Risk Management Framework Review

ORGANISATION: DATE: LEGEND: Y = Addresses criteria, P = Partially addresses criteria, N = Does not address criteria

1. RISK MANAGEMENT PRINCIPLES		ISO31000 REFERENCE	FINDINGS	SYSTEM REFERENCE	AUDIT COMMENTS	ACTION PLAN	DUE DATE	RESPSONSIBILITY
1.1	Does the organisation have a risk management framework which incorporates the following principles: a) Integrated b) Structured and comprehensive c) Customised d) Inclusive e) Dynamic f)Best Available Information i) Human and Cultural Factors J) Continual Improvement	4						
2. RISK FRAMEWORK - LEADERSHIP AND COMMITMENT		**ISO31000 REFERENCE**	**FINDINGS**	**SYSTEM REFERENCE**	**AUDIT COMMENTS**	**ACTION PLAN**	**DUE DATE**	**RESPSONSIBILITY**
2.1	Do top management ensure that risk management is integrated into all organisational activities and demonstrate leadership and commitment by: a) customising and implementing all components of the framework b) issues a statement or policy that establishes a risk management approach, plan or course of action c) ensuring the necessary resources are allocated to managing risks d) assigning authority, responsibility and accountability at appropriate levels within the organisation	5.2						
2.2	Are top management and the oversight body accountable for overseeing risk management through: a) Ensuring that risks are adequately considered when setting the organisations values b)understanding the risks facing the organisation in pursuit of its objectives c) Ensuring systems to manage such risks are implemented and operating effectively d) ensuring that such risks are appropriate in the context of the organisations objectives e) ensuring that information about such risks and their management is properly communicated	5.2						
3. RISK FRAMEWORK - INTEGRATION		**ISO31000 REFERENCE**	**FINDINGS**	**SYSTEM REFERENCE**	**AUDIT COMMENTS**	**ACTION PLAN**	**DUE DATE**	**RESPSONSIBILITY**
3.1	Is organisational structure and context considered in the integration of risk management. Is risk managed in every part of the organisations structure. Does everyone in the organisation have responsibility for managing risk. Do governance arrangements , including the relationships, rules, processes, practices of the org consider risk management. Do management arrangements including strategy implementation and business operations consider risk management. Has accountability and oversight for risk management been identified within the governance arrangements. Has risk management integration considered the organisations needs and culture, purpose, governance, leadership and commitment, strategy, objectives and operations.							
4. RISK FRAMEWORK - DESIGN		**ISO31000 REFERENCE**	**FINDINGS**	**SYSTEM REFERENCE**	**AUDIT COMMENTS**	**ACTION PLAN**	**DUE DATE**	**RESPSONSIBILITY**

SAMPLE - INTENTIONALLY FADED

4.1	In designing the risk management framework, has the organisation examined and understood its external context, including: - the social, culture, political, legal, regulatory, financial, technological, economic and environmental factors. - key drivers and trends affecting the objectives of the organisation. - external stakeholder relationships, perceptions, values, needs and expectations. - contractual relationships and commitments. - the complexity of networks and dependencies.	5.4.1						
4.2	In designing the risk management framework, has the organisation examine and understood its internal context, including: - Vision, mission and values. - governance, structures, roles and responsibilities. - strategy, objectives and policies. - organisational culture. - standards, guidelines and models adopted by the organisation. - capabilities, resources and knowledge of the organisation. - data, information systems and information flows. - relationships with internal stakeholders, taking into account their perceptions and values. - contractual relationships and commitments. - interdependencies and interconnections.	5.4.1						
4.3	Have the board and top management demonstrated and articulated their continual commitment to risk management through a policy, statement or other forms that clearly convey the organisations objectives and commitment to risk management.	5.4.2						
4.4	Has the organisation assigned and communicated authorities, responsibilities and accountabilities for relevant roles with respect to risk management.	5.4.3						
4.5	Has the organisation allocated appropriate resources for risk management including - people, skills, experience and competence. - processes, methods and tools - documented processes and procedures - information and knowledge management systems - professional development and training needs.	5.4.4						
4.6	Has the organisation established and approved an approach to communication and consultation to support the framework and facilitate the effective application of risk management.	5.4.5						
5. RISK FRAMEWORK - IMPLEMENTATION		ISO31000 REFERENCE	FINDINGS	SYSTEM REFERENCE	AUDIT COMMENTS		ACTION PLAN	DUE DATE	RESPSONSIBILITY
5.1	Has the organisation implemented the risk management framework by: - developing an appropriate plan including time and resources. - identifying where, when and how different types of decisions are made across the organisation and by whom. - modifying the applicable decision making processes where necessary. - ensuring risk management arrangements are clearly understood and practiced.	5.5						
6. RISK FRAMEWORK EVALUATION		ISO31000 REFERENCE	FINDINGS	SYSTEM REFERENCE	AUDIT COMMENTS		ACTION PLAN	DUE DATE	RESPSONSIBILITY

SAMPLE - INTENTIONALLY FADED

SAMPLE - INTENTIONALLY FADED

6.1	Does the organisation evaluate the effectiveness of the risk management framework by: - periodically measuring risk management framework performance against its purpose, implementation plans, indicators and expected behaviour; - determining whether the framework remains suitable to support the organisation achieving its objectives.	5.6						
7. RISK FRAMEWORK - IMPROVEMENT		ISO31000 REFERENCE	FINDINGS	SYSTEM REFERENCE	AUDIT COMMENTS	ACTION PLAN	DUE DATE	RESPSONSIBILITY
7.1	Does the organisation continually monitor and adapt the risk management framework to address external and internal changes	5.7.1						
7.2	Does the organisation continually improve the suitability, adequacy and effectiveness of the risk management framework and the way the risk management process is integrated.	5.7.2						
7.3	Where gaps or improvement opportunities are identified, does the organisation develop plans and tasks and assign them to those accountable for implementation.	5.7.3						
8. RISK PROCESS		ISO31000 REFERENCE	FINDINGS	SYSTEM REFERENCE	AUDIT COMMENTS	ACTION PLAN	DUE DATE	RESPSONSIBILITY
8.1	Has the organisation established a risk management process which involves the systematic applications of policies, procedures and practices to the activities of communicating, consulting, establishing the context and assessing, treating, monitoring, reviewing, recording and reporting risk?	6.1						
8.2	Is the risk management process: - an integral part of the management and decision making of the organisation - integrated into the structure, operations and processes of the organisation - able to be applied to strategic, operational, program or project levels - customised to achieve objectives - customised to suit the external and internal context in which they are applied - designed to take into account the dynamic and variable nature of human behaviour and culture	SAMPLE - INTENTIONALLY FADED						
9. COMMUNICATION AND CONSULTATION		ISO31000 REFERENCE	FINDINGS	SYSTEM REFERENCE	AUDIT COMMENTS	ACTION PLAN	DUE DATE	RESPSONSIBILITY
9.1	Has the organisation established effective arrangements for communication, consultation and exchange of information with all external and internal stakeholders within and throughout all steps of the risk management process?	6.2						
9.2	Do communication and consultation methods: - bring different areas of expertise together for each step of the risk management process - ensure that different views are appropriately considered when defining risk criteria and when evaluating risks - provide sufficient information to facilitate risk oversight and decision making - build a sense of inclusiveness and ownership among those affected by the risk	6.2						
10. SCOPE, CONTEXT AND CRITERIA		ISO31000 REFERENCE	FINDINGS	SYSTEM REFERENCE	AUDIT COMMENTS	ACTION PLAN	DUE DATE	RESPSONSIBILITY
10.1	Has the organisation established and defined the scope, context and criteria to customise the risk management process, including defining the scope of its risk management activities?	6.3.1						
10.2	Has the defined scope considered application of the risk management process at different levels, including strategic, operational, program, project or other activities)?	6.3.2						
10.3	Has planning considered: - objectives and decisions that need to be made - outcomes expected from the steps to be taken in the process - time, locations, specific inclusions and exclusions - appropriate risk assessment tools and techniques - resources required, responsibilities and records to be kept - relationships with other projects, processes and activities.	6.3.2						

10.4	Has establishing the context of the risk management processes considered the environment in which the organisation seeks to define and achieve its objectives, Does it demonstrate an understanding of the external and internal environment in which the organisation operates and reflect the specific activities to which the risk management process is to be applied?	6.3.3	SAMPLE - INTENTIONALLY FADED					
10.5	Has the organisation established a risk criteria which: - specifies the amount and type of risk it may or may not take, relative to objectives - evaluates the significance of risk and supports decision making processes - is aligned with and customised to the specific purpose and scope of the activity under consideration - reflects the organisations values, objectives and resources and is consistent with policies and statements about risk management	6.3.4						
10.6	In establishing risk criteria, have the following factors been considered: - the nature and type of uncertainties that can affect outcomes and objectives - how consequences (negative and positive) and likelihood will be defined and measured - time related factors - consistency in the use of measurements - how the level of risk is to be determined - how combinations and sequences of multiple risks will be taken into account - the organisations capacity	6.3.4						
11. RISK ASSESSMENT - IDENTIFICATION		ISO31000 REFERENCE	FINDINGS	SYSTEM REFERENCE	AUDIT COMMENTS	ACTION PLAN	DUE DATE	RESPSONSIBILITY
11.1	Does the organisation have processes for the effectives identification, analysis and evaluation of risk which is conducted systematically, iteratively and collaboratively, drawing on the knowledge and views if stakeholders?	6.4.1						
11.2	Does the organisation have processes to effectively find, recognise and describe risks that might help or prevent an organisation achieving its objectives, including consideration of the following factors: - tangible and intangible sources of risk - causes and events - threats and opportunities - vulnerabilities and capabilities - changes in the external and internal context - indicators of emerging risks - nature and value of assets and resources consequences and their impact on objectives - limitations of knowledge and reliability of information - time related factors - biases, assumptions and beliefs of those involved	6.4.2	SAMPLE - INTENTIONALLY FADED					
11.3	Does the organisation identify risks whether or not their sources are under its control?	6.4.2						
12. RISK ASSESSMENT - ANALYSIS		ISO31000 REFERENCE	FINDINGS	SYSTEM REFERENCE	AUDIT COMMENTS	ACTION PLAN	DUE DATE	RESPSONSIBILITY
12.1	Does the risk process include a process for the analysis of risk in order to comprehend the nature and characteristics of the risk, including: - the likelihood of events and consequences - the nature and magnitude of consequences - complexity and connectivity - time related factors and volatility - effectiveness of existing controls - sensitivity and confidence levels	6.4.3						
13. RISK ASSESSMENT - EVALUATION		ISO31000 REFERENCE	FINDINGS	SYSTEM REFERENCE	AUDIT COMMENTS	ACTION PLAN	DUE DATE	RESPSONSIBILITY
13.1	Does the risk process include a process to support decision making, by evaluating the results of risk analysis with the established risk criteria to determine where additional action is required?	6.4.4						
14. RISK TREATMENT		ISO31000 REFERENCE	FINDINGS	SYSTEM REFERENCE	AUDIT COMMENTS	ACTION PLAN	DUE DATE	RESPSONSIBILITY

14.1	Does the risk treatment process support the organisation in: - formulating and selecting risk treatment options - planning and implementing risk treatment - assessment the effectiveness of that treatment - deciding whether the remaining risk is acceptable - if not acceptable, taking further treatment	6.5						
14.2	Does the risk treatment process support the organisation in balancing the potential benefits derived from achieving an objective against the costs, effort or disadvantages of implementation - including provisions for: - avoiding the risk - taking or increasing the risk to pursue an opportunity - removing the risk source - changing the likelihood - changing the consequence - sharing the risk - retaining the risk by informed decision	6.5.2						
14.3	Does the risk treatment process take into account more than just economic considerations including the organisations obligations, commitments, stakeholder views, values, perceptions, unintended consequences of the treatment, monitoring and review of the effectiveness of the treatment, documentation and recording of decisions relating to risk treatment.	6.5.2						
14.4	Are risk treatment plans developed, documented, monitored and integrated into the management plans and processes of the organisation, including: - the rationale for selection and expected benefits to be gained - those accountable and responsible for approving and implementing the plan - proposed actions - resources required including contingency - performance measures - constraints - required reporting and monitoring - when actions are expected to be undertaken and completed	6.5.3						
15. MONITORING AND REVIEW		ISO31000 REFERENCE	FINDINGS	SYSTEM REFERENCE	AUDIT COMMENTS		ACTION PLAN	DUE DATE	RESPSONSIBILITY
15.1	Does the organisation have systems and processes to assure itself of, and improve the quality and effectiveness of process design, implementation and outcomes through a planning periodic review of the risk management process. Are the results of monitoring and review incorporated into the organisations performance management, measurement and reporting activities.	6.6						
16. RECORDING AND REPORTING		ISO31000 REFERENCE	FINDINGS	SYSTEM REFERENCE	AUDIT COMMENTS		ACTION PLAN	DUE DATE	RESPSONSIBILITY
16.1	Does the organisation have appropriate mechanisms through which to document and report outcomes of the risk management process, including processes which: - communicate risk management activities and outcomes across the organisation - Provide information for decision making - improve risk management activities - assist in interactions with stakeholders including those with responsibility and accountability for risk management activities	6.7						