions and responses can be found in the report Reference Maturity Model (RMM) for Risk Management Survey Findings (attached as Annex I).

- 10. In summary, eight organisations undertook a self-assessment using the RMM, and reported their findings. The basic organisational information indicated a good spread of larger and smaller UN organisations both HQ-based and field-based.
- 11. Regarding the spread of maturity reported in the responses, level '2-Developing' and '3-Established' were most commonly selected across all dimensions, except for ERM Framework and Policy, where '3-Established' and '4-Advanced' were the two most popular selections.
- 12. Regarding the perceived usefulness of the RMM, on a scale of 'not at all useful', 'quite useful', 'very useful' and 'extremely useful', the most popular response was 'very useful' for the establishment of (i) an organisation's current maturity level (ii) an organisation's target maturity level; and (iii) an organisation's risk management roadmap to achieve its target maturity level.
- 13. A number of pertinent and constructive comments were made concerning refinements that could be made in light of experiences of using the model. In general, these comments related to the following refinements: (i) adding greater granularity and clarity to the detail question sheets; and (ii) Clarifying more precisely maturity at initial and leading levels. A number of modifications were subsequently made to the model and detailed question sheets to incorporate this feedback.

RMM for Risk Management (final)

- 14. The RMM comprises three principal elements, attached as Annex II.
 - (i) Usage Guidelines that detail how the model was designed to be used;
 - (ii) A summary matrix, which presents the key aspects of the reference model on one page; and
 - (iii) The evidence checklists, which help provide clarity and propose evidence that would confirm an organisation's assessment of its maturity.
- 15. The RMM maturity levels are defined as follows:
 - (i) **Initial**: Unstructured, managed informally/ inconsistently, ad hoc, reactive;
 - (ii) **Developing**: Structured implementation, basic architecture, some reporting and repeatable management processes;
 - (iii) **Established**: Defined/documented and standardized processes, good organisational coverage, some evidence of use and embedding. Regular reporting and escalation, information used in operational decision making;
 - (iv) Advanced: Well structured, strong evidence of embedding. Standardized reporting and thresholds for escalation and management action. Information used in strategic decision making; and
 - (v) Leading: Fully embedded risk management processes; escalation mechanisms well understood and used at all levels of the organisation. Innovative/creative approach delivers continuous improvement and is able to adapt as the organisation changes.
- 16. The RMM substantive dimensions are defined as follows:

- (i) Enterprise Risk Management (ERM) Framework and Policy: are the collection of policies, procedures and other documents that together describe how the organisation undertakes its risk management;
- (ii) **Governance and Organisational Structure:** sets out the internal risk governance structure, the appropriate delegated authority, roles and responsibilities, and organisational entities to assure the effective management of risk;
- (iii) Process and Integration: "Process" ensures that risks and opportunities that may affect the delivery of organisational results are effectively identified, assessed, responded to, communicated and monitored as per the ERM framework. "Integration" ensures that the interaction / interlinkages with related risk sub-processes or other organisational processes are clearly established;
- (iv) **Systems and Tools:** are the IT components used to record, analyse, integrate and communicate/report on risk information;
- (v) **Risk Capabilities:** are the skills, ability, knowledge and capacity that an organisation has to effectively manage risks to delivery of its results; and
- (vi) **Risk Culture:** is evidenced by the shared values, beliefs, and behaviours of the staff and senior management, together with the organisation's demonstrated attitude to risk.
- 17. The RMM is now considered final, and ready for use should organisations wish to undertake a maturity assessment. The time required for a maturity assessment is largely a function of the size and complexity of the organisation, the scope of the assessment, and the level of detail assessed (e.g. per location, or one overall). Some task force pilot organisations reported undertaking a basic assessment within a work day, whereas others used the services of an external consultant to undertake a detailed assessment of a number of work areas over an extended period.
- 18. Once an organisation has undertaken a maturity self-assessment, the RMM is intended to guide the organisation to develop a risk management roadmap, to strengthen those areas that have fallen behind other maturity elements.

Proposed Decision

19. The HLCM is invited to consider and endorse the RMM and its related documents (as presented in Annex II), to be used as an internal benchmarking and planning tool to help UN organisations identify, for their own needs, (i) their current maturity stage (ii) their target maturity stage; and (iii) to provide a basis for continual improvement.

Annex I - Reference Maturity Model for Risk Management Survey Findings

HLCM Cross-Functional Task Force on Risk Management

Reference Maturity Model for Risk Management Survey Findings

September 2019



Table of Contents

1. Introduction	2
2. General observations about respondents	2
2.1. Q1: What is the approximate number of staff in your organisation?	2
2.1.1. Analysis:	2
2.2. Q2: At which maturity level(s) did you assess your entity for each dimension? You may select multiple levels for each dimension if necessary (Optional)	
2.2.1. By Dimension	3
2.2.2. By Organisation	4
2.2.3. Analysis:	6
2.3. Q3: Was the maturity level that the matrix indicated in line with what you expected? Did you have multiple levels of maturity for a single dimension? If so, were they adjacent levels? Please provide details as appropriate	
2.4. Q4: Please make any other comments about the Summary RMM worksheet. This could include, for example typographical issues, sub-dimensions, irregularities. Please note comments about the question worksheets can be made later	7
2.5. Q5: If any of the questions (in column B of the detail worksheets) were unclear, what could be done to improve clarity?Were there any overlaps, gaps or other issues?	7
2.6. Q6: Regarding the possible responses in the question sheet, could you find the evidence indicated (where applicable)? Were the responses consistent within the various elements of the RMM?	
2.7. Q7: How useful is the RMM to establish: (select all the apply) An organisation's current maturity level? An organisation's target maturity level? An organisation's risk management roadmap to achieve its target maturity level?	8
2.7.1. Analysis:	8
2.8. Q8: Please provide any final comments	9
3. Overall findings and Actions taken	9

1. Introduction

The Cross-Functional Task Force on Risk Management developed a Reference Maturity Model (RMM) for Risk Management that was endorsed by the United Nations High Level Committee on Management at their 37th session in Bonn, Germany in April 2019.

At that time, the approach presented proposed a pilot of the RMM, in order to obtain any final refinements to the model. All organisations on the Task Force were invited to pilot the model during July and August 2019. The findings of each organisation were reported in a survey.

This report summarises the findings of that survey.

2. General observations about respondents

The survey was deliberately anonymous in order to encourage organisations to respond informally, and transparently. The survey was communicated to close on September 6, 2019, and in actuality, all responses provided up to and including September 13, 2019 have been included in this report.

A total of 14 responses were received, and each full response has been saved in a raw data file. Of those, six have been excluded, since they included no information other than the first question on organisation size. This may well have been organisations who did respond later, checking the questions in the questionnaire.

2.1. Q1: What is the approximate number of staff in your organisation?

This question was intended to provide an overview of the breadth of organisations who responded, as well as to help understand better the context in which any comments were made.



Figure 1: Size and nature of responding organisations

2.1.1. Analysis:

- Of the eight respondents, one indicated both their **HQ and Field** based personnel, which explained the total count of nine. If that response is not considered, a ratio of 4:3 HQ:field is observed.
- In terms of the size of organisations that responded, the one that responded both HQ and field-based showed above 5000, thus one of the 1001-5000 (its other response) is not considered. This results with two organisations with 251-1000, two organisations 1001-5000 and four organisation over 5000 personnel. This indicates a good spread over respondents' organisational size.

2.2. Q2: At which maturity level(s) did you assess your entity for each dimension? You may select multiple levels for each dimension if necessary (Optional).

The intention of this question was to understand if responding organisations represented a fair spread of maturity and also to put the responses into the context of the organisation's maturity. Finally, it intended to find out if organisations had assessed themselves having multiple maturity levels, and especially if there was a gap between of levels between any such cases.

2.2.1. Summary of all responses

In the table below, each response is represented by an X. In the cases where multiple levels were selected, all are shown.

	1 - Initial	2 - Developing	3 - Established	4 - Advanced	5 - Leading
I. ERM Framework and Policy		х	ххххх	ххх	х
II. Governance and organisational Structure		ххх	XXXXX XXX		x
III. Process and Integration	х	хххх	хххх	хх	
IV. Systems and Tools	x	хххх	ххх	х	
V. Risk Capabilities	х	хххх	ххххх	ХХ	
VI. Risk Culture	Х	хххххх	ХХХ	ХХ	X

2.2.2. By Dimension

I. ERM Framework and Policy

	1 - Initial	2 - Developing	3 - Established	4 - Advanced	5 - Leading
Org 1					
Org 2					
Org 3					
Org 4					
Org 5					
Org 6					
Org 5 Org 6 Org 7					
Org 8					

II. Governance and organisational Structure

	1 - Initial	2 - Developing	3 - Established	4 - Advanced	5 - Leading
Org 1					
Org 2					
Org 3					
Org 3 Org 4					
Org 5					
Org 6					
Org 7					
Org 8					

III. Process and Integration

	1 - Initial	2 - Developing	3 - Established	4 - Advanced	5 - Leading
Org 1					
Org 2					
Org 3					
Org 4					
Org 2 Org 3 Org 4 Org 5					
Org 6					
Org 7					
Org 8					

IV. Systems and Tools

	1 - Initial	2 - Developing	3 - Established	4 - Advanced	5 - Leading
Org 1					
Org 2					
Org 3					
Org 4					
Org 5					
Org 6					
Org 7					
Org 8					

V. Risk Capabilities

	1 - Initial	2 - Developing	3 - Established	4 - Advanced	5 - Leading
Org 1					
Org 2					
Org 3					
Org 4					
Org 5					
Org 6					
Org 7					
Org 8					

VI. Risk Culture

	1 - Initial	2 - Developing	3 - Established	4 - Advanced	5 - Leading
Org 1					
Org 2					
Org 3					
Org 3 Org 4 Org 5					
Org 5					
Org 6					
Org 7					
Org 8					

2.2.3. By Organisation

Organisation 1

	1 - Initial	2 - Developing	3 - Established	4 - Advanced	5 - Leading
I. ERM Framework and Policy					
II. Governance and organisational Structure					
III. Process and Integration					
IV. Systems and Tools					
V. Risk Capabilities					
VI. Risk Culture					

RMM Survey findings

Organisation 2

	1 - Initial	2 - Developing	3 - Established	4 - Advanced	5 - Leading
I. ERM Framework and Policy					
II. Governance and organisational Structure					
III. Process and Integration					
IV. Systems and Tools					
V. Risk Capabilities					
VI. Risk Culture					

Organisation 3

	1 - Initial	2 - Developing	3 - Established	4 - Advanced	5 - Leading
I. ERM Framework and Policy					
II. Governance and organisational Structure					
III. Process and Integration					
IV. Systems and Tools					
V. Risk Capabilities					
VI. Risk Culture					

Organisation 4

	1 - Initial	2 - Developing	3 - Established	4 - Advanced	5 - Leading
I. ERM Framework and Policy					
II. Governance and organisational Structure					
III. Process and Integration					
IV. Systems and Tools					
V. Risk Capabilities					
VI. Risk Culture					

Organisation 5

	1 - Initial	2 - Developing	3 - Established	4 - Advanced	5 - Leading
I. ERM Framework and Policy					
II. Governance and organisational Structure					
III. Process and Integration					
IV. Systems and Tools					
V. Risk Capabilities					
VI. Risk Culture					

Organisation 6

	1 - Initial	2 - Developing	3 - Established	4 - Advanced	5 - Leading
I. ERM Framework and Policy					
II. Governance and organisational Structure					
III. Process and Integration					
IV. Systems and Tools					
V. Risk Capabilities					
VI. Risk Culture					

RMM Survey findings

Organisation 7

	1 - Initial	2 - Developing	3 - Established	4 - Advanced	5 - Leading
I. ERM Framework and Policy					
II. Governance and organisational Structure					
III. Process and Integration					
IV. Systems and Tools					
V. Risk Capabilities					
VI. Risk Culture					

Organisation 8

	1 - Initial	2 - Developing	3 - Established	4 - Advanced	5 - Leading
I. ERM Framework and Policy					
II. Governance and organisational Structure					
III. Process and Integration					
IV. Systems and Tools					
V. Risk Capabilities					
VI. Risk Culture					

2.2.4. Analysis:

The tables by dimension illustrate that the survey respondents represented a broad mix of assessed maturity, clustering around developing and established, with each maturity dimension being noted the following number of times:

1 - Initial	2 - Developing	3 - Established	4 - Advanced	5 - Leading
4	23	26	13	3

The tables by organisation illustrate that the spread across maturity levels by dimension appear to be well balanced. There are some isolated cases where an organisation's maturity differs greatly depending on the dimension, which may simply be the case. In one case, risk culture has been assessed as 2, 3 and 5, which can be investigated further.

In only five cases out of the 69 dimensions reported were there three assessed maturity levels, although over half of these were in one organisation. In over 75% of dimensions assessed, a single maturity dimension was reported.

2.3. Q3: Was the maturity level that the matrix indicated in line with what you expected? Did you have multiple levels of maturity for a single dimension? If so, were they adjacent levels? Please provide details as appropriate.

Comments received:

Yes we did have multiple levels since some functions/ activities and perhaps larger operations are more sophisticated.

A little bit on the high end. When level 3, 4 and 5 all say "yes", level 5 would be selected by default. Suggest to ensure there is nuance between levels.

Yes, the maturity level assessed was in line with what we expected. For each dimension, we had different levels of maturity, but most of the times they were adjacent (between level 1 and 3).

Maturity level is what we expected. No. N/A.

yes. no multiple level

Yes it was in line with our expectations. Yes we did have multiple levels of maturity across sub-dimensions

Yes. We have an established structure, policies and processes. and the issue is now to embed the culture into the organisation

In line with expectations. Could not always map cleanly from a sub-dimension to a maturity level.

2.4. Q4: Please make any other comments about the Summary RMM worksheet. This could include, for example typographical issues, subdimensions, irregularities. Please note comments about the question worksheets can be made later.

Comments received:

It is good to have different colors, it makes readable.

For the assessment of the maturity level of the different dimensions, it was complicated to decide on a level in particular. In other words, our results between the summary and the worksheet differs. Also, for some of the dimensions our level was in between of two levels.

The application was most inconsistent at the "initial" and "leading" levels.

- For example, at the "initial" level there should be some basic requirements in place (otherwise there would be a score of "0" earned). But this was not the case across the board, for example section II had no "initial" requirements at all and sections I, IV and V had only very limited definitions of what would constitute an "initial" level.

- For a "leading" score there generally should be criteria relating to an external view (consideration/involvement of stakeholders) and some element of learning and adapting to change based on the result of the process. Sections, II, IV, V and VI could benefit from a review of the "leading" methodology.

The "established" state should be basic requirement of each element, with developing and advanced showing gradients on either side. These are much more nuanced and should be even more carefully reviewed as the majority of the scorings will be in these areas.

Quite wordy, can we make the statements in each box a little more succinct?

Process and RISK Integration

2.5. Q5: If any of the questions (in column B of the detail worksheets) were unclear, what could be done to improve clarity? Were there any overlaps, gaps or other issues?

Comments received:

In some cases the questions are not comprehensive, and in others some questions overlap. Our solution was to weight the questions in importance, so that we came up with a usable score. Also questions should be more consistently evidential/objective rather than 'gut feel'.

Eliminate "double barrelled" questions

- In a number of the detailed questions and documentation points there are two (or more) criteria joined by the word "and". As a result, it is very unclear how to score the items if only one item is present, or one is a more mature state of development than the other. This makes the questions unduly complex to decipher. If this can't be eliminated (which is preferable), then additional instruction could be provided in the levels of maturity. (For ex if A or B = level 3; if A and B = level 4....)

- It would be optimal for each box/cell to include only one element or criteria to be assessed by that question.

Most of the questions were clear. We would suggest to change questions II(1) and II(9).

Questions are very well formulated

2.6. Q6: Regarding the possible responses in the question sheet, could you find the evidence indicated (where applicable)? Were the responses consistent within the various elements of the RMM?

Comments received:

We sought to answer the questions, then separately we considered our evidence, then sometimes adjusted responses. Problem is that we're a large organisation so there's always some evidence to draw on, but is it sufficient?

Yes, we did not have problems. See previous response for some suggestions.

Yes and Yes

yes. consistent

Yes - generally we could find the evidence but it was not necessarily clear from the evidence what level we should be.

2.7. Q7: How useful is the RMM to establish: (select all the apply) An organisation's current maturity level? An organisation's target maturity level? An organisation's risk management roadmap to achieve its target maturity level?

There were some issues noted with this question, where in the earlier responses, respondents were not able to select more than one answer "extremely useful". This technical error was fixed after it was reported.

	NOT AT ALL USEFUL-	QUITE USEFUL-	VERY USEFUL-	EXTREMELY USEFUL-	TOTAL-
An organisation's current maturity level?	0	2	3	2	7
An organisation's target maturity level?	0	1	5	0	6
An organisation's risk management roadmap to achieve its target maturity level?	0	3	4	0	7

2.7.1. Analysis:

Overall, respondents found the RMM 'very useful' for assessing an organisation's target maturity level.

All respondents selected at a minimum 'quite useful' for all proposed uses.

2.8. Q8: Please provide any final comments.

Comments received:

It is helpful in identifying gaps and priorities.

Questionnaire for self-assessing each dimension is missing.

Great work! kindly note that question 7 was impossible to answer.

We will send more detailed comments on the model separately - overall it is a great tool but needs more clarity on how to calculate levels given variance across location and functions in maturity. - Overall many of the statements are absolute or binary whereas the reality is we do them to varying extents in different field and HQ locations - the model makes it hard for us to know where to place ourselves as we cannot simply answer 'yes' or 'no'. The detailed questions should reflect the extent to which certain criteria are met at different levels (e.g. always for advanced, or most of the time for established). Also quality was not featured enough - for example we could have a basic risk appetite in place on one sheet of paper and meet the criteria.

- Final point - we note that at established there are already a number of interdependencies on different organisational systems (i.e. RBM, ICF) that may stop an organisation being established if its risk management is very strong but RBM is weak (for example). It may be worth considering moving these interdependencies to level 4.

Wanted to put extremely useful for each of the above but survey will not allow multiple responses with the same selection

3. Overall findings and Actions taken

The comments were overall very positive, indicating that respondents were able to use the model to assess their current risk management maturity, and to plan for moving towards their target state.

Certain findings or comments merit further consideration as part of the RMM pilot stream, the following table summarizes the actions to be considered.

Finding or comment	Actions taken
For the assessment of the maturity level of the different	Thorough check of the summary table
dimensions, it was complicated to decide on a level in	and the worksheet undertaken. Refine
particular. In other words, our results between the	the worksheet as necessary to agree
summary and the worksheet differs.	with the summary sheet.
Our prost to an our others is much as hot up on lowels	
Suggest to ensure there is nuance between levels.	
Could not always map cleanly from a sub-dimension to	
a maturity level.	
In some cases the questions are not comprehensive,	
and in others some questions overlap. Our solution	
was to weight the questions in importance, so that we	
came up with a usable score. Also questions should be	
more consistently evidential/objective rather than 'gut	
feel'.	
We would suggest to change questions II(1) and II(9).	Reviewed questions II(1) and II(9) for potential changes for clarity /
	consistency.

The application was most inconsistent at the "initial" and "leading" levels. - For example, at the "initial" level there should be some basic requirements in place (otherwise there would be a score of "0" earned). But this was not the case across the board, for example section II had no "initial" requirements at all and sections I, IV and V had only very limited definitions of what would constitute an "initial" level. - For a "leading" score there generally should be criteria relating to an external view (consideration/involvement of stakeholders) and some element of learning and adapting to change based on the result of the process. Sections, II, IV, V and VI could benefit from a review of the "leading" methodology.	A number of refinements have been made to 'leading' based on the comments. For the comments on 'initial', this is as designed.
One organisation found they had assessed maturity levels 2, 3 and 5 for Risk Culture	Investigated how this could have been, by reviewing the differences. However, this must be an error, since the summary table notes 'Each maturity level adds to the previous level'. This guidance will be made clearer in the instruction sheet to accompany the RMM.
Quite wordy, can we make the statements in each box a little more succinct?	In light of the summary table having already received HLCM endorsement, changes to the summary sheet are only sought where inaccurate. Reviewed detailed sheets with a view to shortening sentences where possible.
Process and RISK Integration	Reviewed this sub-dimension for any particular needs.
Questionnaire for self-assessing each dimension is missing.	The detailed sheets were perhaps missing from the version used by this respondent.
Eliminate "double barrelled" questions - In a number of the detailed questions and documentation points there are two (or more) criteria joined by the word "and". As a result, it is very unclear how to score the items if only one item is present, or one is a more mature state of development than the other. This makes the questions unduly complex to decipher. If this can't be eliminated (which is preferable), then additional instruction could be provided in the levels of maturity. (For ex if A or B = level 3; if A and B = level 4) - It would be optimal for each box/cell to include only one element or criteria to be assessed by that question.	Reviewed and removed a number of 'double barrelled" questions. Also refined many questions to have more granularity in the possible responses.

Annex II - Reference Maturity Model for Risk Management

- (i) Usage Guidelines
- (ii) Summary matrix
- (iii) Evidence checklists

HLCM Cross-Functional Task Force on Risk Management

Reference Maturity Model for Risk Management Usage Guidelines

September 2019



Table of Contents

1. In	itroduction	1
1.1	Background	1
1.2	Purpose of the Reference Maturity Model	1
1.3	Tailoring the Reference Maturity Model	1
1.4	Resources to undertake a self-assessment	1
2. TI	he structure of the model	2
2.1	The summary matrix	2
2.2	The evidence checklists	2
2.3	RMM maturity levels	2
2.4	RMM dimensions	3
3. U	ndertaking a self-assessment	3
3.1	Preparing for the self-assessment	3
3.2	Starting the self-assessment	4
4. Ta	aking the findings forward	5
4.1	Target state	5
4.2	Developing an implementation roadmap	5

1. Introduction

1.1 Background

Under the oversight of the HLCM, and supported by the CEB Secretariat, in November 2018 a cross functional task force was formed to develop a maturity model and guidelines concerning aspects of risk management.

The Reference Maturity Model (RMM) for Risk Management was the output of considerable interagency collaboration involving around 20 UN organisations. The summary matrix of the RMM (the first page) was endorsed by the HLCM at their 37th session in April 2019. The taskforce then finalised evidence checklists, explained further in this document, and piloted the model across eight UN organisations.

This explanatory note has been developed to assist organisations to use the model.

1.2 Purpose of the Reference Maturity Model

From the outset, the model was conceived to be a management improvement initiative, to be nonprescriptive, scalable, and applicable to all UN entities. It was recognised that the model should present indicative characteristics and be applicable to a broad range of operating environments and mandates, including HQ-based organisations, as well as organisations with multiple field / country office structures.

The model is not intended to be a compliance initiative, and nor is it designed for the comparison of risk management maturity between organisations.

The purpose of the RMM is to:

- allow an organisation to perform a self-assessment of its risk management maturity;
- to identify those aspects that may benefit from strengthening, in order to bring alignment to the various dimensions; and
- to ascertain the target maturity level, considering the organisation's mandate, operating structure and size.

1.3 Tailoring the Reference Maturity Model

It is anticipated that entities will, in practice, *adapt* the RMM to suit their mission and mandate. The RMM has been developed to be scalable and can be used to assess the maturity of, for example, an entire organisation, a certain region or a field office. In order to reduce ambiguity or interpretation, an organisation may choose to make certain criteria more explicit. An organisation may simplify the model if it better suits their communication needs.

Whatever the case, organisations are free to adapt the RMM to suit their needs.

1.4 Resources to undertake a self-assessment

The amount and type of resources required directly relates to how the organisation chooses to undertake the self-assessment. Some organisations decide to bring in external expert assistance, should there be many locations to assess. Other HQ-based organisations have reported that an informed risk management specialist could undertake an overall maturity assessment in a matter of hours.

A rough guide could be one work day per location.

2. The structure of the model

2.1 The summary matrix

The summary matrix is illustrated in Figure 1. It shows a table with five maturity levels, from 1-Initial to 5-Leading on the horizontal axis, as described in <u>section 2.3</u>. For each maturity level, the criteria for achieving that level is expressed on the vertical axis, in terms of six dimensions, as described in <u>section 2.4</u>. Each dimension is, in turn, articulated in between two and five sub-dimensions.



Five maturity levels

Figure 1: The Summary Matrix

Five maturity levels

	I. ERM Framework and Policy	INITIAL	DEVELOPING	ESTABLISHED	ADVANCED	I FADING
Sub-dimensions copied from	Framework implementation and appetit			ESTRELEMED The organisation has established an ERM framework and defined risk appethe (or risk criteria) in some areas and related escalation procedures, which have been approved by the appropriate delegated authority.	The organisation has implemented an ERM framework including risk appetite, tolerance (or criteria) together with a related repeatable escalation process, which have been approved by the appropriate delegated authority. The ERM framework is integrated	The organisation, recognised as a leader among peers and risk innovator, has embedded an ERM framework and risk appetite, tolerance and criteria and related escalation process, which have been approved by the appropriate delegated
Summary Matrix	Framework components and coverage	An implicit risk management framework is place without being formably codified.	In Limited framework components are in place	The organisation has issued risk guidelines, policies, procedures and has implemented key related processes. A risk scale (e.g. rating) is established for the organisation in the context of las programme/project management.	The ERM framework is tailored to appropriately reflect RBM and decentralised to address the needs of all operational entities (including HA), field, program, project). Granular integrated related risk scales (e.g. rating) for different hierarchical levels (e.g. enteprise, program, project) or a single appropriate organisation scale is in	The ERM Framework is integrated in strategy setting, planning, decision making and enterprise integrated performance management.
(Framework implementation and appetite					
	1 How would you describe your overarching E	RM Framework? Fragmented - some elements exist but not cohesive	Developed, but not approved or approved but not comprehensive for the entire organization	Comprehensive and approved by the appropriate delegated authority	Integrated into strategy setting, planning and decision making	Seen by key stakeholders as a source of competitive advantage
	2 Does your organisation have a risk appetite process?	(or criteria) escalation No	Limited / intuitive	Yes, describes existing risk-taking escalation practices	Yes, updated regularly and guides work planning	Yes, guides strategy planning, implementatio and reporting
Questions	3 Are mechanisms implemented to ensure that stakeholders is actively sought, and that the regularly updated?		Limited / informal	Ad hoc feedback and review		Systematic feedback and review on an ongoing basis including with key external stakeholders
per sub- dimension	Framswork components and coverage 4 How would you describe your organisation's procedures and -processes?	risk guidelines, policies, Very limited - perhaps components exist at a project or office level	Under development, but limited in scope and coverage	Issued guidelines, policies, procedures & implemented key related processes	Tailored, addresses the needs of all operational entities	Integral to organisational processes
	5 How would you describe the risk scales (risk impact)?	ratings for likelihood and Simple scale with limited substantive complexity	Certain entities may use their own scales	Risk scale (e.g. rating) is established for programme/project management	Multiple entities have inter-related - or the same risk rating scale, with consistent qualitative dimensions	Multiple entities have inter-related - or the same risk rating scale, with some quantitative dimensions
Documented	6 How would you describe the ERM frameword organisational processes and coverage?	Ks integration with other Not integrated or existent.	Limited	Risk management process integrated at time of planning and considered with internal controls	The ERM framework is fully integrated in planning and partially integrated with internal controls, strategy setting and decision making.	The ERM Framework drives strategy setting, planning, decision making, internal controls and enterprise performance management
	DOCUMENTATION / EVIDENCE TO VERI					
evidence to	1 Overarching ERM framework/policy docume 2 RM operating procedures / guidelines	ntation Fragmented, limited No	Not approved Under development	HQ plus maybe other entities. Yes but of limited sophistication and detail	Over 75% organisation coverage Yes	Organisation 100% covered Yes
	3 Risk appetite (or criteria) Statement and rela	ted escalation procedures No	Under development	Yes in certain limited areas	Yes	Yes
support 1	4 Accountability framework documentation	No	Under development	Yes but not comprehensive or fully linked to ERM	Yes	Yes
	5 Internal control framework documentation	No	No	Yes but not comprehensive or fully linked to ERM	Yes	Yes
responses	6 Planning and performance management risk procedures	obased policies and No	No	Partial	Partial	Yes

Figure 2 - the evidence questionnaire

Each dimension's information from the Summary Matrix is repeated on the evidence checklists in the first rows. Below that, a series of questions and related responses are used to establish the maturity level. The last rows correspond to tangible documents or other evidence, used to support the overall assessment.

2.3 RMM maturity levels

The RMM maturity levels are defined as follows:

- (i) **Initial**: Unstructured, managed informally/ inconsistently, ad hoc, reactive.
- (ii) **Developing**: Structured implementation, basic architecture, some reporting and repeatable management processes.
- (iii) **Established**: Defined/documented and standardised processes, good organisational coverage, some evidence of use and embedding. Regular reporting and escalation, information used in operational decision making.

2.2 The evidence checklists

- (iv) Advanced: Well structured, strong evidence of embedding. Standardised reporting and thresholds for escalation and management action. Information used in strategic decision making.
- (v) Leading: Fully embedded risk management processes; escalation mechanisms well understood and used at all levels of the organisation. Innovative/creative approach delivers continuous improvement and can adapt as the organisation changes.

2.4 RMM dimensions

The RMM substantive dimensions are defined as follows:

- (i) Enterprise Risk Management (ERM) Framework and Policy: are the collection of policies, procedures and other documents that together describe how the organisation undertakes its risk management. Sub-dimensions: Framework implementation and appetite; Framework components and coverage.
- (*ii*) **Governance and Organisational Structure:** sets out the internal risk governance structure, the appropriate delegated authority, roles and responsibilities, and organisational entities to assure the effective management of risk. *Sub-dimensions: Governance structure; Delegation of authority; Function*
- (*iii*) **Process and Integration:** "Process" ensures that risks and opportunities that may affect the delivery of organisational results are effectively identified, assessed, responded to, communicated and monitored as per the ERM framework. "Integration" ensures that the interaction / interlinkages with related risk sub-processes or other organisational processes are clearly established. *Sub-dimensions: Process; Integration with internal controls; Integration with planning.*
- *(iv)* **Systems and Tools:** are the IT components used to record, analyse, integrate and communicate/report on risk information. *Sub-dimensions: Platforms, systems and tools; Links to other systems.*
- (v) **Risk Capabilities:** are the skills, ability, knowledge and capacity that an organisation must effectively manage risks to deliver its results. *Sub-dimensions: Competencies; Capacity; Reporting.*
- (vi) Risk Culture: is evidenced by the shared values, beliefs, and behaviours of the staff and senior management, together with the organisation's demonstrated attitude to risk. Subdimensions: Tone at the top; Transparency; Lessons learnt; Risk informed decision making; Application of accountabilities and ownership.

3. Undertaking a self-assessment

3.1 Preparing for the self-assessment

It is recommended to begin by assembling the risk related documents that the assessor knows already exist. This may include risk policies, manuals, registers and organisational charts. The assessor should also have access to specialists who can respond to the questions and requests for documentation. It should be agreed what the scope of the assessment is, and whether a separate assessment will be made for certain areas of the organisation.

3.2 Starting the self-assessment

This section will explain how to undertake a self-assessment. Dimension II will be used as an example to demonstrate the steps. The dimensions may be assessed in any order.

i) **Start with the Evidence Checklist.** One can work electronically on the spreadsheet or on a printed version. Only a part of the model is shown in figure 3.

	INITIAL	DEVELOPING	ESTABLISHED
Governance structure	The organisation has in place a fragmented, informal risk governance structure.	The organisation has developed and put in place some elements of a risk governance structure, in accordance with a three lines of defence (TLOD) structure or similar, to oversee the ERM framework.	The organisation has established a risk governance structure (TLOD or similar) to oversee the ERM framework and to ensure that the risks the organisation faces are managed.
Delegation of authority	Accountabilities for managing risk are informal.	Delegation of authority may exist as part of an initiative to implement risk management. Some staff accountabilities for managing risk are formally defined but limited to specific functions of the organisation.	Elements of an organisational risk-based delegation of authority empowers risk committee(s) (e.g. ERM Committee), management and/or other staff. Staff accountabilities for managing risk are generally defined across the organisation.
Function	Certain staff member perform risk management functions without being formally designated this responsibility	The risk management support role may exis as part of another function, such as progran management, performance management or an initiative to implement risk management.	An entity/unit is established within the organisation responsible to ensure that the ERM framework is implemented in the context of programme/project management The organisation operationalises its risk function at all levels (including HQ, field, program, project).
Governance structure			
1 How would you describe the governance structure that oversees the ERM framework?	Fragmented, informal	Some elements in place in accordance with Three Lines of Defence	Established in accordance with Three Lines on Defence
2 Coverage of the risk governance structure that oversees the ERM framework	Limited	Limited	HQ or certain locations
Delegation of authority			
	No	Some staff accountabilities for managing risk are formally defined but limited to specific functions of the organisation	ssued guidelines, policies, procedures & implemented key related processes
4 Does your organisation have an effective risk-based delegation of authority and risk committees' structure with authority for sound and balanced decision making, in compliance with three Lines of Defence (or similar) and ERM framework?	No	Delegation of authority may exist as part of an initiative to implement RM	Elements of a risk-based delegation of authority empower risk committee(s) (or an equivalent senior management committee the has responsibility for risks) management and/or other staff
Function			
5 Does your organisation have an independent RM function, implemented with clear role and responsibility for RM in the organisation?	No independent function exists but some staff members perform risk management roles without formally having responsibility for risk management	The RM support role may exist as part of another function, or an initiative to implement RM	Yes, is implemented in the context of programme/project management at all levels
DOCUMENTATION / EVIDENCE TO VERIFY MATURITY LEVEL			
1 Clearly documented risk roles & responsibilities/accountabilities included in job descriptions, and selection criteria for staff.	No	Partial - responsibilities/accountabilities assigned for RM are reflected in a limited number of job descriptions (e.g. directors/executives) and some policies	Partial - responsibilities/accountabilities assigned for RM are reflected in all risk-relate iob descriptions and most policies as appropriate
2 RM function charter or equivalent established	No		Partial
3 ToRs of Risk Committees established	No	No	May exist as part of another function, or an initiative to implement RM

Figure 3 - Sample assessment

- ii) Start by looking at the questions (see 'start here' on figure 3). Answer the questions and circle the response that corresponds best.
- iii) Use the questions, together with the evidence lines to estimate the best fit for the maturity. It is normal that maturity falls between two levels, in this case, between 2-Developing and 3-Established.
- iv) Assessment by dimension level. Repeat the process above for all dimensions. If the maturity falls between two levels, one may choose to express as the best fit, or report both levels if need be. These levels can be copied through to the Summary Matrix as shown in figure 4. In the example below, the red lines show the assessed maturity, and the highlighted boxes show how the organisation decided to consider their maturity. That is (in this example), dimension I Developing; dimensions II, III and IV Established; dimension V Advanced; dimension VI Developing.

			Reference Matu	Irity Model for Risk Management ir	n the UN System		
Notes:		INITIAL	DEVELOPING	ESTABLISHED	ADVANCED	LEADING	
 Each maturity level adds to the Glossary and checklists comp 	previous level lete the model	Unstructured, managed informally/ inconsistently, ad hoc, reactive.	Structured implementation, basic architecture, some reporting and repeatable management processes.	Defined/documented and standardised processes, good organisational coverage, some evidence of use and embedding. Regular reporting and escalation, information used in operational	Well structured, strong evidence of embedding. Standardised reporting and thresholds for escalation and management action. Information used in strategic decision making.	Fully embedded. Escalation mechanisms well understood and used at all levels of the organisation. Innovative/creative approach delivers continuou improvement and is able to adapt as the organisation changes.	
Dimension Definition	Sub-dimension	LEVEL 1	LEVEL 2	decision making. LEVEL 3	LEVEL 4	LEVEL	
L Enterprise Risk Management (ERM) Framework and Policy: are the collection of policies, procedures and other documents that together	Framework implementation and appetite	The organisation has in place a tragmanted, limited risk management framework.	The organisation has developed an ERM framework, however it has not yet been approved by the appropriate delegated authority.	The organisation has established an ERM framework and defined risk appentie (in risk online) in some and related escalation procedures, which have been approved by the appropriate delegated authority.	The organisation has implemented an ERM transvork including tick apporties, bistrance (or risken) logither with a related repeating the socialision process, which have been approved by the appropriate delegated authority. The ERM transvork is integrated in strategy watting, planning and decision making. Michaniane are implemented to ensure that faceback from stakeholders is actively sought, and that the ERM Immervia is resultive undated.	The organisation, recognised as a leader among pears and risk innovator, has embedded an ERM barnevolk on drisk appetitis, butternora and reliated escatation process, which have been approved by the appropriate delegated authority and may be seen by key stakaholders as a source of competitive advantage.	
describe how the organisation undertakes its risk management.	Framework components and coverage	An implicit risk management framework is in place without being formally codified.	Limited framework components are in place.	The organisation has issued risk guidelines, policies, procedures and has implemented key related processes. A risk scale (e.g. rating) is established for the organisation in the context of its programme/project management.	The ERM framework is tailored to appropriately reflect RBM and decentralised to address the needs of all operational entities (including HD, field, program, posject), Canudar integrated related risk scales (e.g., antigl) or Officent HeardTealAvelle (e.g. enterprise, program, project) or a single appropriate organisation scale is in place.	The ERM Framework is integrated in strategy setting, planning, decision making an enterprise integrated performance management.	
I. Governance and organisational Structure: sets out the internal risk governance structure, the	Governance structure	The organisation has in place a tragmented, informal risk governance structure.	The organisation has developed and put in place some elements of a risk governance structure, in accordance with a three lines of defence (TLOD) structure or similar, to oversee the ERM tramework.	The organisation has established a risk governance structure (TLOD or similar) to oversee the ERM framework and to ensure that the risks the organisation faces are managed.	The organisation has fully integrated its risk governance structure (TLOD or similar) applying it across its operations (including HD, feld, program, project).	The organisation exudes continuous governance improvement and innovation, making it a leader among its peers.	
appropriate delegated authority, roles and responsibilities, and organisational entities to assure the effective	Delegation of authority	Accountabilities for managing risk are informal.	Delegation of authority may exist as part of an initiative to implement risk management. Some staff accountabilises for managing risk are formally defined but limited to specific functions of the organisation.	Elements of an organisational risk-based delegation of authority empowers risk committee(s) (e.g. ERM Committee), management and/o other statt. Statt accountabilities for managing risk are generally defined across the organisation.	An effective risk-based delegation of authority is fully operationalised. Risk committee[s], whose responsibilities include overseeing risk appetite, tolerance or cristria, are implemented in the organization with authority for sound and balanced decision making within their established TOR.	Each level of hierarchy of the organisation has a well defined and comprehensive delegation of authority providing the appropriate accountability for each respective level.	
management of risk.	Function	Certain staff member perform risk management functions without being formally designated this responsibility	The risk management support role may exist as part of another function, such as program management, performance management or an initiative to implement risk management.	An entitylurit is established within the organisation responsible to ensure that the ERM transversitis implemented in the context of programmelproject management. The organisation operationalises its risk function at all levels first with EO. Failt, morram emisert.	A risk management function (e.g. Chiel Risk Officer (CRO)) with the stanutionganisational position for impartially/objectively (from the first LOD), resources and excess to the debased authority, keeps pace with changes to the organisation's task profile, to the external risk landscape and with instustry best practice.	CRO role and responsibility regarding ERM are integrated with strategy setting and dearly anchored with management across the organisation.	
IL Process and Integration: Process ensures that risks and opportunities that may affect the delivery of organisational results are effectively	Process	The organisation undertakes certain elements of the risk management process on an ad hoc basis. There may be inconsistencies in the methodologies applied for risk assessment, monitoring and reporting.	A limited process with a methodology for risk assessment, monitoring and reporting is established but not reliably followed. Limited follow through of mitigation measures by primarily focusing on broad level mitigation plans for critical risks.	The organisation has established a systematic process with a methodology for risk assessment, response, monitoring, escalation and reporting.	The organisation has inclemented a systematic risk management process with clear methodology, which is other inflow based on quality waves. Reachaid and expensions and is equally applicable across its operations (including HQ, Seld, program, project).	The ERM process is continuelly optimised based on pre-defined indicators, making the organization is abder among its poers. Independent neviews/audit of the risk process are undertaken regularly.	
identified, assessed, responded to, communicated and monitored as per the ERM framework. Integration ensures that the interaction / interlinkages with related risk sub-processes or other	Integration with internal controls	There is a lack of integration between risk assessment and internal controls which are primarily managed separately to risks.	There is a lack of integration between risk assessment and internal controls which are primarily managed separately to risks atthough generally key controls include identification of the risks they miligate.	Basic informal links between risks and internal controls are recognised. Controls for certain administrative processes are documented and assigned ownership.	The links are recognised between (i) internal controls and risks; and (ii) control effectiveness and valued risk assessments. Controls for all key processes are comprehensively documented, assessed, assigned contentity and control offseta are established to measure the control effectiveness and subsequent residual risk assessments.	A comprehensive risk-based control framework is in place that recognises and reflects the links of all controls to the risks they milligate which enables identification of control gaps as well as includancies or inefficient controls.	
organisational processes are clearly established.	Integration with planning	There is limited recognition of the need for integration between risk assessment and results based planning.	results based planning process is recognised and communicated, although its application is limited.	Link between results based planning and risk management is establishe by undertaking the risk management process at the sime of planning. A process is incorporate recourse for mitigation planning is an integrated element of the resource planning for the relevant activity.	Total alignment between results based planning and risk management across the organization (inclusting HG, faid, program, project). Miligation planning is reliably managed and the degree of success or failure ed miligation planning are reported during and after the implementation cycle.	There is full integration of risk and opportunity analysis into strategy setting and results based planning and the entire implementation cycle.	
N. Systems and Tools: are the IT components used to record, analyse, integrate and communicate/secution	Platforms, systems and tools	Risks are recorded in various documents, typically at the start of work only.	Manual risk assessment/ response tools in place (e.g. spreadsheet).	Consolidable risk assessment tools (e.g. consolidated risk register), or a basic technology implementation of an ERM system with monitoring and reporting capabilities.	Technology is exploited to improve all aspects of risk management, for example, dynamic risk dashboards, financial risk modelling and forecasting tools.	Advanced risk (and data) modelling and forecasting tools are used to support scenario analysis and strategy setting.	
risk information.	Links to other systems	Weak manual links to other information systems or tools.	Manual link to other information systems or tools.	systems (e.g. planning). Links typically not automated.	Advanced ERM technology platform available across operations (including HQ, field, program, project) along with capturing/integration of data from the other processes which is integrated / linked though semi-automated extract/load operations.	The ERM technology platform is fully integrated with the planning and performance management system with dynamic dashboards for planning, monitoring and analysis.	
V. Risk Capabilities: are the skills, ability, knowledge and capacity that an organisation has to	Competencies	Risk related competencies are perceived to have little value, are based on individuals and vary with their innate skills, knowledge and abilities.	Certain managers value risk related competencies and encourage their teams to develop risk skills, knowledge and abilities through ad hoc or bespoke training programmes.	Risk management is recognised as a management competency and training awareness courses concerning risk management are in place as part of a wider ERM staff development programme.	Servior management signals the importance of proactively developing risk management as a core competency for itself and all staff, and a comprehensive ERM staff development programme is in place.	Staff are motivated to actively continue to perfect their risk skills, knowledge and abilities. The organisation continually improves its comprehensive ERM staff development program and risk processes are once referenced in other organisational competencies and staff development programmes.	
effectively manage risks to delivery of its results.	Capacity	The organisation occasionally re-prioritises its actions and takes on additional risk in pursuit of certain objectives but on limited occasions and without full information or clear analysis.	The organisation regularly re-prioritises its actions and takes on additional risk in pursuit of certain objectives, however, without full information or clear analysis.	The organisation is able to accept some additional risk in pursuit of its objectives in consideration of its overall risk appetite (or criteria).	The organisation is able to identify and take some viable opportunities based on an assessment of whether it can manage residual risk levels within its risk appetite, tokrance (or criteria).	The organisation can identify and exploit viable opportunities in a timely manner and manage residual risk dynamically within its risk appetite, tolerance (or criteria).	
	Reporting	Information on specific/ significant risks may be presented to senior management on an ad hoc basis.	Risk management information and/or risk indicators are presented to serior management at least annually.	Timely, accurate risk management information reports are available to al relevant staff and regularly presented to serior management.	Dynamic risk information reports are accessible to service management and all staff (as appropriate) across the organisation's operations (including HQ, field, program, project), highlighting areas exceeding of risk appetite, tolerance (or criteria), and are refined based on management feedback.	Dynamic risk information dashboards and risk appoints, tolerance (or orberia) are self-improved and proactively used across the organisation's operations (including HQ, field, program, project).	
VI. Risk Culture: is evidenced by the shared values, beliefs, and behaviours of the stall and	Tone at the top	Senior management demonstrates limited commitment to risk management.	Senior management expectations with regards to risk management are expressed reactively in an ad hoc and/or informal manner.	Senior management expectations are clear and they systematically demonstrate commitment to fisk management - risk cubure is aligned whethe overall organisational cubure.	Senior management leads by example in integrating risk management into its strategic activities.	Serior management leads by example in integrating risk management into its daily activities and creates an active, organisation wide awareness of, and dialogue on risks.	
behaviours of the staff and senior management, together with the organisation's demonstrated atsitude to risk.	Transparency	Limited risk information is collected, however, not systematically.	Certain risk information is collected but not communicated systematically.	isk information is systematically collected and formally communicated at in appropriate forum and also in a top-down manner.	Risk information is systematically collected and formally communicated up and down the hierarchy (including HQ, field, program, project) and in certain cases shared externally.	Comprehensive risk information is systematically and transparently collected and shared across the organisation (and enternally as appropriate).	
	Lessons learnt	Information from risk events that materialised or were effectively managed is captured in isolated cases but not analysed.	Information from risk events that materialised or were effectively managed is captured and analysed in isolated cases.	Information from risk management successes and failures is captured and analysed on a regular basis.	Information on risk management successes and failures from the field and HQ is collected systematically and analysed along with reliable data on incidents and risk events with systematic learning of lessons.	The organisation continuously learns from its risk management successes and failures, as well as from experiences outside of the organisation, and actively manages knowledge of these both in all areas of operations.	
	Risk informed decision making	Business decisions are typically taken in isolation of risk factors. The evaluation of risk and reward is undertaken in an ad hoc and intuitive manner.	Business decisions may be taken following a consideration of some risk factors.	The overall attitude to risk is understood and business decisions are made with reference to this based on reliable and finely risk information	The boundaries of acceptable risk are set for all key areas and business decisions are made with reference to these, managers in both the field and HQ proactively consider risk/teward in decision making.	Dynamic risk information is used across the organisation (including HD, field, program, project) to make proactive effective risk decisions.	
	Application of accountabilities and ownership	Some staff assume accountability for risk management themselves outside of any formal process.	Accountabilities assigned for risk management are reflected in a limited number of job descriptions.	Appropriate risk taking is assessed in staff performance management based on defined staff accountabilities.	Staff accountabilities for managing risk are understood (and acted upon) across the organisation; these accountabilities are clearly mapped to performance targets of staff.	Staff at all levels act proactively on their risk accountabilities, seeking out and challenging risk strategies associated with key business risks under their control. Risks across the organisation are overseen optimally and effectively by empowered servior management with strong awareness of inter-velated risk areas.	

Figure 4 - RMM Assessment

v) **Overall Maturity.** Some organisations may wish to express an overall maturity. This can be taken as a range. In this example, the organisation might say that they are between Developing and Established overall.

4. Taking the findings forward

4.1 Target state

The organisation may choose to express its target risk management maturity state at any time. However, most organisations decide after getting a sense of the current maturity. While different organisations have different target states, some organisations have suggested that 'Established' should be a minimum target, however, this remains at the organisation's discretion.

4.2 Developing an implementation roadmap

Depending how distant the target state is from the current assessment, the roadmap may be more, or less complex. The model proposes that the maturity across the dimensions should be somewhat aligned. For example, there is little value to having Leading level 'Systems and Tools', if the Risk Culture remains, for example, Developing or Established. Thus, to turn the model into a roadmap, an organisation may wish to focus on moving each sub-dimension to the right of the RMM, one cell at a time, to align with other levels. The hypothetical organisation in figure 4 may wish to work on strengthening the sub-dimensions that fall short of Established, i.e. some of those within dimensions I, III, IV and VI.

			Reference Mat	urity Model for Risk Management in t	he UN System	
Notes:		INITIAL	DEVELOPING	ESTABLISHED	ADVANCED	LEADING
 Each maturity level adds to the Glossary and checklists compared 	he previous level plete the model	Unstructured, managed informally/ inconsistently, ad hoc, reactive.	Structured implementation, basic architecture, some reporting and repeatable management	Defined/documented and standardised processes, good organisational coverage, some evidence of use and embedding.	Well structured, strong evidence of embedding. Standardised reporting and thresholds for escalation and management action. Information used in	Fully embedded risk management processes; escalation mechanisms well understood and used at all levels of the organisation. Innovative/creative
Dimension Definition	Sub-dimension	LEVEL 1	processes.	Defined/documented and standardised processes, good organisational coverage, some evidence of use and embedding. Regular reporting and escalation, information userational decision making.	strategic decision making.	approach delivers continuous improvement and can adapt as the organisation changes.
I. Enterprise Risk Management (ERM) Framework and Policy: are the collection of policies, procedures and other documents that	Framework implementation and appetite	The organisation has in place a fragmented, limited risk management framework.	The organisation has developed an ERM framework, however it has not yet been approved by the appropriate delegated authority.	The organisation has established an EBM framework and defined risk appetitie (or risk criteria) is now areas and related escalation procedures, which have been approved by the appropriate delegated authority.	The organisation has implemented an ERM framework including risk appetite, tolerance (or costenia) toppleter with a related repeated lescatiator process, which have been approved by the appropriate delegated authority. The ERM framework is integrated in strategy setting, planning and decision making, Mechaniams are implemented to ensure that feedback from tabeholders is actively sought, and that the ERM framework is regularly updated.	The organisation, recognised as a leader among pares and risk innovator, has embedded an EMF framework and risk appetite insteamce and relate escalation process, which have been approved by the appropriate delegated authority and may be seen by key stakeholders as a source of competitive advantage.
together describe how the organisation undertakes its risk management.	Framework components and coverage	An implicit risk management framework is in place without being formally codified.	Limited framework components are in place.	The organisation has issued risk guidelines, policies, procedures and has implemented key related processes. A risk scale (e.g. rating) is established for the organisation in the context of its programme/project management.	The ERM framework is tailored to appropriately reflect RBM and decentralised to address the needs of all operational entities (including HQ, field, programme, project). Canual integrated related risk scales (e.g. rating) for different hierarchical levels (e.g. enterprise, programme, project) or a single appropriate organisation cale is in place.	The ERM Framework is integrated in strategy setting, planning, decision making and enterprise integrated performance management.
II. Governance and organisational Structure: sets out the internal risk	Governance structure	The organisation has in place a fragmented, informal risk governance structure.	The organisation has developed and put in place some elements of a risk governance structure, in accordance with a three lines of defence (TLOD) structure or similar, to oversee the ERM framework.	The organisation has established a risk governance structure (TLOD or similar) to oversee the ERM framework and to ensure that the risks the organisation faces are managed.	The organisation has fully integrated its risk governance structure (TLOD or similar) applying it across its operations (including HQ, field, programme, project).	The organisation exudes continuous governance improvement and innovation, making it a leader among its peers.
governance structure, the appropriate delegated authority, roles and responsibilities, and organisational entities to	Delegation of authority	Accountabilities for managing risk are informal.	Delegation of authority may exist as part of an initiative to implement risk management. Some staff accountabilities for managing risk are formally defined but limited to specific functions of the constructions of the start of the star	Elements of an organisational risk-based delegation of authority empowers risk committee(s) (e.g. ERM Committee), management and/or other staff. Staff accountabilities for managing risk are generally defined across the organisation.	An effective risk-based delegation of authority is fully operationalised. Risk committee(s), whose responsibilities include overseeing risk appetite, tolerance or criteria, are implemented in the organisation with authority for sound and balanced decision making within their established TOR.	Each level of hierarchy of the organisation has a well defined and comprehensive delegation of authority providing the appropriate accountability for each respective level.
assure the effective management of risk.	Function	Certain staff member perform risk management functions without being formally designated this responsibility.	The risk management support role may exist as part of another function, such as programme management, performance management or an initiative to implement risk management.	An entitylunit is established within the organisation responsible to ensure that the ERM framework is implemented in the context of programme/project management. The organisation operationalises its risk function at all levels (including HQ, field, programme, project).	A risk management function (e.g. Chief Risk Officer (CRO)) with staturelorganisational position for impartialligh/decivity (from the first LOD), resources and access to the delegated authority, keeps pace with changes to the organisation's risk profile, to the external risk landscape and with industry best practice.	CRO role and responsibility regarding ERM are integrated with strategy setting and clearly anchored with management across the organisation.
III. Process and Integration: Process ensures that risks and opportunities that may affect the delivery of organisational results are effectively identified	Process	The organisation undertakes certain elements of the risk management process on an ad hoc basis. There may be inconsistencies in the methodologies applied for risk assessment, monitoring and reporting.	A limited process with a methodology for risk assessment, monitoring and reporting is established but not reliably followed. Limited follow through of mitigation measures by primarily focusing on broad level mitigation plans for critical risks.	The organisation has established a systematic process with a methodology for risk assessment, response, monitoring, escalation and reporting.	The organisation has implemented a systematic risk management process with clear methodogo, which is further refined based on quality revews, feedback and experience and is equally applicable across its operations (including HQ, field, programme, project).	The ERM process is continually optimised based on pre-defined indicators, making the criginalisation a leader among its peers. Independent reviews/audit of the risk process are undertaken regularly.
effectively identified, assessed, responded to, communicated and monitored as per the ERM framework. <i>Integration</i> ensures that the interaction / interlinkages	Integration with internal controls	There is a lack of integration between risk assessment and internal controls which are primarily managed separately to risks.	There is a lack of integration between risk assessment and internal controls which are primarily managed separately to risks although generally key controls include identification of the risks they mitigate.	Basic informal links between risks and internal controls are recognised. Controls for cartina administrative processes are documented and assigned ownership.	The firsk are recognised batween (i) informal controls and risks; and (ii) control effectiveness and rolleder risk assessments. Controls for all key processes are comprehensively documented, assessed, assigned ownership and control criteria are estabilished to measure the control effectiveness and subsequent residual risk assessments.	A comprehensive risk-based control framework is in place that recognises and reflects the inits of all cortrol to the risks they milliple which enables identification of control gaps as well as redundancies or inefficient controls.
with related risk sub- processes or other organisational processes are clearly established.	Integration with planning	There is limited recognition of the need for integration between risk assessment and results based planning.	The importance of integration of risk assessments with results based planning process is recognised and communicated, although its application is limited.	Link between results based planning and risk management is established by undertaking the risk management process at the time of planning. A process to incorporate resources for mitigation planning is an integrated element of the resource planning for the relevant activity.	Total alignment between results based planning and risk management across the organisation (including HQ, field, programme, project). Mitigation planning is reliably managed and the degree of success or failure of mitigation planning are reported during and after the implementation cycle.	There is full integration of risk and opportunity analysis into strategy setting and results based planning and the entire implementation cycle.
IV. Systems and Tools: are the IT components used to record, analyse, integrate and	Platforms, systems and tools	Risks are recorded in various documents, typically at the start of work only.	Manual risk assessment/ response tools in place (e.g. spreadsheet).	Consolidable risk assessment tools (e.g. consolidated risk register), or a basic technology implementation of an ERM system with monitoring and reporting capabilities.	Technology is exploited to improve all aspects of risk management, for example, dynamic risk dashboards, financial risk modelling and forecasting tools.	Advanced risk (and data) modelling and forecasting tools are used to support scenario analysis and strategy setting.
communicate/report on risk information.	Links to other systems	Weak manual links to other information systems or tools.	Manual link to other information systems or tools.	Links between risk management systems established with other key systems (e.g. planning). Links typically not automated.	Advanced ERM technology platform available across operations (including HQ, field, programme, project) along with capturing/integration of data from the other processes which is integrated / linked though semi-automated extract/load operations.	The ERM technology platform is fully integrated with the planning and performance management system with dynamic dashboards for planning, monitoring and analysis.
V. Risk Capabilities: are the skills, ability, knowledge and capacity that an organisation must effectively manage risks	Competencies	Risk related competencies are perceived to have little value, are based on individuals and vary with their innate skills, knowledge and abilities.	Certain managers value risk related competencies and encourage their teams to develop risk skills, knowledge and abilities through ad hoc or bespoke training programmes.	Risk management is recognised as a management competency and training/awareness courses concerning risk management are in place as part of a wider ERM staff development programme.	Senior management signals the importance of proactively developing risk management as a core competency for itself and all staff, and a comprehensive ERM staff development programme is in place.	Staff are motivated to actively continue to perfect their risk skills, knowledge and abilities. The organisation continually improves its comprehensive ERM staff development programme and risk processes are cross referenced in other organisational competencies and staff development programmes.
to deliver its results.	Capacity	The organisation occasionally re-prioritises its actions and takes on additional risk in pursuit of certain objectives but on limited occasions and without full information or clear analysis.	The organisation regularly re-prioritises its actions and takes on additional risk in pursuit of certain objectives, however, without full information or clear analysis.	The organisation is able to accept some additional risk in pursuit of its objectives in consideration of its overall risk appetite (or criteria).	The organisation is able to identify and take some viable opportunities based on an assessment of whether it can manage residual risk levels within its risk appetite, tolerance (or criteria).	The organisation can identify and exploit viable opportunities in a timely manner and manage residual risk dynamically within its risk appetite, tolerance (or criteria).
	Reporting	Information on specific/ significant risks may be presented to senior management on an ad hoc basis.	Risk management information and/or risk indicators are presented to senior management at least annually.	Timely, accurate risk management information reports are available to all relevant staff and regularly presented to senior management.	Dynamic risk information reports are accessible to senior management and all staff (as appropriate) across the organisation's operations (including HO, field, programme, project), highlighting areas excessioning of risk appetite, tolerance (or criteria), and are refined based on management feedback.	Dynamic risk information dashboards and risk appetite, tolerance (or criteria) are self-improved and proactively used across the organisation's operations (including HQ, field, programme, project).
VI. Risk Culture: is evidenced by the shared values, beliefs, and behaviours of the staff and	Tone at the top	Senior management demonstrates limited commitment to risk management.	Senior management expectations with regards to risk management are expressed reactively in an ad hoc and/or informal manner.	Senior management expectations are clear and they systematically demonstrate commitment to risk management - risk culture is aligned with the overall organisational culture.	Senior management leads by example in integrating risk management into its strategic activities.	Senior management leads by example in integrating risk management into its dail activities and creates an active, organisation wide awareness of, and dialogue on risks.
senior management, together with the organisation's	Transparency	Limited risk information is collected, however, not systematically.	Certain risk information is collected but not communicated systematically.	Risk information is systematically collected and formally communicated at an appropriate forum and also in a top-down manner.	Risk information is systematically collected and formally communicated up and down the hierarchy (including HQ, field, programme, project) and in certain cases shared externally.	Comprehensive risk information is systematically and transparently collected and shared across the organisation (and externally as appropriate).
demonstrated attitude to risk.	Lessons learnt	Information from risk events that materialised or were effectively managed is captured in isolated cases but not analysed.	Information from risk events that materialised or were effectively managed is captured and analysed in isolated cases.	Information from risk management successes and failures is captured and analysed on a regular basis.	Information on risk management successes and failures from the field and HQ is collected systematically and analysed along with reliable data on incidents and risk events with systematic learning of lessons.	The organisation continuously learns from its risk management successes and failures, as well as from experiences outside of the organisation, and actively manages knowledge of these both in all areas of operations.
	Risk informed decision making	Business decisions are typically taken in isolation of risk factors. The evaluation of risk and reward is undertaken in an ad hoc and intuitive manner.	Business decisions may be taken following a consideration of some risk factors.	The overall attitude to risk is understood and business decisions are made with reference to this based on reliable and timely risk information.	The boundaries of acceptable risk are set for all key areas and business decisions are made with reference to these; managers in both the field and HQ proactively consider risk/reward in decision making.	Dynamic risk information is used across the organisation (including HQ, field, programme, project) to make proactive effective risk decisions.
	Application of accountabilities and ownership	Some staff assume accountability for risk management themselves outside of any formal process.	Accountabilities assigned for risk management are reflected in a limited number of job descriptions.	Appropriate risk taking is assessed in staff performance management based on defined staff accountabilities.	Staff accountabilities for managing risk are understood (and acted upon) across the organisation; these accountabilities are clearly mapped to performance targets of staff.	Staff at all levels act proactively on their risk accountabilities, seeking out and challenging risk strategies associated with key business risks under their control. Risks across the organisation are overseen optimally and effectively by empowered senior management with strong awareness of inter-related risk areas

Reference Maturity Model - RM

		Evidence checklist	S		
I. ERM Framework and Policy					
	INITIAL	DEVELOPING	ESTABLISHED	ADVANCED	LEADING
Framework implementation and appetite	The organisation has in place a fragmented, limited risk management framework.	The organisation has developed an ERM framework, however it has not yet been approved by the appropriate delegated authority.	The organisation has established an ERM framework and defined risk appetite (or risk criteria) in some areas and related escalation procedures, which have been approved by the appropriate delegated authority.	The organisation has implemented an ERM framework including risk appetite, tolerance (or criteria) together with a related repeatable escalation process, which have been approved by the appropriate delegated authority. The ERM framework is integrated in strategy setting, planning and decision making. Mechanisms are implemented to ensure that feedback from stakeholders is actively sought, and that the ERM framework is regularly updated.	authority and may be seen by key stakeholders as a source of competitive advantage.
Framework components and coverage	An implicit risk management framework is in place without being formally codified.	Limited framework components are in place.	The organisation has issued risk guidelines, policies, procedures and has implemented key related processes. A risk scale (e.g. rating) is established for the organisation in the context of its programme/project management.	The ERM framework is tailored to appropriately reflect RBM and decentralised to address the needs of all operational entities (including HQ, field, programme, project). Granular integrated related risk scales (e.g. rating) for different hierarchical levels (e.g. enterprise, programme, project) or a single appropriate organisation scale is in place.	The ERM Framework is integrated in strategy setting, planning, decision making and enterprise integrated performance management.
Framework implementation and appetite					
1 How would you describe your overarching ERM Framework?	Fragmented - some elements exist but not cohesive	Developed, but not approved or approved but not comprehensive for the entire organization	Comprehensive and approved by the appropriate delegated authority	Integrated into strategy setting, planning and decision making	Seen by key stakeholders as a source of competitive advantage
2 Does your organisation have a risk appetite (or criteria) escalation process?	No	Limited / intuitive	Yes, describes existing risk-taking escalation practices	Yes, updated regularly and guides work planning	Yes, guides strategy planning, implementation and reporting
3 Are mechanisms implemented to ensure that feedback from stakeholders is actively sought, and that the ERM framework is regularly updated?	No	Limited / informal	Ad hoc feedback and review	Systematic feedback and annual review	Systematic feedback and review on an ongoing basis including with key external stakeholders
Framework components and coverage		1			
4 How would you describe your organisation's risk guidelines, policies, procedures and -processes?	Very limited - perhaps components exist at a project or office level	Under development, but limited in scope and coverage	Issued guidelines, policies, procedures & implemented key related processes	Tailored, addresses the needs of all operational entities	Integral to organisational processes
5 How would you describe the risk scales (risk ratings for likelihood and impact)?	Simple scale with limited substantive complexity		Risk scale (e.g. rating) is established for programme/project management	Multiple entities have inter-related - or the same risk rating scale, with consistent qualitative dimensions	Multiple entities have inter-related - or the same risk rating scale, with some quantitative dimensions
6 How would you describe the ERM framework's integration with other organisational processes and coverage?	Not integrated or existent.	Limited	Risk management process integrated at time of planning and considered with internal controls	The ERM framework is fully integrated in planning and partially integrated with internal controls, strategy setting and decision making	The ERM Framework drives strategy setting, planning, decision making, internal controls and enterprise performance management
DOCUMENTATION / EVIDENCE TO VERIFY MATURITY LEVEL					
1 Overarching ERM framework/policy documentation 2 RM operating procedures / guidelines	Fragmented, limited No	Not approved Under development	HQ plus maybe other entities. Yes but of limited sophistication and detail	Over 75% organisation coverage Yes	Organisation 100% covered Yes
3 Risk appetite (or criteria) Statement and related escalation procedures	No	Under development	Yes in certain limited areas	Yes	Yes
4 Accountability framework documentation	No	Under development	Yes but not comprehensive or fully linked to ERM	Yes	Yes
5 Internal control framework documentation	No	No	Yes but not comprehensive or fully linked to ERM	Yes	Yes
6 Planning and performance management risk-based policies and procedures	No	No	Partial	Partial	Yes

. Governance and Organisational Structure					
	INITIAL	DEVELOPING	ESTABLISHED	ADVANCED	LEADING
Governance structure	The organisation has in place a fragmented, informal risk governance structure.	The organisation has developed and put in place some elements of a risk governance structure, in accordance with a three lines of defence (TLOD) structure or similar, to oversee the ERM framework.	The organisation has established a risk governance structure (TLOD or similar) to oversee the ERM framework and to ensure that the risks the organisation faces are managed.	The organisation has fully integrated its risk governance structure (TLOD or similar) applying it across its operations (including HQ, field, programme, project).	The organisation exudes continuous governance improvement and innovation, making it a leader among its peers.
Delegation of authority	Accountabilities for managing risk are informal.	Delegation of authority may exist as part of an initiative to implement risk management. Some staff accountabilities for managing risk are formally defined but limited to specific functions of the organisation.	Elements of an organisational risk-based delegation of authority empowers risk committee) (e.g. ERM Committee), management and/or other staff. Staff accountabilities for managing risk are generally defined across the organisation.	An effective risk-based delegation of authority is fully operationalised. Risk committee(s), whose responsibilities include overseeing risk appetite, tolerance or criteria, are implemented in the organisation with authority for sound and balanced decision making within their established TOR.	Each level of hierarchy of the organisation has a well defined and comprehensive delegation of authority providing the appropriate accountability for each respective level.
Function	Certain staff member perform risk management functions without being formally designated this responsibility.	The risk management support role may exist as part of another function, such as programme management, performance management or an initiative to implement risk management.	An entity/unit is established within the organisation responsible to ensure that the ERM framework is implemented in the context of programme/project management. The organisation operationalises its risk function at all levels (including HQ, field, program, project).	A risk management function (e.g. Chief Risk Officier (CRO)) with stature/organisational position for impartiality/objectivity (from the first LOD), resources and access to the delegated authority, keeps pace with changes to the organisation's risk profile, to the external risk landscape and with industry best practice.	CRO role and responsibility regarding ER are integrated with strategy setting and clearly anchored with management across the organisation.
Governance structure					
1 How would you describe the governance structure that oversees the ERM framework?	Fragmented, informal	Some elements in place in accordance with Three Lines of Defence	Established in accordance with Three Lines of Defence	Fully integrated risk governance structure applied across its operations	Continuous governance improvement and innovation, making it a leader among its peers
2 Coverage of the risk governance structure that oversees the ERM framework	Limited	Limited	HQ or certain locations	Applied across operations (including HQ, field, programme, project)	
Delegation of authority					
3 Does your organisation have a governance structure assigning ERM Framework roles and responsibilities to governing body (e.g. board, management), management and other personnel?	No	Some staff accountabilities for managing risk are formally defined but limited to specific functions of the organisation		Yes - An effective risk-based delegation of authority is fully operationalised	
4 Does your organisation have an effective risk-based delegation of authority and risk committees' structure with authority for sound and balanced decision making, in compliance with three Lines of Defence (or similar) and ERM framework?	No	Delegation of authority may exist as part of an initiative to implement RM	Elements of a risk-based delegation of authority empower risk committee(s) (or an equivalent senior management committee that has responsibility for risks) management and/or other staff	Risk committee(s), whose responsibilities include overseeing risk appetite, tolerance or criteria, are implemented with authority within their ToRs	Independent risk committee(s) established. Er level of hierarchy of the organisation has a we defined and comprehensive delegation of authority providing the appropriate accountabi for each respective level
Function					
5 Does your organisation have an independent RM function, implemented with clear role and responsibility for RM in the organisation?	No independent function exists but some staff members perform risk management roles without formally having responsibility for risk management	The RM support role may exist as part of another function, or an initiative to implement RM	Yes, is implemented in the context of programme/project management at all levels	Yes, a Chief Risk Officer (CRO) (or equivalent) has appropriate stature/organisational position, resources, access to the delegated authority, keeps pace with changes and best practice	Yes, CRO role is integrated with strategy setti and clearly anchored with management acros the organisation
DOCUMENTATION / EVIDENCE TO VERIFY MATURITY LEVEL					
 Clearly documented risk roles & responsibilities/accountabilities included in job descriptions, and selection criteria for staff. 	No	Partial - responsibilities/accountabilities assigned for RM are reflected in a limited number of job descriptions (e.g. directors/executives) and some policies	Partial - responsibilities/accountabilities assigned for RM are reflected in all risk-related job descriptions and most policies as appropriate	Yes -responsibilities/accountabilities assigned for RM are reflected in all job descriptions and all policies as appropriate	Yes -responsibilities/accountabilities assigned for RM are reflected in all job descriptions and policies as appropriate
2 RM function charter or equivalent established	No	No	Partial	Yes	Yes
3 ToRs of Risk Committees established	No	No	May exist as part of another function, or an initiative to implement RM	Yes	Yes and the committee involves some independent members

III. Process and Integration					
	INITIAL	DEVELOPING	ESTABLISHED	ADVANCED	LEADING
Process	The organisation undertakes certain elements of the risk management process on an ad hoc basis. There may be inconsistencies in the methodologies applied for risk assessment, monitoring and reporting.	A limited process with a methodology for risk assessment, monitoring and reporting is established but not reliably followed. Limited follow through of mitigation measures by primarily focusing on broad level mitigation plans for critical risks.	systematic process with a methodology for	The organisation has implemented a systematic risk management process with clear methodology, which is further refined based on quality reviews, feedback and experience and is equally applicable across its operations (including HQ, field, programme, project).	The ERM process is continually optimised based on pre-defined indicators, making the organisation a leader among its peers. Independent reviews/audit of the risk process are undertaken regularly.
Integration with internal controls	There is a lack of integration between risk assessment and internal controls which are primarily managed separately to risks.	There is a lack of integration between risk assessment and internal controls which are primarily managed separately to risks although generally key controls include identification of the risks they mitigate.	Basic informal links between risks and internal controls are recognised. Controls for certain administrative processes are documented and assigned ownership.	The links are recognised between (i) internal controls and risks; and (ii) control effectiveness and related risk assessments. Controls for all key processes are comprehensively documented, assessed, assigned ownership and control criteria are established to measure the control effectiveness and subsequent residual risk assessments.	A comprehensive risk-based control framework is in place that recognises and reflects the links of all controls to the risks they mitigate which enables identification of control gaps as well as redundancies or inefficient controls.
Integration with planning	There is limited recognition of the need for integration between risk assessment and results based planning.	The importance of integration of risk assessments with results based planning process is recognised and communicated, although its application is limited.	Link between results based planning and risk management is established by undertaking the risk management process at the time of planning. A process to incorporate resources for mitigation planning is an integrated element of the resource planning for the relevant activity.	Total alignment between results based planning and risk management across the organisation (including HQ, field, programme, project). Mitigation planning is reliably managed and the degree of success or failure of mitigation planning are reported during and after the implementation cycle.	There is full integration of risk and opportunity analysis into strategy setting and results based planning and the entire implementation cycle.
Process					
1 Does the organisation identify and assess risks in accordance with documented policies, processes and a defined risk scale(s)?	Inconsistently	Limited process / coverage not systematic	Yes, systematic process with a methodology for risk assessment, response, monitoring, escalation and reporting	Yes, refined based on quality review, feedback and experience	Yes, tailored through regular reviews / audits for continuous improvement
2 At which levels/areas are risks systematically identified and registered?	Potentially project or certain high risk areas	HQ and potentially project	HQ or certain locations/functions	Applied across operations (including HQ, field, programme, project)	
3 How are risk responses addressed?	Identified ad hoc, potentially for projects	Limited follow through, some critical risks may have mitigation plans	Systematically	With a view to optimizing - not eliminating risk	Successes and failures monitored and learned from
4 At what level is risk ownership institutionalised and understood by staff and senior management?	Potentially project or certain high risk areas	HQ and potentially project	HQ or certain locations/functions	Applied across operations (including HQ, field, programme, project)	
5 Does the organisation and risk owners regularly monitor identified risks for changes (when event occurs or when risks are escalated)?	No	No	For changes, but after risk occurrence rare	Yes, including risk event evaluation	
6 Does the organisation's RM process identify potential overlaps or duplications in risk responses?	No	Ad hoc	Not systematically	Yes	
7 Does the organisation evaluate risk events when they occur to better understand their causal effect?	No	No	Not systematically	Yes, with feedback for critical events	Yes, systematically to improve performance
8 Does the organisation regularly evaluate and iteratively implement changes to improve its ERM processes?	No	No	Ad hoc	Yes, in line with emerging best practice	Yes, leader among peers
Integration with internal controls					
9 Are internal controls identified and recorded, and assigned ownership?	No	Some documented internal controls	For certain administrative processes	For key organisational processes	For all organisational processes
10 What is the level of integration between RM and internal controls management?	None formally although some overlap exists by chance	Limited	Basic informal links between risks and internal controls are recognised	The links are recognised between (i) internal controls and risks; and (ii) control effectiveness and related risk assessments	Continually improving through monitoring and feedback
11 Are control criteria established to measure the control effectiveness and subsequent residual risk assessments?	No	No	Under development	Yes, with feedback for critical events	Yes, systematically to improve performance
12 Does the organisation address control gaps, control redundancy and control effectiveness and optimization?	No	No	No	Under development	Yes
13 Risk information is presented in combination with associated processes (moved from capabilities)	No	No	Risk information available/presented together with planning information	Data analytics enables risk information to be reported / accessed together with some of the following: Business Continuity, Internal Controls, Security, Information Security	Data analytics enables risk information to be reported / accessed together with all risk sub- frameworks
14 Is risk and control information used to develop evidence-based statement of internal control (SIC)? (moved from capabilities)	No	No	May be manual	Semi-automated	Automatic report generation for SIC

01/10/2019

Integration with planning	_				
15 How would you describe degree of integration between RM and results based planning?	Limited	Importance is recognised and communicated, although its application remains limited	Established by undertaking the RM process at the time of planning	Alignment across most of the organisation (including HQ, field, programme, project)	Full integration across organisation of risk and opportunity analysis into strategy setting and results based planning and the entire implementation cycle
16 Does the organisation link risks with its results framework?	Informally	Key risks	To one level of strategic objective	To two levels of strategic objective	Fully integrated with all levels of strategic objectives
17 What link exists between risk mitigation planning and organisational planning	None	Limited	Resources for mitigation planning are part of the resource planning for the relevant activity	Mitigation planning is reliable, successes or failures are reported and feedback into planning process	The linked between mitigation planning and organisational planning is optimised
DOCUMENTATION / EVIDENCE TO VERIFY MATURITY LEVEL					
1 Process maps for RM	No	Top level (level 0) maps	Second level (level 1) maps	Fully mapped	
2 Risks included in annual planning documentation	No	Possible	Yes at a high level	Yes and in detail	
3 Project/programme level risk identification checklist	No	No	Yes		
4 Process maps for processes that include internal controls	No	No	For certain administrative processes	For key organisational processes	For all organisational processes
5 List of controls links to risks	No	No	For certain administrative processes	For key organisational processes	For all organisational processes
6 Risks included in multi-annual strategic planning documentation	No	No	Possible	Yes	Yes and mitigation actions clearly reflected in the plan and linked to the risks

LEADING

IV. Systems and Tools					
	INITIAL	DEVELOPING	ESTABLISHED	ADVANCED	LEADING
Platforms, systems and tools	Risks are recorded in various documents, typically at the start of work only.	Manual risk assessment/ response tools in place (e.g. spreadsheet).	Consolidable risk assessment tools (e.g. consolidated risk register), or a basic technology implementation of an ERM system with monitoring and reporting capabilities.	Technology is exploited to improve all aspects of risk management, for example, dynamic risk dashboards, financial risk modelling and forecasting tools.	Advanced risk (and data) modelling and forecasting tools are used to support scenario analysis and strategy setting.
Links to other systems	Weak manual links to other information systems or tools.	Manual link to other information systems or tools.	Links between risk management systems established with other key systems (e.g. planning). Links typically not automated.	Advanced ERM technology platform available across operations (including HQ, field, programme, project) along with capturing/integration of data from the other processes which is integrated / linked though semi-automated extract/load operations.	The ERM technology platform is fully integrated with the planning and performance management system with dynamic dashboards for planning, monitoring and analysis.
Platforms, systems and tools					
1 What sort of tool or system does your organisation use to enable the RM process?	Various spreadsheets or documents	Unified, or coordinated spreadsheets or documents	Software system with functionality such as: support for multiple entities; consolidation; risk assessments; risk response; monitoring and reporting capabilities	Advanced functionality ERM system, with some modelling and forecasting tools used to support scenario analysis and strategy setting	System provides leading functionality, such as real-time information reports/multi-layer dashboard indicating red flags highlighting areas outside the risk appetite and risk tolerance
Links to other systems					
2 How would you describe the level of integration with the internal control process?	None	Under development	Continuing mitigation actions are typically recorded as controls and linked to risks	Controls are predominantly structured in a control framework and linked to some risks	Fully developed control framework available in the system to link to risks
3 How would you describe the level of integration between the ERM system and other processes which is integrated / linked though semi-automated extract/load operations.	None or very limited manual links	Regular but manual link to other information systems or tools	Integration with performance / planning system may be through a third system (e.g. Business Intelligence) or through manual load (e.g. list of organisational objectives loaded into ERM)	Advanced functionality ERM system including inter-operability with other risk sub-frameworks (e.g. Security, Cyber, Business continuity) and incident reports though semi-automated extract/load operations	The ERM technology platform is fully integrated with the planning and performance management system and incident reporting systems with dynamic dashboards for planning, monitoring and analysis
4 Does the system offer integration with the planning process (including resource planning for mitigation actions)?	No	Weak	Partially integrated	Yes	Yes, seamless two-way data integration
DOCUMENTATION / EVIDENCE TO VERIFY MATURITY LEVEL					
1 Tool or system has risk registers typically at the levels	Project / may be static	Also at programme / unit and 'top 10' organisational risks	Also at Field / external office	Quality assured risk registers with regular internal review	Transparent and truly owned risk registers available to stakeholders
2 Availability of advanced stage technological platform with dynamic risk dashboards, financial risk modelling and forecasting tools.	No	No	Under development	Yes, for some parts of the organisation	Yes, organisation-wide

v.	Risk Capabilities					
		INITIAL	DEVELOPING	ESTABLISHED	ADVANCED	
	Competencies	Risk related competencies are perceived to have little value, are based on individuals and vary with their innate skills, knowledge and abilities.	Certain managers value risk related competencies and encourage their teams to develop risk skills, knowledge and abilities through ad hoc or bespoke training programmes.	Risk management is recognised as a management competency and training/averness courses concerning risk management are in place as part of a wider ERM staff development programme.	Senior management signals the importance of proactively developing risk management as a core competency for itself and all staff, and a comprehensive ERM staff development programme is in place.	Staff are motivated to actively continue to perfect their risk skills, knowledge and abilities. The organisation continually improves its comprehensive ERM staff development programme and risk processes are cross referenced in other organisational competencies and staff development programmes.
	Capacity	The organisation occasionally re-prioritises its actions and takes on additional risk in pursuit of certain objectives but on limited occasions and without full information or clear analysis.	The organisation regularly re-prioritises its actions and takes on additional risk in pursuit of certain objectives, however, without full information or clear analysis.	The organisation is able to accept some additional risk in pursuit of its objectives in consideration of its overall risk appetite (or criteria).	The organisation is able to identify and take some viable opportunities based on an assessment of whether it can manage residual risk levels within its risk appetite, tolerance (or criteria).	The organisation can identify and exploit viable opportunities in a timely manner and manage residual risk dynamically within its risk appetite, tolerance (or criteria).
	Reporting	Information on specific/ significant risks may be presented to senior management on an ad hoc basis.	Risk management information and/or risk indicators are presented to senior management at least annually.	Timely, accurate risk management information reports are available to all relevant staff and regularly presented to senior management.	Dynamic risk information reports are accessible to senior management and all staff (as appropriate) across the organisation's operations (including HQ, field, programme, project), highlighting areas exceeding of risk appetite, tolerance (or criteria), and are refined based on management feedback.	Dynamic risk information dashboards and risk appetite, tolerance (or criteria) are self- improved and proactively used across the organisation's operations (including HQ, field, programme, project).
1	Do staff have the skills they need to manage risks and exploit opportunities	Possibly through past experiences	In certain cases	increasingly, particularly in HQ	Yes in some areas, still some gaps	Yes, organisation wide
	to objectives under their purview?					
	Do staff undertake continuous development of their RM skills?	No Possibly, through past experiences	Selected staff with specific risk management responsibilities develop their skills through their own initiative Ad hoc / developing existing staff	Yes across the organisation as opportunities are presented Yes, may be various qualifications	Yes - across the organisation as opportunities are presented and certain areas are motivated to proactively continually develop their risk skills Yes - encouraged and consistent	Yes - staff across the organisation proactively seek training opportunities to keep them "leading" Yes - required for all managerial and other
	'				5	relevant positions
		No	Certain cases	Management competency	Core Competency	Yes, cross referenced in other organisational competencies
	development programme?	NO	Ad hoc or bespoke risk training	Yes - often classroom training as required	Yes - may be e-Learning or blended training programme	Yes - risk training is embedded in various other training courses as well as risk training
	Capacity Does the organisation use accurate and timely risk information to support its decision to take on additional risk in pursuit of its objectives?	No - although on occasion it re-prioritizes actions or takes on additional risks but without using accurate and timely risk information	Under development	Yes - calculated risk taking is evident in some areas in line with published risk appetite	Yes - calculated risk taking is evident in most areas in line with published risk appetite	Yes, dynamically interacting with risk appetite (o criteria)
7	Is the organisation able to exploit opportunities in a timely manner to maximise their benefit?	No	Intuitively	Partially	Yes for key opportunities	Yes for all levels of opportunities
	Reporting					
8	What risk information is available or presented to senior management?	Basic risk information on demand for key risks	RM information and/or risk indicators for certain areas or processes	Timely and accurate information on key risks, responses including controls	Dynamic risk information accessible to senior management and all staff (as appropriate) across the organisation's operations (including HQ, field, programme, project)	Dynamic risk information dashboards and risk appetite, tolerance (or criteria) self-improved and proactively used across the organisation's operations (including HQ, field, programme, project)
9	Do risk reports highlight areas exceeding of risk appetite, tolerance (or criteria)	No	No	Certain cases	Yes, refined based on management feedback	Yes, learning and refinement based on external stakeholder feedback
10	Capability to provide positive assurance across the organisation's controls in support of RM	Νο	No	Under development	Data analytics used to confirm key control's effectiveness for a limited number of controls	Advanced use of data analytics recognise contro breaches, improve control effectiveness and reduce risk
	DOCUMENTATION / EVIDENCE TO VERIFY MATURITY LEVEL					
	RM training materials	Project level	Also at programme / unit level	eLearning courses	Developed in conjunction with other subject area learning materials	improving
	Completion rates of RM courses Timely, accurate RM information reports produced	Not recorded No	< 10% all staff Occasionally	40% all staff Quarterly for risk committee and/or senior	All staff Quarterly or more, for all staff	All staff with refresher programme Quarterly or more, for all stakeholders or public
		No	May be studying or recognized as a benefit	management Yes, may be various qualifications	Yes - encouraged and consistent	Yes - required
5	RM reflected in the selection criteria and TORs of staff	No	No	For RM staff	For certain areas, e.g. management	For all staff as relevant
	managed within acceptable levels	No	No	Partially	Yes	Yes
7	Statement of Internal Control supported by evidence based risk / control reporting	No	No	May be manual	Semi-automated	Automatic report generation for SIC
8	Documented examples of opportunities exploited in a timely manner based on sound analysis with regards to acceptable risk tolerance levels	No	No	No	Partially	Yes
9	Reporting for highlighting areas outside of risk tolerances	No	No	No	Reports	Reports and dynamic dashboards

/I. Risk Culture					
	INITIAL	DEVELOPING	ESTABLISHED	ADVANCED	LEADING
Tone at the top	Senior management demonstrates limited commitment to risk management.	Senior management expectations with regards to risk management are expressed reactively in an ad hoc and/or informal manner.	Senior management expectations are clear and they systematically demonstrate commitment to risk management - risk culture is aligned with the overall organisational culture.	Senior management leads by example in integrating risk management into its strategic activities.	Senior management leads by example in integrating risk management into its daily activities and creates an active, organisat wide awareness of, and dialogue on risks
Transparency	Limited risk information is collected, however, not systematically.	Certain risk information is collected but not communicated systematically.	Risk information is systematically collected and formally communicated at an appropriate forum and also in a top-down manner.	Risk information is systematically collected and formally communicated up and down the hierarchy (including HQ, field, programme, project) and in certain cases shared externally.	Comprehensive risk information is systematically and transparently collecte and shared across the organisation (and externally as appropriate).
Lessons learnt	Information from risk events that materialised or were effectively managed is captured in isolated cases but not analysed.	Information from risk events that materialised or were effectively managed is captured and analysed in isolated cases.	Information from risk management successes and failures is captured and analysed on a regular basis.	Information on risk management successes and failures from the field and HQ is collected systematically and analysed along with reliable data on incidents and risk events with systematic learning of lessons.	The organisation continuously learns fror its risk management successes and failu as well as from experiences outside of th organisation, and actively manages knowledge of these both in all areas of operations.
Risk informed decision making	Business decisions are typically taken in isolation of risk factors. The evaluation of risk and reward is undertaken in an ad hoc and intuitive manner.	Business decisions may be taken following a consideration of some risk factors.	The overall attitude to risk is understood and business decisions are made with reference to this based on reliable and timely risk information.	The boundaries of acceptable risk are set for all key areas and business decisions are made with reference to these; managers in both the field and HQ proactively consider risk/reward in decision making.	Dynamic risk information is used across organisation (including HQ, field, programme, project) to make proactive effective risk decisions.
Application of accountabilities and ownership	Some staff assume accountability for risk management themselves outside of any formal process.	Accountabilities assigned for risk management are reflected in a limited number of job descriptions.	Appropriate risk taking is assessed in staff performance management based on defined staff accountabilities.	Staff accountabilities for managing risk are understood (and acted upon) across the organisation; these accountabilities are clearly mapped to performance targets of staff.	Staff at all levels act proactively on their accountabilities, seeking out and challeng risk strategies associated with key busine risks under their control. Risks across th organisation are overseen optimally and effectively by empowered senior management with strong awareness of in related risk areas.
Tone at the top					
1 Are risks to the organisation communicated by senior management?	Limited; reactively	Ad hoc, informally; reactively	Proactively including some information on risk that have occurred	Proactively, including information on risk that have occurred and near misses	As appropriate with feedback and analysis fr external stakeholders
2 How would you describe senior management's expectations regarding RM?	Expectations about RM are not clearly set or communicated	Senior management makes occasional reference to RM, but it lacks sufficient consistency and sincerity	Senior management systematically demonstrates commitment to RM	Senior management leads by example and ensures RM is a part of each relevant process	Senior management creates an active, organisation-wide dialogue on risks
3 Is the risk culture of the organisation aligned with positive aspects of organisational culture? e.g. high integrity; performance driven; strong accountability and ownership; agility and adaptivity; and innovativeness.	Generally not	Partially	Yes, mostly	Yes, totally	Yes, with risk culture influencing organisatio culture
4 Is risk a standing agenda item on senior management meetings?	No	No	Inconsistently	Yes, with some limitations / exceptions	Yes, with sincerity
Transparency					
5 Do staff have the confidence to identify and frankly discuss risks?	Potentially project or certain high risk areas	HQ and potentially project	HQ or certain locations / functions	Across operations (including HQ, field, programme, project)	Externally with third line of defence or goven bodies
6 Do staff have the confidence to escalate risks to senior management?	Potentially project or certain high risk areas	HQ and potentially project	HQ or certain locations / functions	Across operations (including HQ, field, programme, project)	
7 Is risk information (i.e. risk events and incidents, risk responses, underlying data relevant to the risks etc.) collected?	Limited, not systematically	Some collected but not communicated systematically	Yes, systematically collected and formally communicated	Yes, systematically collected and formally communicated up and down the hierarchy	Yes, systematically and transparently collect and shared
8 Does senior management share appropriate RM information in a transparent manner?	Not systematically	Partially - may be a tendency to avoid recognising or communicating risks	Generally only within the organisation	Shared across the organisation and certain cases shared externally	Greater focus on sharing externally as appropriate

VI. Risk Culture (continued)					
	INITIAL	DEVELOPING	ESTABLISHED	ADVANCED	LEADING
Lessons learnt					
9 When risks materialised or were effectively managed, is the information effectively captured and shared?	In isolated cases but with no value adding analysis	In isolated cases	Regularly, but not across all areas	Regularly and comprehensively	Shared in a timely way and learnt from
10 Are lessons from RM successes and failures learnt ?	No	No		Yes, information on successes and failures from the field and HQ are collected systematically and analysed	Yes, the organisation continuously learns from RM successes and failures (inside and outside the organisation) and systematically applies lessons across the organisation
Risk informed decision making					
11 Are key business decisions supported by an evaluation of risk and reward?	Implicitly	Partially	Yes, based on overall attitude to risk	Yes, based on approved risk appetite statement	Yes, based on near 'real-time' information
12 Are key business decisions taken after a documented consideration of risk factors?	Maybe informally	Maybe in consideration of some risk factors	Business decisions are made with reference to this based on reliable and timely risk information	Business decisions are made with reference to risk appetite (or criteria)	Dynamic risk information is used across the organisation (including HQ, field, programme, project) to make proactive effective risk decisions in relation to risk appetite
Application of accountabilities and ownership					
13 Are responsibilities/accountabilities for managing risk across the organisation clearly mapped to performance objectives and targets of specific staff and integral to overall performance management?	No	No	In certain cases, although follow through may be inconsistent	Yes - staff are held accountable for meeting their RM related objectives	Yes - staff at all levels act proactively on their risk accountabilities, seeking out and challenging risk strategies associated with key business risks under their ownership
DOCUMENTATION / EVIDENCE TO VERIFY MATURITY LEVEL					
 Agendas and supporting documentations for senior management meetings demonstrating importance attached to RM 	No	Some meeting minutes, project documentation and other documents make reference to risks	All relevant documents show commitment to RM	RM is documented as part of other relevant process	Every opportunity to include RM in documentation is seized
2 Systematic documentation of RM successes and failures at both the field and HQ	No	For certain areas / functions	May be HQ focused	Yes, organisation wide	Yes, including appropriate external review
3 Staff Performance management references RM	No	For certain areas / functions	Objectives	Objectives and appraisals	Objectives and appraisals, with quality review
4 Risk and incident reports with evidence of:	No	For certain areas / functions	To the risk governance mechanism, may be HQ focused	To and from the risk governance mechanism, HQ and the field, and business units and senior management	Additionally with quality review and feedback
5 Business cases supporting key decisions with evidence of:	No reference to risk appetite or tolerance levels	No reference to risk appetite or tolerance levels	Explicit reference made to risk appetite or tolerance levels	Supported by evidence	Additionally with quality review and feedback
6 Documented lessons learnt from identified RM successes and failures	No	No	Partial documentation of lessons learnt from identified RM successes and failures	Documented evidence of lessons learnt being identified and partially applied	Documentation of lessons learnt from experiences inside and outside the organisation and how these can be applied within the organisation

01/10/2019

Glossary of terms used in this document

Accountability framework	Documentation or references documents that describe the system that ensures accountability in an organisation.
Chief Risk Officer	The senior officer responsible to ensure that there is a framework in place for risk management, and that risks are correctly identified, assessed, responded to and reported in
	accordance with the framework.
Control criteria	The set of variables that are used to assess the effectiveness of each internal control.
Control effectiveness	A measure of how reliably the internal control operates.
Dynamic risk dashboards	Typically existing within business intelligence systems, these display real-time or near-time risk information in an easy to comprehend format.
ERM	Enterprise Risk Management, focusing in particular on the cross-functional, organisation-wide application of Risk Management.
ERM framework	The policy, procedures, manual, roles and responsibilities, processes and activities for the management of risk management across the organisation.
Financial risk modelling	Financial risk modelling is the use of formal econometric techniques to determine the aggregate risk in a financial portfolio.
Internal control framework	The policy, procedures, manual, roles and responsibilities, processes and activities for the management of internal controls.
Internal controls	Internal controls (also called controls) take various forms, such as the regulations and rules; office instructions and controls in information technology systems.
Methodology	A way or set of rules that describe how to undertake an activity.
Mitigation plans	One off measures that are intended to reduce the impact or likelihood of risks.
Operational entities	An organisational unit, division, department, section, body etc.
Process	A series of logically related activities or tasks performed together to produce a defined set of results.
Process maps	A document that visually presents the flow of activities (and controls) of a process.
Quality reviews	An inspection with a specific structure, defined roles and procedure designed to ensure a process's completeness and adherence to standards.
RBM	Results Based Management which also incorporates results based planning.
Residual risk	The residual risk remains after taking into consideration existing mitigation measures and controls.
Risk	The possibility that an event will occur or a scenario will evolve that may affect the achievement of defined objectives.
Risk appetite	The amount of risk an organisation is willing to accept in pursuit of value. Each organisation pursues various objectives to add value and should broadly understand the risk it is willing to undertake in doing so. (COSO aligned)
Risk assessment	The activity of measuring each risk's likelihood and impact in the context of a pre-defined risk scale.
Risk criteria	Risk criteria are terms of reference and are used to evaluate the significance or importance of an organisation's risks.
Risk management function	An organisational entity or role that facilitates that management of risk.
Risk platform	An advanced computer system, with links to other related systems, that is designed to management risks and internal controls and other risk related information.
Risk policy	Sets out the organisation's approach, roles and responsibilities for managing risks and controls in a consistent and business-oriented manner.
Risk register	A listing of risks and responses used to communicate the risks of an entity.
Risk response	Risk responses may include one-off mitigation actions and established controls.
Risk scale	A matrix (rating) that plots likelihood (probability) against impact.
Risk system	A computer system designed to record risks and sometimes controls.
Risk tolerance	Guides operating units as they implement risk appetite within their sphere of operation. Risk tolerances communicate a degree of flexibility, while risk appetite sets a limit beyond
	which additional risk should not be taken. (COSO)
RM	Risk Management
Statement of internal control	The Statement on Internal Control (SIC) is an accountability document that describes the effectiveness of internal controls in the organisation and is personally signed by the Accounting Officer (often SG / DG).
Three Lines of Defence (TLOD)	Conceptual governance model that delineates responsibility to three lines and oversight (web search recommended for graphical representation).
ToRs	Terms of Reference.
1013	

Annex III – Terms of Reference for Cross-Functional Task Force on Risk Management

CEB

Chief Executives Board for Coordination

CEB/2018/HLCM/15 27 September 2018

HIGH-LEVEL COMMITTEE ON MANAGEMENT (HLCM)

Thirty-Sixth Session, 11-12 October 2018 UNESCO Headquarters, Paris

DRAFT TERMS OF REFERENCE for THE GROUP ON HLCM CROSS-FUNCTIONAL ENGAGEMENT ON RISK MANAGEMENT

Background

- 1. At its 35th session in April 2018, HLCM agreed on the need for a joint, cross-functional engagement towards system-wide harmonization of risk management practices, including information sharing on fraudulent behaviors of implementing partners; assessments of risk appetite and risk tolerance; incorporating acceptance of residual risk in organizational policies; implementing smarter upstream controls; examining the costs of controls as compared to the value of the potential loss they are intended to mitigate; and, development of common definitions of risk categories to enable a common approach to reporting risks.
- 2. As part of this work, the Committee requested the Finance and Budget Network to take the lead in developing a common approach to reporting fraud and presumptive fraud, as well as to review how risk analysis might be incorporated into the budgeting processes of UN system organizations.

Composition

3. The membership of the group is small in number to enable agility and rapid delivery. It is comprised of UN system organizations that represent different spheres of work undertaken by the UN system as a whole. The group will be co-chaired by WIPO and WFP. The Finance and Budget Network will be represented in the group by IAEA, UNDP, UNESCO, UNHCR and WIPO, as concluded at the 31st Meeting of the CEB Finance and Budget Network (CEB/2018/HLCM/FB/5). The group will interact and consult with UN RIAS to ensure benefit is derived from their input and contributions.

Objective

4. It is recognized that organizations are at different levels of maturity with respect to risk management and take different approaches to risk management. As such, a one size fits all approach would be undesirable, however significant benefit could be derived from the establishment of a system wide risk management reference model. Therefore, this group is tasked to focus on three areas that could potentially be addressed over two phases as follows:

Phase 1

i) Establish a maturity model for UN entities, illustrating a potential realistic mid-term target state that takes into account commonalities and differences of organizations' size, structure and mandate. The model may serve firstly to benchmark the level of risk maturity in an organization through various dimensions and secondly, as a guide for agencies implementing risk management. Both would serve as a basis for communication on risk management with Governing and Oversight bodies.

Phase 2

- ii) Develop guidance on how a UN system organization may approach the establishment of key organizational risk management approaches, to include:
 - a) Risk appetite and risk tolerance recognized by the Governing body;
 - b) Embedding risk management into performance/planning processes;
 - c) Integrating control systems with Enterprise Risk Management; and
 - d) Establishing an organizational structure that supports effective cross-functional risk management and clarifies roles and responsibilities, including a recommended approach to implementing the 3 lines of defence
- iii) Propose a sustainable and pragmatic mechanism for exchanging views/advice and accessing best and leading risk management practices (not restricted to the UN system) to ultimately include policy, process, tools and systems and structures.

Deliverables

5. The following documents are foreseen as deliverables:

Phase 1

i) The definition of a multiple stage maturity model that exhibits the characteristics and features of an organization deemed to be in each defined stage of organizational risk management maturity. The model may include maturity dimensions of, for example, risk culture, process and integration, policy framework, governance and organizational structure, system and tools, and risk capabilities. The model may serve as both a benchmarking tool to provide consistent comparison of UN system organizations' risk management maturity, and also as an implementation guide to advance risk management in the organization.

Phase 2

- ii) Pragmatic guidance for organizations intending to enhance their existing Risk Management Framework, to include considerations, limitations, benefits and drawbacks when developing key organizational risk management approaches. This guidance would initially focus on how a UN system organization may implement:
 - a) Risk appetite and risk tolerance;
 - b) The embedding of Enterprise Risk Management into performance/ planning processes;
 - c) The integration of the organization's internal control framework with Enterprise Risk Management; and
 - d) An organizational structure that recognizes the emerging and cross-functional nature of Enterprise Risk Management (e.g. program, finance, physical and information security, resilience, etc.) and embeds the three lines of defense model.
- iii) A proposal for a forum and/or sharing mechanism (e.g. platform/repository) that permits organizations to effectively exchange views and access best practices together with sample deliverables related to policy, process, systems and structures.

Timeline

- 6. The timeline for Phase 1 has been established at approximately 10-12 weeks, ideally to report progress back to the subsequent HLCM meeting.
- 7. If the benefits and interest from UN system organizations so dictates, Phase 2 and any subsequent phases may be planned.