Annex II - Reference Maturity Model for Risk Management

(i) Usage Guidelines

HLCM Cross-Functional Task Force on Risk Management

Reference Maturity Model for Risk Management Usage Guidelines

September 2019

Table of Contents

1. Introduction 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. The 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. Undertaking a self-assessment 3
3.1 Preparing for the self-assessment 3
3.2 Starting the self-assessment 4
4. Taking 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 inter-agency 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 non-prescriptive, 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 section 2.3. For each maturity level, the criteria for achieving that level is expressed on the vertical axis, in terms of six dimensions, as described in section 2.4. Each dimension is, in turn, articulated in between two and five sub-dimensions.

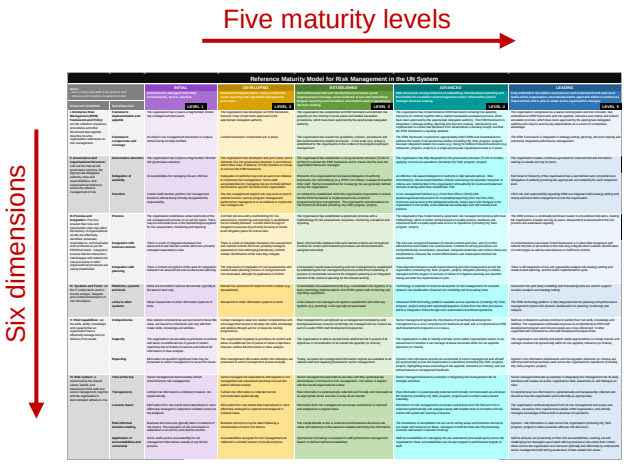
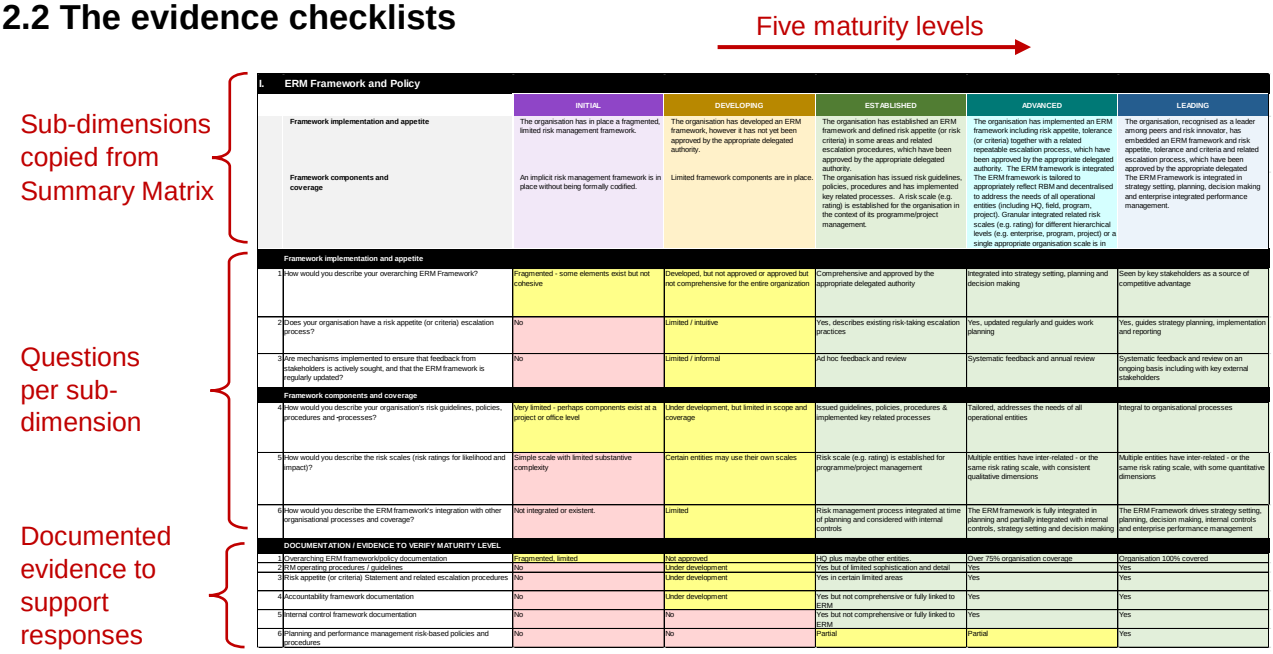


Figure 1: The Summary Matrix

2.2 The evidence checklists



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	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
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, program, project). Granular integrated related risk scales (e.g. rating) for different hierarchical levels (e.g. enterprise, 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 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					
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	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
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	Fragmented, limited	Not approved	HQ plus maybe other entities.	Over 75% organisation coverage	Organisation 100% covered
2 RM operating procedures / guidelines	No	Under development	Yes but of limited sophistication and detail	Yes	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

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.

(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. *Sub-dimensions: 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.

Start here

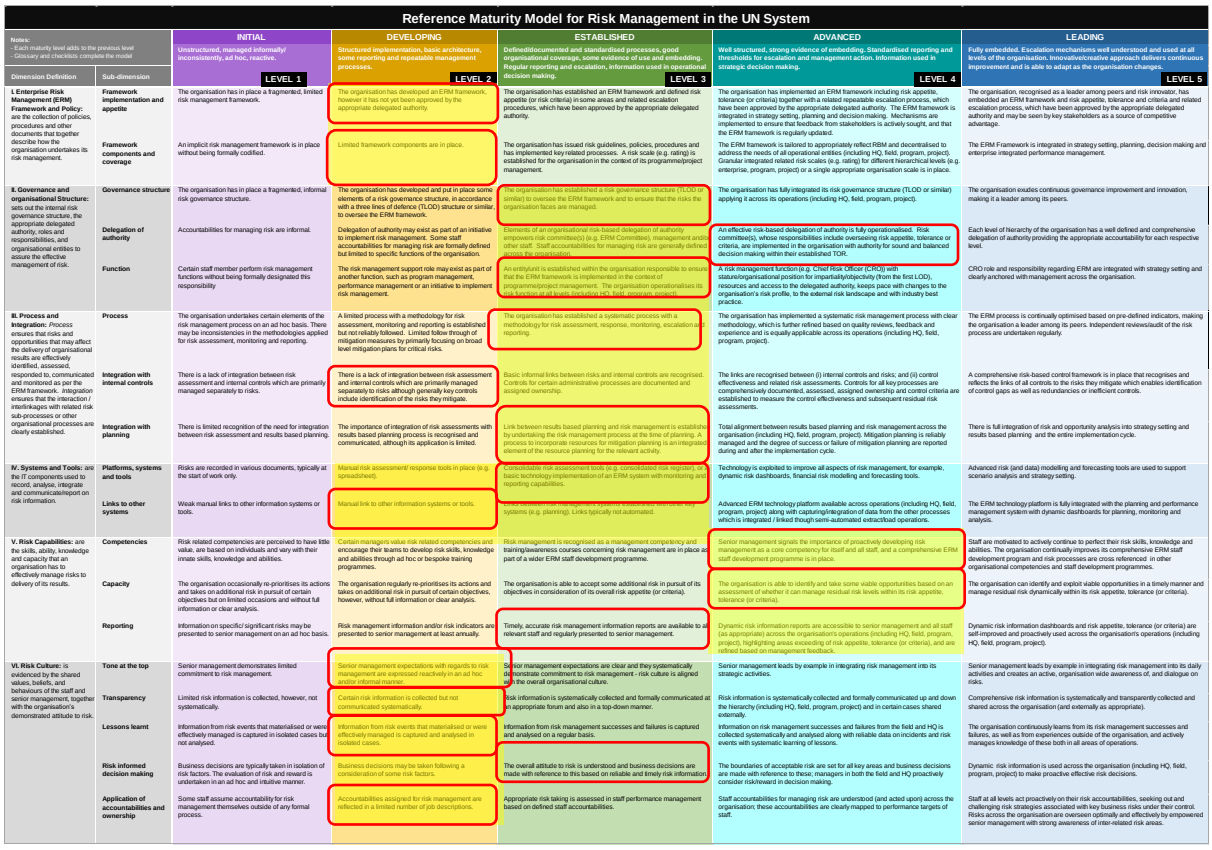
II.	Governance and Organisational Structure			
		INITIAL	DEVELOPING	ESTABLISHED
	Governance structure	The organisation has in place a fragmented, informal risk governance structure.	The organisation has developed and put in place some elements of a risk governance structure, in accordance with a three 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 exist as part of another function, such as program 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 of Defence
2	Coverage of the risk governance structure that oversees the ERM framework	Limited	Limited	HQ or certain locations
	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	Issued 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 that 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-related job descriptions and most policies as appropriate
2	RM function charter or equivalent established	No	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 Maturity Model for Risk Management in the UN System

Notes: - Each maturity level adds to the previous level - Glossary and checklists complete the model		INITIAL Unstructured, managed informally/ inconsistently, ad hoc, reactive. LEVEL 1	DEVELOPING Structured implementation, basic architecture, some reporting and repeatable management processes. LEVEL 2	ESTABLISHED Definedidocumented and standardised processes, good organisational coverage, some evidence of use and embedding. Regular reporting and escalation, information used in operational decision making. LEVEL 3	ADVANCED Well structured, strong evidence of embedding. Standardised reporting and thresholds for escalation and management action. Information used in strategic decision making. LEVEL 4	LEADING Fully embedded. Escalation mechanisms well understood and used at all levels of the organisation. Innovativelcreative approach delivers continuous improvement and is able to adapt as the organisation changes. LEVEL 5
Dimension Definition	**Sub-dimension**					
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.	**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.	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 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, program, project). Granular integrated related risk scales (e.g. rating) for different hierarchical levels (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 and enterprise integrated performance 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.	**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, program, 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(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.
	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 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 Officer (CRO)) with statute/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 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, 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.	**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 methodology, which is further refined based on quality reviews, feedback and experience and is equally applicable across its operations (including HQ, field, program, 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, program, 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 communicate/report on risk information.	**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).	Consolidated risk assessment tools (e.g. consolidated risk register), on 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.	Some automated links between risk systems (consolidated risk register) and key 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 effectively manage risks to delivery of its results.	**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 program 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, program, 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, program, project).
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.	**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, organisation 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, program, project) and in certain cases shared externally.	Comprehensive risk information is systematically and transparently collected 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 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, 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 senior management with strong awareness of inter-related 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.