Annex II - Reference Maturity Model for Risk Management

(ii) Summary Matrix

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 Defined/documented 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 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. 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, 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.
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, 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(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 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, programme, project).	A risk management function (e.g. Chief Risk Officer (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 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, 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.
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).	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.
V. Risk Capabilities: are the skills, ability, knowledge and capacity that an organisation must effectively manage risks to deliver 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 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).
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, 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).
	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.