Annex II - Reference Maturity Model for Risk Management

(iii) Evidence Checklists

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 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.
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

II. 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(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, program, 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.
	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	Issued guidelines, policies, procedures & implemented key related processes	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. 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					
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 setting and clearly anchored with management across the organisation
	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	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 all 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.	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.

	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

III. Process and Integration (continued)

		INITIAL	DEVELOPING	ESTABLISHED	ADVANCED	LEADING
	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

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	LEADING
	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).
1	Do staff have the skills they need to manage risks and exploit opportunities to objectives under their purview?	Possibly, through past experiences	In certain cases	increasingly, particularly in HQ	Yes in some areas, still some gaps	Yes, organisation wide
2	Do staff undertake continuous development of their RM skills?	No	Selected staff with specific risk management responsibilities develop their skills through their own initiative	Yes across the organisation as opportunities are presented	Yes - across the organisation as opportunities are presented and certain areas are motivated to proactively continually develop their risk skills	Yes - staff across the organisation proactively seek training opportunities to keep them "leading"
3	Do some staff in RM roles hold RM qualifications?	Possibly, through past experiences	Ad hoc / developing existing staff	Yes, may be various qualifications	Yes - encouraged and consistent	Yes - required for all managerial and other relevant positions
4	Is risk awareness recognised as a competency across the organisation?	No	Certain cases	Management competency	Core Competency	Yes, cross referenced in other organisational competencies
5	Is tailored RM training available in support of the wider ERM staff 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					
6	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 (or 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	No	No	Under development	Data analytics used to confirm key control's effectiveness for a limited number of controls	Advanced use of data analytics recognise control breaches, improve control effectiveness and reduce risk
	DOCUMENTATION / EVIDENCE TO VERIFY MATURITY LEVEL					
1	RM training materials	Project level	Also at programme / unit level	Also at Field / external office, e.g. well designed eLearning courses	Developed in conjunction with other subject area learning materials	Refined with external feedback, continuously improving
2	Completion rates of RM courses	Not recorded	< 10% all staff	40% all staff	All staff	All staff with refresher programme
3	Timely, accurate RM information reports produced	No	Occasionally	Quarterly for risk committee and/or senior management	Quarterly or more, for all staff	Quarterly or more, for all stakeholders or public
4	Professional qualifications of staff in RM (IRM, CRMA, M_O_R etc.)	No	May be studying or recognized as a benefit	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
6	Business cases for key decisions assessing whether residual risk can be 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

VI. 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, 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.
	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 from 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 organisational 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 governing 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 collected 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	Inconsistently	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					
1	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

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.