

Addendum A: Conceptual ERM implementation model: theoretical frameworks, building blocks, best practice requirements and proposed deliverables

Theoretical frameworks		Building blocks	Best practice requirements						Proposed deliverables	
Deming cycle	Weisbord organisational design model		Level 1	Source	Ref.	Level 2	Source	Ref.	Purpose	Deliverables
Plan	Purpose, Leadership	I. Get permission.	Ensure legal and regulatory compliance.	ISO 31000	4.2				To motivate the need for an ERM program.	Compliance requirements (legal + regulatory + best practise frameworks)
			The board should delegate to management the responsibility to design, implement and monitor the risk management plan.	King III	4.4				To ask for permission / mandate to design and implement the ERM program.	Agenda item for Board meeting
									To record the permission / mandate received to design and implement an ERM program.	Minutes of the Board meeting
			The risk committee or audit committee should assist the board in carrying out its risk responsibilities.	King III	4.3	The board should appoint a committee responsible for risk.	King III	4.3.1	To assist the board in carrying out its risk roles and responsibilities.	Board risk committee (BRC) charter
						The risk committee should:		4.3.2		
						consider the risk management policy and plan and monitor the risk management process;		4.3.2.1		
						have as its members executive and non-executive directors, members of senior management and independent risk management experts to be invited, if necessary;		4.3.2.2		
						have a minimum of three members; and		4.3.2.3		
						convene at least twice per year.		4.3.2.4		
						The board's responsibility for risk governance should be expressed in the board charter.		4.1.3		
			Define and endorse the risk management policy.	King III	4.1.1	The board's responsibility for risk governance should manifest in a documented risk management policy and plan.	King III	4.1.5	To document risk management scope, objectives and roles and responsibilities.	Risk management policy
						The board should approve the risk management policy and plan.		4.1.6		
				ISO 31000	4.2 & 4.3.2	The risk management policy should be widely distributed throughout the company.		4.1.7		
Plan	Leadership, Relationships	II. Establish the tone of the organisation.	The introduction of risk management and ensuring its ongoing effectiveness require strong and sustained commitment by management of the organisation, as well as strategic and rigorous planning to achieve commitment at all levels.	ISO 31000	4.2	The CRO should be a suitably experienced person who should have access and interact regularly on strategic matters with the board and/or appropriate board committee and executive management.	King III	4.4.3	A senior level ERM program sponsor / Chief Risk Officer should have clear authority over and accountability for oversight of risk across the enterprise	CRO / Senior level project sponsor
						Ensure that the organisation's culture and risk management policy are aligned.	ISO 31000	4.2	To create risk awareness at all levels of the organisations and to encourage risk based decision making.	Risk management policy
						Determine risk management performance indicators that align with performance indicators of the organisation.			To measure risk management performance against indicators, which are periodically reviewed for appropriateness;	Performance indicators (Key risk indicators)
						Align risk management objectives with the objectives and strategies of the organisation.			To encourage a risk mind-set for decision making.	Risk appetite & risk tolerance
						Assign accountabilities and responsibilities at appropriate levels within the organisation.			To reduce role confusion by establishing clear roles and responsibilities for risk activities across businesses and risk types.	Risk governance model: (incl. risk owners' matrix, roles & responsibilities, reporting & escalation process & incentives guidelines.)
						Ensure that the necessary resources are allocated to risk management.			To ensure the effective and efficient implementation of the ERM program.	Risk management plan (People, Processes and Budget)
						Communicate the benefits of risk management to all stakeholders.			To raise risk awareness and create excitement for the project.	Benefits of risk management
			The induction and ongoing training programs of the board should incorporate risk governance. (Note: apply to all the levels in the organisation)	King III	4.1.4				To create a common risk language, improve risk awareness and encourage risk based decision making.	Risk awareness gap analysis
										Risk maturity model
										Risk awareness plan

Addendum A: Conceptual ERM implementation model: theoretical frameworks, building blocks, best practice requirements and proposed deliverables

Theoretical frameworks		Building blocks	Best practice requirements						Proposed deliverables	
Deming cycle	Weisbord organisational design model		Level 1	Source	Ref.	Level 2	Source	Ref.	Purpose	Deliverables
Plan	Purpose, Relationships, Structure, External environment	III. Design the rules of the game.	Design the risk management framework.	ISO 31000	4.3	Task: Understanding the organisation and its context (Know your organisation)				
						Establish the external context:	ISO 31000	4.3.1 & 5.3.2	To get an overall picture of the external environment based PESTLE and / or Porter's 5 forces.	Environmental scanning report
						(a) the social and cultural, political, legal, regulatory, financial, technological, economic, natural and competitive environment, whether international, national, regional or local;				
						(b) key drivers and trends having impact on the objectives of the organisation; and				
						(c) External stakeholder analysis				
						Establish the internal context:	ISO 31000	4.3.1 & 5.3.3	To describe the internal value chain of the organisation and to identify areas that would create risks and opportunities	
						(a) Governance, organisational structure, roles and accountabilities;				Environmental scanning of the INTERNAL value chain
										SWOT analysis
										Organisational organigram
										Divisional organigram
										Departmental organigram
										Delegation of authority
										Committee structure
										Committee charters
										List of policies
										Copy of policies
										Action plans (strategies)
										Risk competency model
										Job profiles / specification
							Technical job specs			
	List of systems									
	Process maps									
	Escalation policy									
	Escalation process									
	Connected stakeholder analysis									
	Internal stakeholder analysis									
	Organisational culture survey results									
	List of standards, guidelines and models									
	Contracts register									
	Establish the context of the risk management process (The context of the risk management process will vary according to the needs of an organisation. It can involve, but is not limited to:	ISO 31000	4.3.1 & 5.3.4	To create ONE set of risk management rules for the organisation.	Risk management file / manual that includes:					
(a) Defining the goals and objectives of the risk management activities;	Risk management goals & -objectives									
(b) Defining responsibilities for and within the risk management process;	Risk governance model									
(c) Defining the scope, as well as the depth and breadth of the risk management activities to be carried out, including specific inclusions and exclusions;	Top-down & Bottom-up risk management activities									

Addendum A: Conceptual ERM implementation model: theoretical frameworks, building blocks, best practice requirements and proposed deliverables

Theoretical frameworks		Building blocks	Best practice requirements						Proposed deliverables	
Deming cycle	Weisbord organisational design model		Level 1	Source	Ref.	Level 2	Source	Ref.	Purpose	Deliverables
Plan	Purpose, Relationships, Structure, External environment	III. Design the rules of the game.	Design the risk management framework.	ISO 31000	4.3	(e) Defining the activity, process, function, project, product, service or asset in terms of time and location;	ISO 31000	4.3.1 & 5.3.4	To create ONE set of risk management rules for the organisation.	Top-down & Bottom-up risk management activities
						(f) Defining the relationships between a particular project, process or activity and other projects, processes or activities of the organisation;				Interconnectedness maps
						(g) Defining the risk assessment methodologies;				Risk assessment methodologies
						(h) Defining the way performance and effectiveness is evaluated in the management of risk;				Key risk indicators
						(i) Identifying and specifying the decisions that have to be made; and				Decision matrix
						(j) Identifying, scoping or framing studies needed, their extent and objectives, and the resources required for such studies.				Research to clarify context
						Define the risk criteria (When defining risk criteria, factors to be considered should include the following:	ISO 31000 / King III	4.3.1 & 5.3.5 / 4.2.1 & 4.2.2	To create standardised risk assessment criteria for the organisation as a whole. To give risk owners and other risk stakeholders insight into risk management in their terms.	Risk management file / manual that includes:
						(a) The nature and types of causes and consequences that can occur and how they will be measured;				Examples of causes and consequences
						(b) How likelihood will be defined;				Risk assessment tools and techniques
						(c) The timeframe(s) of the likelihood and/or consequence(s);				Risk management plan
						(d) How the level of risk is to be determined;				Risk appetite guidelines
						(e) The views of stakeholders;				Risk tolerance levels guidelines
						(f) The level at which risk becomes acceptable or tolerable; and				
						(g) Whether combinations of multiple risks should be taken into account and, if so, how and which combinations should be considered.				
						Task: establishing the risk management policy	ISO 31000	4.3.2	To document risk management scope, objectives and roles and responsibilities.	Risk management policy
						(a) A policy and plan for a system and process of risk management should be developed.	King III	4.1.1		
						(c) The board's responsibility for risk governance should manifest in a documented risk management policy and plan.		4.1.5		
						(d) The board should approve the risk management policy and plan.		4.1.6		
						The risk management policy should be widely distributed throughout the company.		4.1.7		
						Task: develop an accountability matrix / risk governance framework	ISO 31000	4.3.3	To establish clear roles and responsibilities for risk activities across businesses and risk types.	Risk governance model: (incl. risk owners' matrix, roles & responsibilities, reporting & escalation process & incentives guidelines.)
						(a) Identifying risk owners that have the accountability and authority to manage risks;				
						(b) Identifying who is accountable for the development, implementation and maintenance of the framework for managing risk;				

Addendum A: Conceptual ERM implementation model: theoretical frameworks, building blocks, best practice requirements and proposed deliverables

Theoretical frameworks		Building blocks	Best practice requirements						Proposed deliverables	
Deming cycle	Weisbord organisational design model		Level 1	Source	Ref.	Level 2	Source	Ref.	Purpose	Deliverables
Plan	Purpose, Relationships, Structure, External environment	III. Design the rules of the game.	Design the risk management framework.	ISO 31000	4.3	(c) Identifying other responsibilities of people at all levels in the organisation for the risk management process;	ISO 31000	4.3.3	To establish clear roles and responsibilities for risk activities across businesses and risk types.	Risk governance model: (incl. risk owners' matrix, roles & responsibilities, reporting & escalation process & incentives guidelines.)
						(d) Establishing performance measurement and external and/or internal reporting and escalation processes; and				
						(e) Ensuring appropriate levels of recognition.				
						Task: integration into organisational processes	King III	4.4.2		
						Develop a common risk language	Researcher		To develop a standardised risk management language for the organisation.	Common risk language
						Risk management should be embedded in all the organisation's practices and processes in a way that it is relevant, effective and efficient.	ISO 31000	4.3.4	To embed risk management in all the organisation's practices and processes in a way that it is relevant, effective and efficient.	Risk owners
										Strategic plan
										Business plan
										Financial plan
										Risk & incident escalation process
						Align risk management objectives with the objectives and strategies of the organisation.	ISO 31000	4.2	To encourage a risk mind-set for decision making.	Risk appetite guidelines
						Determine risk management performance indicators that align with performance indicators of the organisation.	ISO 31000	4.2	To measure risk management performance against indicators, which are periodically reviewed for appropriateness;	Risk tolerance levels guidelines
						Task: Establishing internal communication and reporting mechanisms	ISO 31000	4.3.6	To create one set of rules for risk communication and also to increase risk transparency.	Internal reporting guidelines
						(a) Key components of the risk management framework, and any subsequent modifications, are communicated appropriately;				Communication guidelines
						(b) There is adequate internal reporting on the framework, its effectiveness and the outcomes;				
						(c) Relevant information derived from the application of risk management is available at appropriate levels and times; and				
						(d) There are processes for consultation with internal stakeholders.				
						Task: Establishing external communication and reporting mechanisms	ISO 31000 / King III	4.3.7 / 4.10	To create one set of rules for risk communication and also to increase risk transparency.	Integrated report: risks and opportunities section
						(a) Engaging appropriate external stakeholders and ensuring an effective exchange of information;				External reporting guidelines
						(b) External reporting to comply with legal, regulatory, and governance requirements;				
						(c) Providing feedback and reporting on communication and consultation;				Communication guidelines

Addendum A: Conceptual ERM implementation model: theoretical frameworks, building blocks, best practice requirements and proposed deliverables

Theoretical frameworks		Building blocks	Best practice requirements						Proposed deliverables		
Deming cycle	Weisbord organisational design model		Level 1	Source	Ref.	Level 2	Source	Ref.	Purpose	Deliverables	
Plan	Purpose, Relationships, Structure, External environment	III. Design the rules of the game.	Risk management process.	ISO 31000	5	Step 1: Communication and consultation Step 2: Establish the context Step 3: Risk identification Step 4: Risk analysis Step 5: Risk evaluation Step 6: Risk treatment Step 7: Monitor and review Step 8: Continual improvement	ISO 31000	5.2 4.3.1 & 5.3 5.4.2 5.4.3 5.4.4 5.5 5.6 4.6	To develop a standardised risk management process for the organisation.	Risk management process guidelines	
Plan	Helping mechanisms, Relationships, Rewards	IV. Develop the risk infrastructure.	Task: Allocate appropriate resources for risk management								
			People (skills, experience, competence & training programs).	ISO 31000	4.3.5	People: skills, experience, competence & training programs	ISO 31000	4.3.5	To establish decision making structures, escalation protocol & identify risk stakeholders.	Risk governance models	
									To identify competencies, skills levels and experience required by risk stakeholders.	Risk competency model	
									To ensure proper training for risk stakeholders.	Risk training	
			Committees: the board should delegate certain functions to well-structured committees but without abdicating its own responsibilities.	King III	2.23	Board committees:	King III	2.23	To formalise decision making structures, escalation protocol & identify risk stakeholders.	Board committees charter / terms of reference	
						Formal terms of reference should be established and approved for each committee of the board.					2.23.1
						The committees' terms of reference should be reviewed yearly.					2.23.2
						The committees should be appropriately constituted and the composition and the terms of reference should be disclosed in the integrated report.					2.23.3
						The risk committee should:	King III	4.3.2		Risk committees:	
						consider the risk management policy and plan and monitor the risk management process;				Board risk committee charter	
						have as its members executive and non-executive directors, members of senior management and independent risk management experts to be invited, if necessary;				Executive risk committee charter	
						have a minimum of three members; and convene at least twice per year.					Departmental risk committee charter
						The audit committee should:					
						oversee integrated reporting.	King III	3.4		Audit committee charter	
						have regard to all factors and risks that may impact on the integrity of the integrated report.					
						review and comment on the financial statements included in the integrated report.					
						review the disclosure of sustainability issues in the integrated report to ensure that it is reliable and does not conflict with the financial information.					
						recommend to the board to engage an external assurance provider on material sustainability issues.					
						consider the need to issue interim results.					
						review the content of the summarised information.					

Addendum A: Conceptual ERM implementation model: theoretical frameworks, building blocks, best practice requirements and proposed deliverables

Theoretical frameworks		Building blocks	Best practice requirements						Proposed deliverables		
Deming cycle	Weisbord organisational design model		Level 1	Source	Ref.	Level 2	Source	Ref.	Purpose	Deliverables	
Plan	Helping mechanisms, Relationships, Rewards	IV. Develop the risk infrastructure.	Committees: the board should delegate certain functions to well-structured committees but without abdicating its own responsibilities.	King III	2.23	engage the external auditors to provide assurance on the summarised financial information.	King III	3.4	To formalise decision making structures, escalation protocol & identify risk stakeholders.	Audit committee charter	
						ensure that a combined assurance model is applied to provide a coordinated approach to all assurance activities.					
						ensure that the combined assurance is received is appropriate to address all the significant risks facing the company.					
						monitor the relationship between the external assurance providers and the company.					
						The audit committee should be an integral component of the risk management process.					
						The charter of the audit committee should set out its responsibilities regarding risk management.					
						The audit committee should specifically have oversight of:					
						financial reporting risks;					
						internal financial controls;					
						fraud risks as it relates to financial reporting; and					
						IT risks as it relates to financial reporting.					
						The audit committee should also:					
						ensure that a combined assurance model is applied to provide a coordinated approach to all assurance activities	King III	3.5			Integrated assurance committee charter
						ensure that the combined assurance is received is appropriate to address all the significant risks facing the company.		3.5.1			
				3.5.2							
			Models & tools: the organisation's processes, methods and tools to be used for managing risk.	ISO 31000	4.3.5 & 5.7				To assess and decide on standardised tools that should be used across the organisation.	Risk identification tools	
										Risk analysis tools	
										Risk evaluation tools	
										Risk treatment tools	
										Risk monitoring tools	
										Risk reporting tools	
			Templates: standardised recording, reporting and assessment templates.	Researcher						To standardise policy, framework, recording, reporting and assessment templates.	Models
											Examples:
											Risk management plan
											Risk communication plan
											Stakeholder maps
											Stakeholder register
Risk register											
Risk improvement report											
Integrated assurance dashboard											
Integrated report											
Risk self-assessments											
Stewardship report											
								Recording process			

Addendum A: Conceptual ERM implementation model: theoretical frameworks, building blocks, best practice requirements and proposed deliverables

Theoretical frameworks		Building blocks	Best practice requirements						Proposed deliverables		
Deming cycle	Weisbord organisational design model		Level 1	Source	Ref.	Level 2	Source	Ref.	Purpose	Deliverables	
Plan	Helping mechanisms, Relationships, Rewards	IV. Develop the risk infrastructure.	Processes: documented processes and procedures.	ISO 31000 / King III	4.3.4 & 4.3.5 / 4.4.1				To embed risk management in all the organisation's practices and processes in a way that it is relevant, effective and efficient.	Common risk language	
										Risk owners matrix	
										Strategic planning process	
										Business planing process	
										Financial planning process	
										Change management process	
										Quality assurance process	
			Risk management process								
	Risk & incident escalation process										
			Systems: information and knowledge management systems.	ISO 31000 / King III	4.3.5 & 5.7 / 4.4.1				To select the most appropriate risk management systems.	Risk recording	
										Risk reporting	
										Risk monitoring	
										Risk review	
Do	Leadership, Structure, Relationships, Helping Mechanisms, External environment	V. Implementation.	Implementing the framework for managing risk.	ISO 31000	4.4.1	Define the appropriate timing and strategy for implementing the framework;	ISO 31000	4.4.1	To establish a time line for risk management activities.	Risk management plan (calendar)	
						Apply the risk management policy and process to the organisational processes;			To embed risk management in all the organisation's practices and processes in a way that it is relevant, effective and efficient.	Integration of the risk into organisational processes	
						Comply with legal and regulatory requirements;			To communicate risk related compliance requirements.	Legal, regulatory & best practice compliance register (pertaining to risk)	
						Ensure that decision making, including the development and setting of objectives, is aligned with the outcomes of risk management processes;				To encourage a risk mind-set for decision making.	Risk appetite statements
						Hold information and training sessions; and				To create a common risk language, improve risk awareness and encourage risk based decision making.	Risk tolerance levels
											Risk awareness gap analysis
			Communicate and consult with stakeholders to ensure that its risk management framework remains appropriate.	ISO 31000	4.2 & 4.4.1	To ensure that the risk management framework remains appropriate.	Risk maturity model				
							Risk awareness plan				
							Risk facilitation sessions				
			Implementing the risk management process.	ISO 31000	4.4.2	Step 1: Communication and consultation with external and internal stakeholders should take place during all stages of the risk management process.	ISO 31000	5.2	To identify the internal and external stakeholders for the organisation / division / department / project.	Stakeholder analysis	
									To identify the most appropriate communication tools and establish timelines.	Risk communication plan	
									To ensure that the right information reaches the right people at the right time.	Risk reports e.g. stress tests, risk & control self-assessments, incident reports, risk treatment plans, key risk indicator reports.	
									Step 2: Establish the context (Know your organisation / division / department / project / risk type)	ISO 31000	5.3

Addendum A: Conceptual ERM implementation model: theoretical frameworks, building blocks, best practice requirements and proposed deliverables

Theoretical frameworks		Building blocks	Best practice requirements						Proposed deliverables	
Deming cycle	Weisbord organisational design model		Level 1	Source	Ref.	Level 2	Source	Ref.	Purpose	Deliverables
Do	Leadership, Structure, Relationships, Helping Mechanisms, External environment	V. Implementation.	Implementing the risk management process.	ISO 31000	4.4.2	Establish the external context	ISO 31000	5.3.2 & 4.3.1	To describe the UNIQUE context for the risk management project.	External stakeholder register
						Establish the internal context		5.3.3 & 4.3.1		External stakeholder map
						Establishing the context of the risk management process		5.3.4 & 4.3.1		Internal value chain mind map
						Apply the risk criteria		5.3.5 & 4.3.1		Internal stakeholder register
						Step 3: Risk identification	ISO 31000	5.4.2		Internal stakeholder map
							King III	4.5		Standardised risk management context (refer to building block III)
										Standardised risk criteria (refer to building block III)
						Step 4: Risk analysis	ISO 31000	5.4.3	Process of finding, recognising and describing risks.	Key / Principle / Strategic risk register
							King III	4.5		Divisional / departmental / business unit risk register
										Emerging risk register
						Step 5: Risk evaluation	ISO 31000	5.4.4	Process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable.	Key / Principle / Strategic risk register - risk ratings applied
							King III	4.5		Divisional / departmental / business unit risk register - risk ratings applied
										Key / Principle / Strategic risk profile - risk ratings + current controls applied & risk owners identified
					Step 6: Risk treatment		ISO 31000	5.5	To identify the most appropriate risk treatment for the most significant risks.	Divisional / departmental / business unit risk register risk ratings + current controls applied & risk owners identified
							King III	4.7		List of risk controls
										Risk treatment plans
Check	Rewards	VI. Monitor & review.	Monitoring activities by the Board.			The board should ensure continual risk monitoring by management	King III	4.8	To ensure proper risk oversight.	Risk governance framework
						The board should ensure that effective and continual monitoring of risk management takes place.		4.8.1	To reduce role confusion and provide clear guidelines for risk monitoring.	Risk management plan (monitoring roles and responsibilities)
						The responsibility for monitoring should be defined in the risk management plan.		4.8.2	To periodically measure progress against, and deviation from, the risk management plan.	Status on risk management plan implementation
			Review activities by the Board.	King III	4.1 & 4.3	The board should comment in the integrated report on the effectiveness of the system and process of risk management.	King III	4.1.2	To periodically review whether the risk management framework, policy and plan are still appropriate, given the organisations' external and internal context;	Integrated report (risk and opportunities section)
						The board should ensure that the implementation of the risk management plan is monitored continually.	King III	4.1.8	To periodically measure progress against, and deviation from, the risk management plan.	Risk management plan implementation status report
						The board should review the implementation of the risk management plan at least once a year.	King III	4.1.9		Risk management plan implementation status report
						The performance of the committee should be evaluated once a year by the board.	King III	4.3.3	To ensure effectiveness and efficiency with regards to committee activities.	Board risk committee performance evaluation

Addendum A: Conceptual ERM implementation model: theoretical frameworks, building blocks, best practice requirements and proposed deliverables

Theoretical frameworks		Building blocks	Best practice requirements						Proposed deliverables	
Deming cycle	Weisbord organisational design model		Level 1	Source	Ref.	Level 2	Source	Ref.	Purpose	Deliverables
Check	Rewards	VI. Monitor & review.	Monitor the risk management framework.			The board should monitor that risks taken are within the tolerance and appetite levels.	King III	4.2.3	To ensure compliance with the risk appetite framework.	Risk appetite status report
						To ensure compliance with the risk tolerance levels.		Risk tolerance status report		
						Measure risk management performance against indicators, which are periodically reviewed for appropriateness;	ISO 31000	4.5	To measure risk management performance against indicators, which are periodically reviewed for appropriateness;	KRI performance report
						Periodically measure progress against, and deviation from, the risk management plan;			To periodically measure progress against, and deviation from, the risk management plan.	Risk management plan implementation status report
						Report on risk, progress with the risk management plan and how well the risk management policy is being followed;			To report on risk, progress with the risk management plan and how well the risk management policy is being followed.	Risk management policy compliance report
			Monitor the level of risk awareness	Researcher		To track the improvement of risk awareness.	Risk culture surveys			
			Review the risk management framework.			Periodically review whether the risk management framework, policy and plan are still appropriate, given the organizations' external and internal context;	ISO 31000	4.5	To periodically review whether the risk management framework, policy and plan are still appropriate, given the organisations' external and internal context.	Risk improvement report
						Communicate and consult with stakeholders to ensure that its risk management framework remains appropriate.	ISO 31000	4.2 & 4.4.1		Risk improvement report
						Review the effectiveness of the risk management framework.	ISO 31000	4.5		Risk improvement report
			Monitor the risk management process.	ISO 31000	5.6	Ensuring that controls are effective and efficient in both design and operation.	ISO 31000	5.6	To ensure that controls are effective and efficient in both design and operation.	Risk treatment plans
						Identifying emerging risks.	ISO 31000	5.6	To identify emerging risks in the organisation's internal value chain and external environment.	Emerging risk register
			Review the risk management process.	ISO 31000	5.6	Analysing and learning lessons from events (including near-misses), changes, trends, successes and failures;	ISO 31000	5.6	To analyse and learn lessons from events (including near-misses), changes, trends, successes and failures.	Variance and trend analysis

Addendum A: Conceptual ERM implementation model: theoretical frameworks, building blocks, best practice requirements and proposed deliverables

Theoretical frameworks		Building blocks	Best practice requirements						Proposed deliverables	
Deming cycle	Weisbord organisational design model		Level 1	Source	Ref.	Level 2	Source	Ref.	Purpose	Deliverables
Adjust	PDCA	VII. Continual improvement.	The board should receive assurance regarding the effectiveness of the risk management process.	King III	4.9	Management should provide assurance to the board that the risk management plan is integrated in the daily activities of the company.	King III	4.9.1	To inform the relevant committees and risk stakeholders of the level of assurance provided by assurance providers.	Integrated assurance report.
						Internal audit should:			To periodically review whether the risk management framework, policy and plan are still appropriate, given the organisations' external and internal context;	
						provide a written assessment of the effectiveness of the system of internal controls and risk management to the board.	King III	4.9.2		Risk improvement report
						detect changes in the external and internal context, including changes to risk criteria and the risk itself which can require revision of risk treatments and priorities; and	ISO 31000	5.6		Risk improvement report (List of internal, external, risk management process & risk criteria context changes)
						obtaining further information to improve risk assessment.		5.6		Risk improvement report (risk assessment process & methodology)

Source: Researcher's own compilation

Addendum B: ERM implementation assessment tool - level of implementation checklist

Theoretical frameworks		Building blocks	Best practice requirements		Proposed deliverables		Building Block	Responsi- bility	Implemented (Mark the appropriate field with 1)		Corrective Actions		
Deming cycle	Weisbord organisational design model				Purpose	Deliverables			Yes	No	Activities	Responsibility	Target Date
Plan	Purpose, Leadership	I. Formalise the instruction and get permission.	Instruction / Trigger	Business trigger e.g. event, merger & acquisition due diligence requirement, peer pressure, etc.	To motivate the need for an ERM program.	Business case document	I						
				Ensure legal and regulatory compliance.	To motivate the need for an ERM program.	Compliance register (legal + regulatory + best practise frameworks)	I						
			Permission / Mandate	The board should delegate to management the responsibility to design, implement and monitor the risk management plan.	To ask for permission / mandate to design and implement the ERM program.	Agenda item for the decision making forum e.g. Board meeting, Executive committee meeting.	I						
					To record the permission / mandate received to design and implement an ERM program.	Minutes of the decision making forum e.g. Board meeting, Executive committee meeting.	I						
			Oversight: the risk committee or audit committee should assist the board in carrying out its risk responsibilities	The board should appoint a committee responsible for risk.	To assist the board in carrying out its risk roles and responsibilities.	Board risk committee (BRC) terms of reference / Audit committee charter / Audit and risk committee charter	I						
				The risk committee should:									
				consider the risk management policy and plan and monitor the risk management process;									
				have as its members executive and non-executive directors, members of senior management and independent risk management experts to be invited, if necessary;									
				have a minimum of three members; and									
				convene at least twice per year.									
				The board's responsibility for risk governance should be expressed in the board charter.									
			Define and endorse the risk management policy	The board's responsibility for risk governance should manifest in a documented risk management policy and plan.	To document risk management scope, objectives and roles and responsibilities.	Risk management policy	I						
				The board should approve the risk management policy and plan.									
				The risk management policy should be widely distributed throughout the company.									

Addendum B: ERM implementation assessment tool - level of implementation checklist

Theoretical frameworks		Building blocks	Best practice requirements		Proposed deliverables		Building Block	Responsi- bility	Implemented (Mark the appropriate field with 1)		Corrective Actions		
Deming cycle	Weisbord organisational design model				Purpose	Deliverables			Yes	No	Activities	Responsibility	Target Date
Plan	Leadership, Relationships	II. Establish the tone of the organisation.	Establishing the tone of the organisation: The introduction of risk management and ensuring its ongoing effectiveness require strong and sustained commitment by management of the organisation, as well as strategic and rigorous planning to achieve commitment at all levels.	The CRO should be a suitably experienced person who should have access and interact regularly on strategic matters with the board and/or appropriate board committee and executive management.	A senior level ERM program sponsor / Chief Risk Officer should have clear authority over and accountability for oversight of risk across the enterprise	CRO / Senior level project sponsor	II						
				(a) Ensure that the organisation's culture and risk management policy are aligned.	To create risk awareness at all levels of the organisations and to encourage risk based decision making.	Risk management policy / Risk requirements evident in business, project and HR requirements and standards / Strategic intent document / Risk communication strategy / Internal audit reports / External audit report / Insurance claims	II						
			(b) Determine risk management performance indicators that align with performance indicators of the organisation.	To measure risk management performance against indicators, which are periodically reviewed for appropriateness;	Performance indicators (Key risk indicators)	II							
			(c) Align risk management objectives with the objectives and strategies of the organisation.	To encourage a risk mind-set for decision making.	Strategic plan / Business plan / Risk plan / Risk management objectives / Risk appetite statement / Risk tolerance levels	II							
			(d) Assign accountabilities and responsibilities at appropriate levels within the organisation.	To reduce role confusion by establishing clear roles and responsibilities for risk activities across businesses and risk types.	Risk governance model: (incl. risk owners' matrix, roles & responsibilities, reporting & escalation process & incentives guidelines & individual performance scorecard.)	II							
(e) Ensure that the necessary resources are allocated to risk management.	To ensure the effective and efficient implementation of the ERM program.	Risk management plan (People, Processes and Budget) / Annual performance plan / Operational budget	II										
(f) Communicate the benefits of risk management to all stakeholders.	To raise risk awareness and create excitement for the project.	Risk training material / Business case / Risk management policy / Embedded in risk reports / Board risk report	II										
The induction and ongoing training programs of the board should incorporate risk governance. (Note: apply to all the levels in the organisation)		To create a common risk language, improve risk awareness and encourage risk based decision making.	Risk awareness gap analysis	II									
			Risk maturity assessment	II									
			Risk awareness strategy & plan	II									
Plan	Purpose, Relationships, Structure, External environment	III. Design the rules of the game.	Design the risk management framework.	Task: Understanding the organisation and its context (Know your organisation)	To get an overall picture of the external environment based PESTLE and / or Porter's 5 forces.								
				Establish the external context:									
				(a) the social and cultural, political, legal, regulatory, financial, technological, economic, natural and competitive environment, whether international, national, regional or local;		Environmental scanning report	III						
				(b) key drivers and trends having impact on the objectives of the organisation; and		Key business drivers report	III						
				(c) External stakeholder analysis		Stakeholder analysis	III						
				Establish the internal context:									
				(a) Governance, organisational structure, roles and accountabilities;		To describe the internal value chain of the organisation and to identify areas that would create risks and opportunities	Environmental scanning of the INTERNAL value chain	III					
							SWOT analysis	III					
							Organisational organigram	III					
							Divisional organigram	III					
							Departmental organigram	III					
							Delegation of authority	III					
							Committee structure	III					
							Committee charters	III					
							List of policies	III					
							Copy of policies	III					
				(b) Policies, objectives, and the strategies that are in place to achieve them;	Action plans (strategies)	III							
				(c) Capabilities, understood in terms of resources and knowledge (e.g. capital, time, people, processes, systems and	Risk competency model	III							
				(d) Information systems, information flows and decision making processes (both formal and informal)	Job profiles / specification	III							
					Technical job specs	III							
					List of systems	III							
					Process maps	III							
					Escalation policy	III							
					Escalation process	III							
					Connected stakeholder analysis	III							
					(e) Internal stakeholder analysis	III							
					(f) Temperature checks on organisational culture	Organisational culture survey results	III						

Addendum B: ERM implementation assessment tool - level of implementation checklist

Theoretical frameworks		Building blocks	Best practice requirements		Proposed deliverables		Building Block	Responsi- bility	Implemented (Mark the appropriate field with 1)		Corrective Actions			
Deming cycle	Weisbord organisational design model		Level 1	Level 2	Purpose	Deliverables			Yes	No	Activities	Responsibility	Target Date	
Plan	Purpose, Relationships, Structure, External environment	III. Design the rules of the game.	Design the risk management framework.	(g) Standards, guidelines and models adopted by the organisation; and	To describe the internal value chain of the organisation and to identify areas that would create risks and opportunities	List of standards, guidelines and models	III							
				(h) the form and extent of contractual relationships.		Contracts register	III							
						Internal audit reports	III							
						External audit reports	III							
						Strategic plan	III							
						Business plans	III							
				Establish the context of the risk management process (The context of the risk management process will vary according to the needs of an organisation. It can involve, but is not limited to:	To create ONE set of risk management rules for the organisation.	Risk management file / manual that includes:								
				(a) Defining the goals and objectives of the risk management activities;		Risk management goals & -objectives	III							
				(b) Defining responsibilities for and within the risk management process;		Risk governance model	III							
				(c) Defining the scope, as well as the depth and breadth of the risk management activities to be carried out, including specific		Top-down & Bottom-up risk management activities	III							
				(e) Defining the activity, process, function, project, product, service or asset in terms of time and location;										
				(f) Defining the relationships between a particular project, process or activity and other projects, processes or activities of the organisation;		Interconnectedness maps	III							
				(g) Defining the risk assessment methodologies;		Risk assessment methodologies	III							
				(h) Defining the way performance and effectiveness is evaluated in the management of risk;		Key risk indicators	III							
				(i) Identifying and specifying the decisions that have to be made; and		Decision matrix	III							
				(j) Identifying, scoping or framing studies needed, their extent and objectives, and the resources required for such studies.		Research to clarify context	III							
				Define the risk criteria (When defining risk criteria, factors to be considered should include the following:	To create standardised risk assessment criteria for the organisation as a whole. To give risk owners and other risk stakeholders insight into risk management in their terms.	Risk management file / manual that includes:								
				(a) The nature and types of causes and consequences that can occur and how they will be measured;		Examples of causes and consequences	III							
				(b) How likelihood will be defined;		Risk assessment tools and techniques	III							
				(c) The timeframe(s) of the likelihood and/or consequence(s);		Risk management plan	III							
				(d) How the level of risk is to be determined;		Risk appetite guidelines	III							
				(e) The views of stakeholders;		Risk tolerance levels guidelines	III							
				(f) The level at which risk becomes acceptable or tolerable; and										
				(g) Whether combinations of multiple risks should be taken into account and, if so, how and which combinations should be considered.										
				Task: establishing the risk management policy	To document risk management scope, objectives and roles and responsibilities.	Risk management policy	III							
				(a) A policy and plan for a system and process of risk management should be developed.										
				(c) The board's responsibility for risk governance should manifest in a documented risk management policy and plan.										
				(d) The board should approve the risk management policy and plan.										
				The risk management policy should be widely distributed throughout the company.										
				Task: develop an accountability matrix / risk governance framework	To establish clear roles and responsibilities for risk activities across businesses and risk types.	Risk governance framework: (incl. risk owners' matrix, roles & responsibilities, reporting & escalation process & incentives guidelines & individual performance scorecards)								
(a) Identifying risk owners that have the accountability and authority to manage risks;														

Addendum B: ERM implementation assessment tool - level of implementation checklist

Theoretical frameworks		Building blocks	Best practice requirements		Proposed deliverables		Building Block	Responsi- bility	Implemented (Mark the appropriate field with 1)		Corrective Actions				
Deming cycle	Weisbord organisational design model				Purpose	Deliverables			Yes	No	Activities	Responsibility	Target Date		
Plan	Purpose, Relationships, Structure, External environment	III. Design the rules of the game.	Level 1	Level 2	(b) Identifying who is accountable for the development, implementation and maintenance of the framework for managing risk;	To establish clear roles and responsibilities for risk activities across businesses and risk types.	Risk governance framework: (incl. risk owners' matrix, roles & responsibilities, reporting & escalation process & incentives guidelines & individual performance scorecards)	III							
														(c) Identifying other responsibilities of people at all levels in the organisation for the risk management process;	
														(d) Establishing performance measurement and external and/or internal reporting and escalation processes; and	
														(e) Ensuring appropriate levels of recognition.	
					Task: integration into organisational processes		To embed risk management in all the organisation's practices and processes in a way that it is relevant, effective and efficient.								
					Develop a common risk language			Common risk language	III						
					Risk management should be embedded in all the organisation's practices and processes in a way that it is relevant, effective and efficient.			Risk owners	III						
								Strategic plan	III						
								Business plan	III						
								Financial plan	III						
								Risk & incident escalation process	III						
								New products development	III						
								Operational processes	III						
								Investment decisions	III						
								Combined assurance	III						
								Performance management process	III						
								Change management process	III						
								Quality assurance process	III						
					Align risk management objectives with the objectives and strategies of the organisation.		To encourage a risk mind-set for decision making.	Risk appetite guidelines	III						
					Determine risk management performance indicators that align with performance indicators of the organisation.		To measure risk management performance against indicators, which are periodically reviewed for appropriateness;	Risk tolerance levels guidelines	III						
								Strategic plans	III						
					Task: Establishing internal communication and reporting mechanisms		To create one set of rules for risk communication and also to increase risk transparency.	Business plans	III						
								Performance reporting metrics, i.e. key risk indicators	III						
					Task: Establishing internal communication and reporting mechanisms		To create one set of rules for risk communication and also to increase risk transparency.	Internal reporting guidelines	III						
					(a) Key components of the risk management framework, and any subsequent modifications, are communicated appropriately;			Communication guidelines	III						
					(b) there is adequate internal reporting on the framework, its effectiveness and the outcomes;										
					(c) relevant information derived from the application of risk management is available at appropriate levels and times; and										
					(d) there are processes for consultation with internal stakeholders.										
					Task: Establishing external communication and reporting mechanisms		To create one set of rules for risk communication and also to increase risk transparency.		III						
					(a) Engaging appropriate external stakeholders and ensuring an effective exchange of information;			External reporting guidelines							
					(b) External reporting to comply with legal, regulatory, and governance requirements;			Communication guidelines	III						
					(c) Providing feedback and reporting on communication and consultation;										
Design the risk management process.	Step 1: Communication and consultation	To develop a standardised risk management process for the organisation.	Risk management process guidelines	III											
	Step 2: Establish the context														
	Step 3: Risk identification														
	Step 4: Risk analysis														
	Step 5: Risk evaluation														
	Step 6: Risk treatment														
	Step 7: Monitor and review														
	Step 8: Continuous improvement														

Addendum B: ERM implementation assessment tool - level of implementation checklist

Theoretical frameworks		Building blocks	Best practice requirements		Proposed deliverables		Building Block	Responsi- bility	Implemented (Mark the appropriate field with 1)		Corrective Actions		
Deming cycle	Weisbord organisational design model				Purpose	Deliverables			Yes	No	Activities	Responsibility	Target Date
Plan	Helping mechanisms, Relationships, Rewards	IV. Develop the risk infrastructure.	Task: Allocate appropriate resources for risk management										
			People (skills, experience, competence & training programs).	People: skills, experience, competence & training programs	To establish decision making structures, escalation protocol & identify risk stakeholders.	Risk governance models	IV						
						Performance management scorecards	IV						
					To identify competencies, skills levels and experience required by risk stakeholders.	Job profiles	IV						
					To ensure proper training for risk stakeholders.	Risk training: induction sessions and risk awareness sessions	IV						
			Committees: the board should delegate certain functions to well-structured committees but without abdicating its own responsibilities.	Board committees:	To formalise decision making structures, escalation protocol & identify risk stakeholders.								
				Formal terms of reference should be established and approved for each committee of the board.		Board committees charter / terms of reference	IV						
				The committees' terms of reference should be reviewed yearly.									
				The committees should be appropriately constituted and the composition and the terms of reference should be disclosed in the integrated report.		Integrated report	IV						
				The risk committee should:		Risk committees:							
				consider the risk management policy and plan and monitor the risk management process;		Board risk committee terms of reference	IV						
				have as its members executive and non-executive directors, members of senior management and independent risk management experts to be invited, if necessary;		Executive risk committee terms of reference	IV						
				have a minimum of three members; and		Departmental risk committee terms of reference	IV						
				convene at least twice per year.		Audit and risk committee	IV						
				The audit committee should:		Audit committee charter	IV						
				oversee integrated reporting.									
				have regard to all factors and risks that may impact on the integrity of the integrated report.									
				review and comment on the financial statements included in the integrated report.									
				review the disclosure of sustainability issues in the integrated report to ensure that it is reliable and does not conflict with the financial information.									
				recommend to the board to engage an external assurance provider on material sustainability issues.									
				consider the need to issue interim results.									
				review the content of the summarised information.									
				engage the external auditors to provide assurance on the summarised financial information.									
				ensure that a combined assurance model is applied to provide a coordinated approach to all assurance activities.									
				ensure that the combined assurance is received is appropriate to address all the significant risks facing the company.									
				monitor the relationship between the external assurance providers and the company.									
				The audit committee should be an integral component of the risk management process.									
				The charter of the audit committee should set out its responsibilities regarding risk management.									
				The audit committee should specifically have oversight of:									
				financial reporting risks;									
				internal financial controls;									

Addendum B: ERM implementation assessment tool - level of implementation checklist

Theoretical frameworks		Building blocks	Best practice requirements		Proposed deliverables		Building Block	Responsi- bility	Implemented (Mark the appropriate field with 1)		Corrective Actions		
Deming cycle	Weisbord organisational design model		Level 1	Level 2	Purpose	Deliverables			Yes	No	Activities	Responsibility	Target Date
Plan	Helping mechanisms, Relationships, Rewards	IV. Develop the risk infrastructure.	Committees: the board should delegate certain functions to well-structured committees but without abdicating its own responsibilities.	fraud risks as it relates to financial reporting; and	To formalise decision making structures, escalation protocol & identify risk stakeholders.	Audit committee charter	IV						
				IT risks as it relates to financial reporting.		Combined assurance committee terms of reference	IV						
				The audit committee should also:									
				ensure that a combined assurance model is applied to provide a coordinated approach to all assurance activities									
				ensure that the combined assurance is received is appropriate to address all the significant risks facing the company.		Risk specific committee terms of reference e.g. Fraud risk committee	IV						
			Models & tools: the organisation's processes, methods and tools to be used for managing risk		To assess and decide on standardised tools that should be used across the organisation.	Risk identification tools	IV						
						Risk analysis tools	IV						
						Risk evaluation tools	IV						
						Risk response tools	IV						
						Risk monitoring tools	IV						
						Risk reporting tools	IV						
						Risk quantification models	IV						
			Templates: standardised recording, reporting and assessment templates		To standardise policy, framework, recording, reporting and assessment templates.	Examples:							
						Risk management plan	IV						
						Risk communication plan	IV						
						Stakeholder maps	IV						
						Stakeholder register	IV						
						Risk register	IV						
						Risk improvement report	IV						
						Integrated assurance dashboard	IV						
						Integrated report	IV						
						Risk self-assessments	IV						
						Stewardship report	IV						
						Recording process	IV						
						Risk acceptance form	IV						
						Risk retirement form	IV						
						Reporting dashboards	IV						
						Reporting scorecards	IV						
						Risk policy	IV						
						Risk management framework	IV						
						Risk committee terms of reference	IV						
			Processes: documented processes and procedures.		To embed risk management in all the organisation's practices and processes in a way that it is relevant, effective and efficient.	Common risk language	IV						
						Risk owners matrix	IV						
						Strategic planning process	IV						
						Business planing process	IV						
						Financial planning process	IV						
						Change management process	IV						
						Quality assurance process	IV						
						Risk management process	IV						
						Risk & incident escalation process	IV						
						External audit process	IV						
			Systems: information and knowledge management systems		To select the most appropriate risk management systems.	Performance management process	IV						
						Risk recording	IV						
						Risk reporting	IV						
						Risk monitoring	IV						
						Risk review	IV						
Do	Leadership, Structure, Relationships, Helping Mechanisms, External environment	V. Implement the ERM program.	Implementing the framework for managing risk.	Define the appropriate timing and strategy for implementing the framework;	To establish a time line for risk management activities.	Risk management plan (calendar)	V						
						Cristical path analysis for key dependencies	V						
			Apply the risk management policy and process to the organisational processes;	To embed risk management in all the organisation's practices and processes in a way that it is relevant, effective and efficient.		Common risk language	V						
						Risk owners matrix	V						
						Strategic planning process	V						
						Business planing process	V						
						Financial planning process	V						
						Change management process	V						
						Quality assurance process	V						

Addendum B: ERM implementation assessment tool - level of implementation checklist

Theoretical frameworks		Building blocks	Best practice requirements		Proposed deliverables		Building Block	Responsi- bility	Implemented (Mark the appropriate field with 1)		Corrective Actions			
Deming cycle	Weisbord organisational design model				Purpose	Deliverables			Yes	No	Activities	Responsibility	Target Date	
Do	Leadership, Structure, Relationships, Helping Mechanisms, External environment	V. Implement the ERM program.	Implementing the framework for managing risk.	Apply the risk management policy and process to the organisational processes;	To embed risk management in all the organisation's practices and processes in a way that it is relevant, effective and efficient.	Risk management process	V							
						Risk & incident escalation process	V							
						Performance management process	V							
				Comply with legal and regulatory requirements;	To communicate risk related compliance requirements.	Legal, regulatory & best practice compliance register (pertaining to risk)	V							
					Ensure that decision making, including the development and setting of objectives, is aligned with the outcomes of risk management processes;	To encourage a risk mind-set for decision making.	Risk appetite statements	V						
							Risk tolerance levels	V						
							Strategic plan	V						
						ERM framework & policy	V							
				Hold information and training sessions; and	To create a common risk language, improve risk awareness and encourage risk based decision making.	Risk awareness gap analysis	V							
						Risk maturity assessment	V							
						Risk awareness strategy & -plan	V							
				To ensure that the risk management framework remains appropriate.	Risk facilitation sessions	V								
			Implementing the risk management process.	Step 1: Communication and consultation with external and internal stakeholders should take place during all stages of the risk management process.	To identify the internal and external stakeholders for the organisation / division / department / project.	Stakeholder analysis	V							
					To identify the most appropriate communication tools and establish timelines.	Risk communication plan	V							
					To ensure that the right information reaches the right people at the right time.	Risk reports e.g. stress tests, risk & control self-assessments, incident reports, risk treatment plans, key risk indicator reports.	V							
				Step 2: Establish the context (Know your organisation / division / department / project / risk type)	To describe the UNIQUE context for the risk management project.									
						Establish the external context	External environment mind map	V						
							External stakeholder register	V						
							External stakeholder map	V						
				Establish the internal context		Internal value chain mind map	V							
							Internal stakeholder register	V						
						Internal stakeholder map	V							
				Establishing the context of the risk management process		Standardised risk management context (refer to building block III)	V							
					Apply the risk criteria	Standardised risk criteria (refer to building block III)	V							
				Step 3: Risk identification	Process of finding, recognising and describing risks.	Key / Principle / Strategic risk register	V							
						Divisional / departmental / business unit risk register	V							
						Emerging risk register	V							
						Risk library	V							
				Step 4: Risk analysis	Process to comprehend the nature of risk and to determine the level of risk (e.g. high, medium, low).									
						Key / Principle / Strategic risk register - risk ratings applied	V							
						Divisional / departmental / business unit risk register - risk ratings applied	V							
						Root cause analysis	V							
				Step 5: Risk evaluation	Process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable.	Key / Principle / Strategic risk profile - risk ratings + current controls applied & risk owners identified	V							
						Divisional / departmental / business unit risk register risk ratings + current controls applied & risk owners identified	V							
				Step 6: Risk response	To identify the most appropriate risk treatment for the most significant risks.	Controls library	V							
			Risk response plans / Action plans			V								
Risk response options	V													

Addendum B: ERM implementation assessment tool - level of implementation checklist

Theoretical frameworks		Building blocks	Best practice requirements		Proposed deliverables		Building Block	Responsi- bility	Implemented (Mark the appropriate field with 1)		Corrective Actions		
Deming cycle	Weisbord organisational design model				Purpose	Deliverables			Yes	No	Activities	Responsibility	Target Date
Check	Rewards	VI. Monitor and review the ERM program.	Monitoring activities by the Board	The board should ensure continual risk monitoring by management	To ensure proper risk oversight.	Risk governance framework	VI						
				The board should ensure that effective and continual monitoring of risk management takes place.	To reduce role confusion and provide clear guidelines for risk monitoring.	Risk management plan (monitoring roles and responsibilities)	VI						
				The responsibility for monitoring should be defined in the risk management plan.	To periodically measure progress against, and deviation from, the risk management plan.	Status report on risk management plan implementation	VI						
			Review activities by the Board	The board should comment in the integrated report on the effectiveness of the system and process of risk management.	To periodically review whether the risk management framework, policy and plan are still appropriate, given the organisations' external and internal context;	Integrated report (risk and opportunities section)	VI						
						Annual board risk report	VI						
				The board should ensure that effective and continual monitoring of risk management takes place.	To periodically measure progress against, and deviation from, the risk management plan.	Risk management plan implementation status report	VI						
					The board should review the implementation of the risk management plan at least once a year.	To periodically review whether the risk management framework, policy and plan are still appropriate, given the organisations' external and internal context;	Risk improvement report	VI					
						Internal audit report	VI						
				Monitor the risk management framework	The performance of the committee should be evaluated once a year by the board.	To ensure effectiveness and efficiency with regards to committee activities.	Board risk committee performance evaluation	VI					
			The board should monitor that risks taken are within the tolerance and appetite levels.		To ensure compliance with the risk appetite framework.	Risk appetite status report	VI						
					To ensure compliance with the risk tolerance levels.	Risk tolerance status report	VI						
			Measure risk management performance against indicators, which are periodically reviewed for appropriateness;		To measure risk management performance against indicators, which are periodically reviewed for appropriateness;	KRI performance report	VI						
			Periodically measure progress against, and deviation from, the risk management plan;		To periodically measure progress against, and deviation from, the risk management plan.	Risk management plan implementation status report	VI						
			Report on risk, progress with the risk management plan and how well the risk management policy is being followed;		To report on risk, progress with the risk management plan and how well the risk management policy is being followed.	Risk management policy compliance report	VI						
						Deviations from risk management policy report	VI						
			Monitor the level of risk awareness	To track the improvement of risk awareness.	Risk culture surveys	VI							
			Review the risk management framework	Periodically review whether the risk management framework, policy and plan are still appropriate, given the organizations' external and internal context;		Risk improvement report	VI						
						Internal audit report	VI						
						Risk calendar	VI						
				Communicate and consult with stakeholders to ensure that its risk management framework remains appropriate.	To periodically review whether the risk management framework, policy and plan are still appropriate, given the organisations' external and internal context.	Risk improvement report	VI						
						Subject matter expert gap analysis	VI						
						Internal audit reports	VI						
						Risk calendar	VI						
					ISO 9000 reports	VI							
			Review the effectiveness of the risk management framework.		Internal audit reports, risk committee effectiveness, qualitative conversations, risk appetite and risk tolerance level breaches, signed letters of representation.	VI							
			Monitor the risk management process	Ensuring that controls are effective and efficient in both design and operation.	To ensure that controls are effective and efficient in both design and operation.	Subject matter expert gap analysis	VI						
						Combined assurance reports	VI						
						Risk profile status reports	VI						
						Internal audit reports	VI						
				Identifying emerging risks.	To identify emerging risks in the organisation's internal value chain and external environment.	External audit reports	VI						
						Emerging risk register	VI						
			Review the risk management process	Analysing and learning lessons from events (including near-misses), changes, trends, successes and failures;	To analyse and learn lessons from events (including near-misses), changes, trends, successes and failures.	Variance and trend analysis	VI						
						Post mortem sessions	VI						
						Environmental scanning	VI						
Risk reconciliation reports	VI												
Post loss analysis	VI												

Addendum B: ERM implementation assessment tool - level of implementation checklist

Theoretical frameworks		Building blocks	Best practice requirements		Proposed deliverables		Building Block	Responsi- bility	Implemented (Mark the appropriate field with 1)		Corrective Actions		
Deming cycle	Weisbord organisational design model		Level 1	Level 2	Purpose	Deliverables			Yes	No	Activities	Responsibility	Target Date
Adjust	Leadership, Purposes, Structure, Relationships, Rewards, Helpful mechanisms, External environment	VII. Continual improvement of the ERM program.	The board should receive assurance regarding the effectiveness of the risk management process	Management should provide assurance to the board that the risk management plan is integrated in the daily activities of the company.	To inform the relevant committees and risk stakeholders of the level of assurance provided by assurance providers.	Combined assurance report.	VII						
						Risk reports to various committees	VII						
						Risk maturity assessment	VII						
						Benchmarking assessments (peer reviews & best practice)	VII						
				Internal audit should: ~~provide a written assessment of the effectiveness of the system of internal controls~~	To periodically review whether the risk management framework, policy and plan are still appropriate, given the organisations' external and internal context;								
						Risk improvement report	VII						
				detect changes in the external and internal context, including changes to risk criteria and the risk itself which can require revision of risk treatments and priorities; and		Internal audit report	VII						
						Risk improvement report (List of internal, external, risk management process & risk criteria context changes)	VII						
				obtaining further information to improve risk assessment.		Risk improvement report (risk assessment process & methodology)	VII						

Source: Researcher's own compilation

Addendum C: ERM implementation assessment tool - degree of formality checklist

Theoretical frameworks		Building blocks	Best practice requirements		Proposed deliverables		Building Block	Responsi- bility	Degree of Formality (Mark the appropriate field with 1)				Corrective Actions		
Deming cycle	Weisbord organisational design model		Level 1	Level 2	Purpose	Deliverables			YES	Not started	In process	Done	Activities	Responsibility	Target Date
Plan	Purpose, Leadership	I. Formalise the instruction and get permission.	Instruction / Trigger	Business trigger e.g. event, merger & acquisition due diligence requirement, peer pressure, etc.	To motivate the need for an ERM program.	Business case document	I		1						
				Ensure legal and regulatory compliance.	To motivate the need for an ERM program.	Compliance register (legal + regulatory + best practise frameworks)	I		1						
			Permission / Mandate	The board should delegate to management the responsibility to design, implement and monitor the risk management plan.	To ask for permission / mandate to design and implement the ERM program.	Agenda item for the decision making forum e.g. Board meeting, Executive committee meeting.	I		1						
					To record the permission / mandate received to design and implement an ERM program.	Minutes of the decision making forum e.g. Board meeting, Executive committee meeting.	I		1						
			Oversight: the risk committee or audit committee should assist the board in carrying out its risk responsibilities	The board should appoint a committee responsible for risk.	To assist the board in carrying out its risk roles and responsibilities.	Board risk committee (BRC) terms of reference / Audit committee charter / Audit and risk committee charter	I	CRO							
				The risk committee should:											
				consider the risk management policy and plan and monitor the risk management process;											
				have as its members executive and non-executive directors, members of senior management and independent risk management experts to be invited, if necessary;											
				have a minimum of three members; and											
				convene at least twice per year.											
				The board's responsibility for risk governance should be expressed in the board charter.											
			Define and endorse the risk management policy	The board's responsibility for risk governance should manifest in a documented risk management policy and plan.	To document risk management scope, objectives and roles and responsibilities.	Risk management policy	I	CRO							
				The board should approve the risk management policy and plan.											
				The risk management policy should be widely distributed throughout the company.											
Plan	Leadership, Relationships	II. Establish the tone of the organisation.	Establishing the tone of the organisation: The introduction of risk management and ensuring its ongoing effectiveness require strong and sustained commitment by management of the organisation, as well as strategic and rigorous planning to achieve commitment at all levels.	The CRO should be a suitably experienced person who should have access and interact regularly on strategic matters with the board and/or appropriate board committee and executive management.	A senior level ERM program sponsor / Chief Risk Officer should have clear authority over and accountability for oversight of risk across the enterprise	CRO / Senior level project sponsor	II		1						
				(a) Ensure that the organisation's culture and risk management policy are aligned.	To create risk awareness at all levels of the organisations and to encourage risk based decision making.	Risk management policy / Risk requirements evident in business, project and HR requirements and standards / Strategic intent document / Risk communication strategy / Internal audit reports / External audit report / Insurance claims	II	CRO							

Addendum C: ERM implementation assessment tool - degree of formality checklist

Theoretical frameworks		Building blocks	Best practice requirements		Proposed deliverables		Building Block	Responsi- bility		Degree of Formality (Mark the appropriate field with 1)				Corrective Actions		
Deming cycle	Weisbord organisational design model				Purpose	Deliverables				YES	Not started	In process	Done	Activities	Responsibility	Target Date
Plan	Leadership, Relationships	II. Establish the tone of the organisation.	Establishing the tone of the organisation: The introduction of risk management and ensuring its ongoing effectiveness require strong and sustained commitment by management of the organisation, as well as strategic and rigorous planning to achieve commitment at all levels.	(b) Determine risk management performance indicators that align with performance indicators of the organisation.	To measure risk management performance against indicators, which are periodically reviewed for appropriateness;	Performance indicators (Key risk indicators)	II	CRO								
				(c) Align risk management objectives with the objectives and strategies of the organisation.	To encourage a risk mind-set for decision making.	Strategic plan / Business plan / Risk plan / Risk management objectives / Risk appetite statement / Risk tolerance levels	II	CRO								
				(d) Assign accountabilities and responsibilities at appropriate levels within the organisation.	To reduce role confusion by establishing clear roles and responsibilities for risk activities across businesses and risk types.	Risk governance model: (incl. risk owners' matrix, roles & responsibilities, reporting & escalation process & incentives guidelines & individual performance scorecard.)	II		1							
				(e) Ensure that the necessary resources are allocated to risk management.	To ensure the effective and efficient implementation of the ERM program.	Risk management plan (People, Processes and Budget) / Annual performance plan / Operational budget	II		1							
				(f) Communicate the benefits of risk management to all stakeholders.	To raise risk awareness and create excitement for the project.	Risk training material / Business case / Risk management policy / Embedded in risk reports / Board risk report	II		1							
			The induction and ongoing training programmes of the board should incorporate risk governance. (Note: apply to all the levels in the organisation)		To create a common risk language, improve risk awareness and encourage risk based decision making.	Risk awareness gap analysis	II	CRO								
						Risk maturity assessment	II	CRO								
						Risk awareness strategy & plan	II	CRO								
Plan	Purpose, Relationships, Structure, External environment	III. Design the rules of the game.	Design the risk management framework.	Task: Understanding the organisation and its context (Know your organisation)	To get an overall picture of the external environment based PESTLE and / or Porter's 5 forces.											
				Establish the external context:												
				(a) the social and cultural, political, legal, regulatory, financial, technological, economic, natural and competitive environment, whether international, national, regional or local;		Environmental scanning report	III	CRO								
				(b) key drivers and trends having impact on the objectives of the organisation; and		Key business drivers report	III		1							
				(c) External stakeholder analysis		Stakeholder analysis	III		1							
				Establish the internal context:												
				(a) Governance, organisational structure, roles and accountabilities;		Environmental scanning of the INTERNAL value chain	III	CRO (get from CSO)								
						SWOT analysis	III		1							
						Organisational organigram	III		1							
						Divisional organigram	III		1							
						Departmental organigram	III		1							
						Delegation of authority	III		1							
						Committee structure	III		1							
						Committee charters	III		1							
						(b) Policies, objectives, and the strategies that are in place to achieve them;	List of policies	III	CRO (get from Company Secretary)							
				Copy of policies			III	CRO (get from Company Secretary)								
				Action plans (strategies)			III	CRO (get from Company Secretary)								
				(c) Capabilities, understood in terms of resources and knowledge (e.g. capital, time, people, processes, systems and		Risk competency model	III		1							
						Job profiles / specification	III		1							
						Technical job specs	III		1							
				(d) Information systems, information flows and decision making processes (both formal and informal)		List of systems	III	CRO (get from CTO)								
						Process maps	III		1							
						Escalation policy	III		1							
						Escalation process	III		1							
				Connected stakeholder analysis		Connected stakeholder analysis	III	CRO (get from CSO)								
				(e) Internal stakeholder analysis		Internal stakeholder analysis	III		1							
				(f) Temperature checks on organisational culture		Organisational culture survey results	III		1							
(g) Standards, guidelines and models adopted by the organisation; and	List of standards, guidelines and models	III		1												
(h) the form and extent of contractual relationships.	Contracts register	III	CRO (get from CPO)													

Addendum C: ERM implementation assessment tool - degree of formality checklist

Theoretical frameworks		Building blocks	Best practice requirements		Proposed deliverables		Building Block	Responsi- bility	Degree of Formality (Mark the appropriate field with 1)				Corrective Actions		
Deming cycle	Weisbord organisational design model		Level 1	Level 2	Purpose	Deliverables			YES	Not started	In process	Done	Activities	Responsibility	Target Date
Plan	Purpose, Relationships, Structure, External environment	III. Design the rules of the game.	Design the risk management framework.		To describe the internal value chain of the organisation and to identify areas that would create risks and opportunities	Internal audit reports	III		1						
						External audit reports	III		1						
						Strategic plan	III		1						
						Business plans	III	CRO (get from C-LEVELS)							
				Establish the context of the risk management process (The context of the risk management process will vary according to the needs of an organisation. It can involve, but is not limited to:	To create ONE set of risk management rules for the organisation.	Risk management file / manual that includes:									
				(a) Defining the goals and objectives of the risk management activities;		Risk management goals & -objectives	III		1						
				(b) Defining responsibilities for and within the risk management process;		Risk governance model	III		1						
				(c) Defining the scope, as well as the depth and breadth of the risk management activities to be carried out, including specific		Top-down & Bottom-up risk management activities	III		1						
				(e) Defining the activity, process, function, project, product, service or asset in terms of time and location;											
				(f) Defining the relationships between a particular project, process or activity and other projects, processes or activities of the organisation;		Interconnectedness maps	III		1						
				(g) Defining the risk assessment methodologies;		Risk assessment methodologies	III		1						
				(h) Defining the way performance and effectiveness is evaluated in the management of risk;		Key risk indicators	III	CRO							
				(i) Identifying and specifying the decisions that have to be made; and		Decision matrix	III	CRO							
				(j) Identifying, scoping or framing studies needed, their extent and objectives, and the resources required for such studies.		Research to clarify context	III	CRO							
				Define the risk criteria (When defining risk criteria, factors to be considered should include the following:	To create standardised risk assessment criteria for the organisation as a whole. To give risk owners and other risk stakeholders insight into risk management in their terms.	Risk management file / manual that includes:									
				(a) The nature and types of causes and consequences that can occur and how they will be measured;		Examples of causes and consequences	III		1						
				(b) How likelihood will be defined;		Risk assessment tools and techniques	III		1						
				(c) The timeframe(s) of the likelihood and/or consequence(s);		Risk management plan	III	CRO							
				(d) How the level of risk is to be determined;		Risk appetite guidelines	III	CRO							
				(e) The views of stakeholders;		Risk tolerance levels guidelines	III	CRO							
				(f) The level at which risk becomes acceptable or tolerable; and											
				(g) Whether combinations of multiple risks should be taken into account and, if so, how and which combinations should be considered.											
				Task: establishing the risk management policy	To document risk management scope, objectives and roles and responsibilities.	Risk management policy	III	CRO							
				(a) A policy and plan for a system and process of risk management should be developed.											
				(c) The board's responsibility for risk governance should manifest in a documented risk management policy and plan.											
				(d) The board should approve the risk management policy and plan.											
				The risk management policy should be widely distributed throughout the company.											
				Task: develop an accountability matrix / risk governance framework	To establish clear roles and responsibilities for risk activities across businesses and risk types.	Risk governance framework: (incl. risk owners' matrix, roles & responsibilities, reporting & escalation process & incentives guidelines & individual performance scorecards)	III		1						
				(a) Identifying risk owners that have the accountability and authority to manage risks;											
				(b) Identifying who is accountable for the development, implementation and maintenance of the framework for managing risk;											

Addendum C: ERM implementation assessment tool - degree of formality checklist

Theoretical frameworks		Building blocks	Best practice requirements		Proposed deliverables		Building Block	Responsi- bility		Degree of Formality (Mark the appropriate field with 1)				Corrective Actions		
Deming cycle	Weisbord organisational design model				Purpose	Deliverables				YES	Not started	In process	Done	Activities	Responsibility	Target Date
Plan	Purpose, Relationships, Structure, External environment	III. Design the rules of the game.	Design the risk management framework.	(c) Identifying other responsibilities of people at all levels in the organisation for the risk management process;	To establish clear roles and responsibilities for risk activities across businesses and risk types.	Risk governance framework: (incl. risk owners' matrix, roles & responsibilities, reporting & escalation process & incentives guidelines & individual performance scorecards)	III									
				(d) Establishing performance measurement and external and/or internal reporting and escalation processes; and												
				(e) Ensuring appropriate levels of recognition.												
				Task: integration into organisational processes	To embed risk management in all the organisation's practices and processes in a way that it is relevant, effective and efficient.											
				Develop a common risk language		Common risk language	III		1							
				Risk management should be embedded in all the organisation's practices and processes in a way that it is relevant, effective and efficient.		Risk owners	III	CRO								
						Strategic plan	III	CSO								
						Business plan	III	C-LEVELS								
						Financial plan	III	CFO								
						Risk & incident escalation process	III		1							
						New products development	III	CRO								
						Operational processes	III	CRO								
						Investment decisions	III	CRO								
						Combined assurance	III	CRO								
						Performance management process	III	CRO								
						Change management process	III	CHRO								
						Quality assurance process	III	CPO								
				Align risk management objectives with the objectives and strategies of the organisation.	To encourage a risk mind-set for decision making.	Risk appetite guidelines	III	CRO								
						Risk tolerance levels guidelines	III	CRO								
						Strategic plans	III	CSO								
						Business plans	III	C-LEVELS								
				Determine risk management performance indicators that align with performance indicators of the organisation.	To measure risk management performance against indicators, which are periodically reviewed for appropriateness;	Performance reporting metrics, i.e. key risk indicators	III	CRO								
				Task: Establishing internal communication and reporting mechanisms	To create one set of rules for risk communication and also to increase risk transparency.	Internal reporting guidelines	III		1							
				(a) Key components of the risk management framework, and any subsequent modifications, are communicated appropriately;		Communication guidelines	III		1							
				(b) there is adequate internal reporting on the framework, its effectiveness and the outcomes;												
				(c) relevant information derived from the application of risk management is available at appropriate levels and times; and												
				(d) there are processes for consultation with internal stakeholders.												
				Task: Establishing external communication and reporting mechanisms	To create one set of rules for risk communication and also to increase risk transparency.	External reporting guidelines	III		1							
				(a) Engaging appropriate external stakeholders and ensuring an effective exchange of information;		Communication guidelines	III		1							
				(b) External reporting to comply with legal, regulatory, and governance requirements;												
				(c) Providing feedback and reporting on communication and consultation;												
			Design the risk management process.	Step 1: Communication and consultation	To develop a standardised risk management process for the organisation.	Risk management process guidelines	III		1							
				Step 2: Establish the context												
				Step 3: Risk identification												
				Step 4: Risk analysis												
				Step 5: Risk evaluation												
				Step 6: Risk treatment												
				Step 7: Monitor and review												
				Step 8: Continuous improvement												

Addendum C: ERM implementation assessment tool - degree of formality checklist

Theoretical frameworks		Building blocks	Best practice requirements		Proposed deliverables		Building Block	Responsi- bility	Degree of Formality (Mark the appropriate field with 1)				Corrective Actions		
Deming cycle	Weisbord organisational design model		Level 1	Level 2	Purpose	Deliverables			YES	Not started	In process	Done	Activities	Responsibility	Target Date
Plan	Helping mechanisms, Relationships, Rewards	IV. Develop the risk infrastructure.	Task: Allocate appropriate resources for risk management												
			People (skills, experience, competence & training programs).	People: skills, experience, competence & training programs	To establish decision making structures, escalation protocol & identify risk stakeholders.	Risk governance models	IV	CRO							
						Performance management scorecards	IV	CRO							
					To identify competencies, skills levels and experience required by risk stakeholders.	Job profiles	IV		1						
					To ensure proper training for risk stakeholders.	Risk training: induction sessions and risk awareness sessions	IV	CRO							
			Committees: the board should delegate certain functions to well-structured committees but without abdicating its own responsibilities.	Board committees:	To formalise decision making structures, escalation protocol & identify risk stakeholders.										
				Formal terms of reference should be established and approved for each committee of the board.		Board committees charter / terms of reference	IV	CRO							
				The committees' terms of reference should be reviewed yearly.											
				The committees should be appropriately constituted and the composition and the terms of reference should be disclosed in the integrated report.		Integrated report	IV	CRO							
				The risk committee should:		Risk committees:									
				consider the risk management policy and plan and monitor the risk management process;		Board risk committee terms of reference	IV	CRO							
				have as its members executive and non-executive directors, members of senior management and independent risk management experts to be invited, if necessary;		Executive risk committee terms of reference	IV	CRO							
				have a minimum of three members; and		Departmental risk committee terms of reference	IV	CRO							
				convene at least twice per year.		Audit and risk committee	IV	CRO							
				The audit committee should:		Audit committee charter	IV	CAE							
				oversee integrated reporting.											
				have regard to all factors and risks that may impact on the integrity of the integrated report.											
				review and comment on the financial statements included in the integrated report.											
				review the disclosure of sustainability issues in the integrated report to ensure that it is reliable and does not conflict with the financial information.											
				recommend to the board to engage an external assurance provider on material sustainability issues.											
				consider the need to issue interim results.											
				review the content of the summarised information.											
				engage the external auditors to provide assurance on the summarised financial information.											
				ensure that a combined assurance model is applied to provide a coordinated approach to all assurance activities.											
				ensure that the combined assurance is received is appropriate to address all the significant risks facing the company.											
				monitor the relationship between the external assurance providers and the company.											
				The audit committee should be an integral component of the risk management process.											
				The charter of the audit committee should set out its responsibilities regarding risk management.											
				The audit committee should specifically have oversight of:											
				financial reporting risks;											

Addendum C: ERM implementation assessment tool - degree of formality checklist

Theoretical frameworks		Building blocks	Best practice requirements		Proposed deliverables		Building Block	Responsi- bility	Degree of Formality (Mark the appropriate field with 1)				Corrective Actions		
Deming cycle	Weisbord organisational design model		Level 1	Level 2	Purpose	Deliverables			YES	Not started	In process	Done	Activities	Responsibility	Target Date
Plan	Helping mechanisms, Relationships, Rewards	IV. Develop the risk infrastructure.	Committees: the board should delegate certain functions to well-structured committees but without abdicating its own responsibilities.	internal financial controls;	To formalise decision making structures, escalation protocol & identify risk stakeholders.	Audit committee charter	IV	CAE							
				fraud risks as it relates to financial reporting; and		Combined assurance committee terms of reference	IV	CAE							
				IT risks as it relates to financial reporting.											
				The audit committee should also:		Risk specific committee terms of reference e.g. Fraud risk committee	IV	CRO							
				ensure that a combined assurance model is applied to provide a coordinated approach to all assurance activities											
				ensure that the combined assurance is received is appropriate to address all the significant risks facing the company.											
			Models & tools: the organisation's processes, methods and tools to be used for managing risk		To assess and decide on standardised tools that should be used across the organisation.	Risk identification tools	IV		1						
						Risk analysis tools	IV		1						
						Risk evaluation tools	IV		1						
						Risk response tools	IV		1						
						Risk monitoring tools	IV		1						
						Risk reporting tools	IV		1						
			Templates: standardised recording, reporting and assessment templates		To standardise policy, framework, recording, reporting and assessment templates.	Risk quantification models	IV		1						
						Examples:									
						Risk management plan	IV		1						
						Risk communication plan	IV		1						
						Stakeholder maps	IV		1						
						Stakeholder register	IV		1						
						Risk register	IV		1						
						Risk improvement report	IV		1						
						Integrated assurance dashboard	IV		1						
						Integrated report	IV		1						
						Risk self-assessments	IV		1						
						Stewardship report	IV		1						
						Recording process	IV		1						
						Risk acceptance form	IV		1						
						Risk retirement form	IV		1						
						Reporting dashboards	IV		1						
						Reporting scorecards	IV		1						
						Risk policy	IV		1						
						Risk management framework	IV		1						
						Risk committee terms of reference	IV		1						
			Processes: documented processes and procedures.		To embed risk management in all the organisation's practices and processes in a way that it is relevant, effective and efficient.	Common risk language	IV		1						
						Risk owners matrix	IV	CRO							
						Strategic planning process	IV		1						
						Business planing process	IV		1						
						Financial planning process	IV		1						
						Change management process	IV		1						
						Quality assurance process	IV		1						
						Risk management process	IV		1						
						Risk & incident escalation process	IV		1						
						External audit process	IV	CAE							
			Systems: information and knowledge management systems		To select the most appropriate risk management systems.	Performance management process	IV	CHRO							
						Risk recording	IV		1						
						Risk reporting	IV		1						
						Risk monitoring	IV		1						
						Risk review	IV		1						

Addendum C: ERM implementation assessment tool - degree of formality checklist

Theoretical frameworks		Building blocks	Best practice requirements		Proposed deliverables		Building Block	Responsi- bility	Degree of Formality (Mark the appropriate field with 1)				Corrective Actions		
Deming cycle	Weisbord organisational design model		Level 1	Level 2	Purpose	Deliverables			YES	Not started	In process	Done	Activities	Responsibility	Target Date
Do	Leadership, Structure, Relationships, Helping Mechanisms, External environment	V. Implement the ERM program.	Implementing the framework for managing risk.	Define the appropriate timing and strategy for implementing the framework;	To establish a time line for risk management activities.	Risk management plan (calendar)	V		1						
						Critical path analysis for key dependencies	V	CRO							
				Apply the risk management policy and process to the organisational processes;	To embed risk management in all the organisation's practices and processes in a way that it is relevant, effective and efficient.	Common risk language	V		1						
						Risk owners matrix	V	CRO							
						Strategic planning process	V		1						
						Business planing process	V		1						
						Financial planning process	V		1						
						Change management process	V		1						
						Quality assurance process	V		1						
						Risk management process	V		1						
						Risk & incident escalation process	V		1						
						Performance management process	V	CHRO							
				Comply with legal and regulatory requirements;	To communicate risk related compliance requirements.	Legal, regulatory & best practice compliance register (pertaining to risk)	V		1						
				Ensure that decision making, including the development and setting of objectives, is aligned with the outcomes of risk management processes;	To encourage a risk mind-set for decision making.	Risk appetite statements	V	CRO							
						Risk tolerance levels	V	CRO							
						Strategic plan	V		1						
				Hold information and training sessions; and	To create a common risk language, improve risk awareness and encourage risk based decision making.	ERM framework & policy	V		1						
						Risk awareness gap analysis	V	CRO							
						Risk maturity assessment	V	CRO							
						Risk awareness strategy & -plan	V	CRO							
					To ensure that the risk management framework remains appropriate.	Risk awareness strategy & -plan	V	CRO							
						Risk facilitation sessions	V		1						
			Implementing the risk management process.	Step 1: Communication and consultation with external and internal stakeholders should take place during all stages of the risk management process.	To identify the internal and external stakeholders for the organisation / division / department / project.	Stakeholder analysis	V		1						
					To identify the most appropriate communication tools and establish timelines.	Risk communication plan	V	CRO							
					To ensure that the right information reaches the right people at the right time.	Risk reports e.g. stress tests, risk & control self-assessments, incident reports, risk treatment plans, key risk indicator reports.	V	CRO							
				Step 2: Establish the context (Know your organisation / division / department / project / risk type)											
						External environment mind map	V	Risk Owners							
						External stakeholder register	V		1						
						External stakeholder map	V		1						
				Establish the internal context	To describe the UNIQUE context for the risk management project.	Internal value chain mind map	V	Risk Owners							
						Internal stakeholder register	V		1						
						Internal stakeholder map	V		1						
						Standardised risk management context (refer to building block III)	V		1						
				Establishing the context of the risk management process		Standardised risk criteria (refer to building block III)	V		1						
				Apply the risk criteria											
				Step 3: Risk identification	Process of finding, recognising and describing risks.	Key / Principle / Strategic risk register	V	Risk Owners							
						Divisional / departmental / business unit risk register	V	Risk Owners							
						Emerging risk register	V	CRO							
						Risk library	V	CRO							
				Step 4: Risk analysis	Process to comprehend the nature of risk and to determine the level of risk (e.g. high, medium, low).	Key / Principle / Strategic risk register - risk ratings applied	V	Risk Owners							
						Divisional / departmental / business unit risk register - risk ratings applied	V	Risk Owners							
						Root cause analysis	V	Risk Owners							
				Step 5: Risk evaluation	Process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable.	Key / Principle / Strategic risk profile - risk ratings + current controls applied & risk owners identified	V	Risk Owners							
						Divisional / departmental / business unit risk register risk ratings + current controls applied & risk owners identified	V	Risk Owners							
			Step 6: Risk response	To identify the most appropriate risk treatment for the most significant risks.		Controls library	V	CRO							
						Risk response plans / Action plans	V	Risk Owners							
						Risk response options	V	Risk Owners							

Addendum C: ERM implementation assessment tool - degree of formality checklist

Theoretical frameworks		Building blocks	Best practice requirements		Proposed deliverables		Building Block	Respon- sibility	Degree of Formality (Mark the appropriate field with 1)				Corrective Actions		
Deming cycle	Weisbord organisational design model				Purpose	Deliverables			YES	Not started	In process	Done	Activities	Responsibility	Target Date
Check	Rewards	VI. Monitor and review the ERM program.	Monitoring activities by the Board	The board should ensure continual risk monitoring by management	To ensure proper risk oversight.	Risk governance framework	VI		1						
				The board should ensure that effective and continual monitoring of risk management takes place.	To reduce role confusion and provide clear guidelines for risk monitoring.	Risk management plan (monitoring roles and responsibilities)	VI		1						
				The responsibility for monitoring should be defined in the risk management plan.	To periodically measure progress against, and deviation from, the risk management plan.	Status report on risk management plan implementation	VI	CRO							
			Review activities by the Board	The board should comment in the integrated report on the effectiveness of the system and process of risk management.	To periodically review whether the risk management framework, policy and plan are still appropriate, given the organisations' external and internal context;	Integrated report (risk and opportunities section)	VI	CRO							
				The board should ensure that effective and continual monitoring of risk management takes place.	To periodically measure progress against, and deviation from, the risk management plan.	Risk management plan implementation status report	VI	CRO							
					The board should review the implementation of the risk management plan at least once a year.	To periodically review whether the risk management framework, policy and plan are still appropriate, given the organisations' external and internal context;	Risk improvement report	VI	CAE						
				Internal audit report		VI	CAE								
				The performance of the committee should be evaluated once a year by the board.	To ensure effectiveness and efficiency with regards to committee activities.	Board risk committee performance evaluation	VI	Company Secretary							
				Monitor the risk management framework	The board should monitor that risks taken are within the tolerance and appetite levels.	To ensure compliance with the risk appetite framework.	Risk appetite status report	VI	CRO						
			To ensure compliance with the risk tolerance levels.			Risk tolerance status report	VI	CRO							
			Measure risk management performance against indicators, which are periodically reviewed for appropriateness;		To measure risk management performance against indicators, which are periodically reviewed for appropriateness;	KRI performance report	VI	CRO							
			Periodically measure progress against, and deviation from, the risk management plan;		To periodically measure progress against, and deviation from, the risk management plan.	Risk management plan implementation status report	VI	CRO							
						Risk management policy compliance report	VI	CCO							
			Report on risk, progress with the risk management plan and how well the risk management policy is being followed;		To report on risk, progress with the risk management plan and how well the risk management policy is being followed.	Deviations from risk management policy report	VI	CCO							
						Monitor the level of risk awareness	To track the improvement of risk awareness.	Risk culture surveys	VI	CRO					
			Review the risk management framework		Periodically review whether the risk management framework, policy and plan are still appropriate, given the organizations' external and internal context;	To periodically review whether the risk management framework, policy and plan are still appropriate, given the organisations' external and internal context.	Risk improvement report	VI	CAE						
				Internal audit report			VI	CAE							
				Risk calendar			VI		1						
				Communicate and consult with stakeholders to ensure that its risk management framework remains appropriate.	Risk improvement report		VI	CAE							
					Subject matter expert gap analysis		VI		1						
					Internal audit reports		VI	CAE							
					Risk calendar		VI		1						
					ISO 9000 reports		VI	CPO							
			Review the effectiveness of the risk management framework.		Internal audit reports, risk committee effectiveness, qualitative conversations, risk appetite and risk tolerance level breaches, signed letters of representation.	VI	CAE								
			Monitor the risk management process	Ensuring that controls are effective and efficient in both design and operation.	To ensure that controls are effective and efficient in both design and operation.	Subject matter expert gap analysis	VI		1						
						Combined assurance reports	VI	CAE							
						Risk profile status reports	VI		1						
						Internal audit reports	VI	CAE							
				Identifying emerging risks.	To identify emerging risks in the organisation's internal value chain and external environment.	External audit reports	VI	CAE							
						Emerging risk register	VI	CRO							
			Review the risk management process	Analysing and learning lessons from events (including near-misses), changes, trends, successes and failures;	To analyse and learn lessons from events (including near-misses), changes, trends, successes and failures.	Variance and trend analysis	VI	CRO							
						Post mortem sessions	VI	CRO							
						Environmental scanning	VI	CRO							
						Risk reconciliation reports	VI	CRO							
						Post loss analysis	VI	CRO							

Addendum C: ERM implementation assessment tool - degree of formality checklist

Theoretical frameworks		Building blocks	Best practice requirements		Proposed deliverables		Building Block	Responsi- bility		Degree of Formality (Mark the appropriate field with 1)				Corrective Actions		
Deming cycle	Weisbord organisational design model		Level 1	Level 2	Purpose	Deliverables				YES	Not started	In process	Done	Activities	Responsibility	Target Date
Adjust	Leadership, Purposes, Structure, Relationships, Rewards, Helpful mechanisms, External environment	VII. Continual improvement of the ERM program.	The board should receive assurance regarding the effectiveness of the risk management process	Management should provide assurance to the board that the risk management plan is integrated in the daily activities of the company.	To inform the relevant committees and risk stakeholders of the level of assurance provided by assurance providers.	Combined assurance report.	VII	CAE								
						Risk reports to various committees	VII		1							
						Risk maturity assessment	VII		1							
						Benchmarking assessments (peer reviews & best practice)	VII		1							
				Internal audit should: provide a written assessment of the effectiveness of the system of internal controls; detect changes in the external and internal context, including changes to risk criteria and the risk itself which can require revision of risk treatments and priorities; and obtaining further information to improve risk assessment.	To periodically review whether the risk management framework, policy and plan are still appropriate, given the organisations' external and internal context;											
						Risk improvement report	VII	CAE								
						Internal audit report	VII	CAE								
						Risk improvement report (List of internal, external, risk management process & risk criteria context changes)	VII	CAE								
						Risk improvement report (risk assessment process & methodology)	VII	CAE								

Source: Researcher's own compilation

ENTERPRISE RISK MANAGEMENT (ERM) QUESTIONNAIRE

CONFIDENTIAL

Format: Electronic Survey

Ethics clearance number: ECONIT-2016-038

Student: Ms Hermie le Roux

Student number: 11112891

Contact number: 084 777 2803

Email: applyerm@gmail.com

Degree: PhD (Risk Management)

Promotor: Dr. Diana Viljoen

University: North-West University, Vaal Triangle Campus, Faculty of Economic Sciences and IT,
School of Economic Sciences

Dear Participant

You are invited to participate in an academic research study conducted by Ms. Hermie le Roux, a student of the School of Economic Sciences, North-West University, Vaal Triangle Campus in partial fulfilment of her PhD in Risk Management.

The study will be conducted according to the ethical guidelines and principles of the international Declaration of Helsinki and the ethical guidelines of the National Health Research Ethics Council. Please note that the research ethics committee members or relevant authorities may inspect the research records.

OVERVIEW OF THE RESEARCH STUDY:

1. Title of the research study:

Enterprise risk management (ERM) program implementation model and - assessment tool for use by the risk facilitator

2. Research problem:

The role of the risk practitioner (such as the chief executive officer, chief risk officer or another risk custodian) has changed from that of an advisor to a business partner as expectations regarding timely and transparent risk information from external and internal risk stakeholders have escalated (Senior Supervisors Group, 2009). The risk practitioners' ability to keep organisational decision makers informed of existing, new and emerging risks, and therefore opportunities, is pivotal to the organisations' success as it enables risk-based and timely organisational decisions leading to the creation, protection or enhancement of value within their business.

It stands to reason that a risk practitioner employed by an organisation operating within the ERM domain with a clear understanding of the concept ERM, the adoption drivers of ERM, the proposed value add for their organisation and the barriers to ERM – should be able to develop an ERM implementation program and assessment tool to create, protect or enhance their organisation's value. However, it is clear from the ambiguity surrounding the common understanding of ERM that it is difficult to implement (Colquitt, Hoyt & Lee, 1999; Kleffner, Lee & McGannon, 2003; Liebenberg & Hoyt, 2003; Aabo, Fraser & Simkins, 2005; Beasley, Clune and Hermanson, 2005; Nocco & Stulz, 2006; Pagach & Warr, 2011).

Based on the results of the preliminary literature review and the researcher's own risk management experience of 24 years, an in-depth study has been done on how to translate

an overarching, strategic ERM approach into a practice-based ERM framework with specific tools to enable any organisation; within any industry, to sufficiently implement ERM. The purpose of the study was to develop an ERM implementation model and assessment tool that can be used by all risk stakeholders as a clear guideline for ERM program implementation and to assess the status on ERM implementation and the degree of formality of ERM implementation within South African organisations.

3. Objectives of **this** questionnaire:

- To collect general information regarding your industry, your organisation and your position in the organisation;
- To collect information with regards to your enterprise risk management (ERM) program, i.e. general information, the importance of ERM and ranking the barriers to ERM program implementation

4. Duration of data collection: Approximately 10 minutes

YOUR PARTICIPATION:

1. Voluntary Participation:

Your participation in this survey is voluntary. You may refuse to take part in the research or exit the survey at any time without penalty. You are also free to decline to answer any particular question you do not wish to answer for any reason.

2. Benefits:

You will receive no direct benefits from participating in this research study. However, your responses may help us learn more about the barriers to Enterprise Risk Management program implementation.

3. Risks:

The expected risks or discomfort in participating in the study are minimal.

4. Contact:

If you have questions at any time about the study or the procedures, you may contact my research promotor, Dr. Diana Viljoen via phone at +2716-910 3313 or via email at diana.viljoen@nwu.ac.za.

5. Inclusion and exclusion criteria:

You have been invited to participate in this research because you are an adult person (18 years or older) who has at least secondary education. The questionnaires are in English, so you have to be sufficiently fluent in English to participate.

ELECTRONIC CONSENT:

Please select your choice below. You may print a copy of this consent form for your records.
Selecting the “Agree” option (with an X) indicates that

- You have read the above information
- You voluntarily agree to participate
- You are 18 years of age or older

Agree

Disagree

RULES OF ENGAGEMENT:

- The answers you give will be treated as strictly confidential.
- The general results of the study may be published in an academic journal.
- Please answer the questions as completely and honestly as possible.
- Please answer all the questions
- It should take you less than 10 minutes to complete the whole questionnaire.
- Only complete the questionnaire once.

TARGET DATE: 31 March 2016

The survey outline:

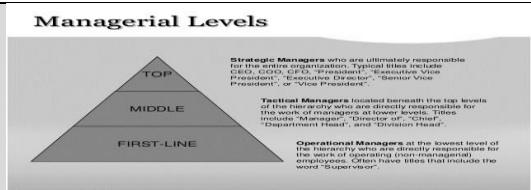
The survey is divided into the following sections:

- Part 1: General information regarding your industry, your organisation and your position in the organisation;
- Part 2: Information on your enterprise risk management (ERM) program
 - Section 1: General information
 - Section 2: Importance of ERM
 - Section 3: Barriers to ERM program implementation

PART 1: General information regarding your industry, your organisation and your position in the organisation

Question 1: Complete the following information about your organisation and your position in the organisation.

(Note: The boxes will expand as required to enable you to fit as much information in as required.)

<u>ORGANISATION:</u>		
1.	Name of organisation	
2.	Type of organisation e.g. (Pty) Ltd., Ltd., Partnership, Charity, etc.	
3.	Industry / Sector	
4.	Country in which your organisation is registered	
<u>PARTICIPANT:</u>		
5.	Name and surname	
6.	Job title	
7.	Level of management	 Managerial Levels Strategic Managers who are ultimately responsible for the entire organization. Typical titles include CEO, CFO, CIO, President, Executive Vice President, Executive Director, Senior Vice President, or Vice President. Tactical Managers located beneath the top levels of the hierarchy who are directly responsible for the work of managing at lower levels. Titles include Manager, Director of, Chief, Department Head, and Division Head. Operational Managers at the lowest level of the hierarchy who are directly responsible for the work of operating (non-managerial) employees. Often have titles that include the word "Supervisor".

8.	Total number of years of experience	
9.	Total number of years of risk related experience	
10.	Number of employees reporting to the participant	

PART 2: INFORMATION ABOUT YOUR ENTERPRISE RISK MANAGEMENT (ERM) PROGRAM

Section 1: General information regarding your ERM program

Question 1.1: Does your organisation have a formalised Enterprise Risk Management (ERM) program? If no, please provide a list of your organisation's risk management activities. (Use the "other" field to answer this)

- Yes
- No

Question 1.2: Which of the following major factor/s triggered the adoption of the ERM program in your organisation? If other is selected, then please explain.

- Financial crisis of 2008
- Requirements from shareholders / investors / owners
- Corporate governance requirements from the board of directors
- Influence of risk practitioners
- Legal, regulatory and compliance requirements
- Pressure from the market
- Catastrophic event
- Rating agency requirements
- Other, please explain

Question 1.3: Which best practice ERM framework did you use as a basis for your organisational ERM program? If other is selected, then please explain.

- Committee of Sponsoring Organisations (COSO) - Enterprise Risk Management - Integrated Framework
- ISO 31000: 2009 - Risk Management Principles and Guidelines
- AUS/NZ 4360: 2004 Risk Management
- King III: 2009 Code on Corporate Governance in South Africa
- Combination of best practice Risk Management Frameworks
- Unsure
- Other, please explain

Question 1.4: How long has your ERM program been in place?

- Less than 1 year
- 1-3 Years
- 4-7 Years
- Longer than 7 Years

Section 2: Importance of ERM in your organisation

Question 2.1: Who has the primary responsibility for the ERM program in your organisation?

Select only one option?

- Chief Executive Officer
- Chief Financial Officer
- Chief Audit Executive
- Chief Risk Officer
- Chief Compliance Officer
- Other C-Level Officer
- Executive
- Senior Manager

If another C-level officer or Executive or Senior Manager, please indicate who is responsible.

Question 2.2: Is the risk management function integrated into the decision making process for the following areas?

Decisions	Yes	No	I don't know
Budgeting and forecasting	-	-	-
Projects evaluation process	-	-	-
Process, model and system development	-	-	-
Day-to-day operations			
Investment and disinvestment or financing decisions	-	-	-
New product development	-	-	-
Performance management process and incentives management	-	-	-
Strategic and business planning	-	-	-

Question 2.3: At which of the following committees does the EXECUTIVE risk owner report on and discuss KEY risk issues? If other is selected, then please specify.

- Board
 - Audit Committee
 - Board Risk Management Committee
 - Executive Risk Committee
 - Departmental Risk Committee
 - Other, please specify
-
-
-

Question 2.3: At which of the following committees does the DEPARTMENTAL risk owner report on and discuss departmental / project risk issues? If other is selected, then please specify.

- Board
- Audit Committee
- Board Risk Management Committee
- Executive Risk Committee
- Departmental Risk Committee
- Other, please specify

Question 2.5: What is the perceived value added by the ERM program? If other is selected, then please explain.

- To increase risk awareness
 - To align risk appetite and strategy
 - To avoid and / or mitigate risks
 - To enhance risk based decisions
 - To reduce operational surprises and losses
 - To eliminate silos, i.e. identifying and managing risks across the enterprise
 - To improve resource allocation
 - Other, please explain
-
-
-

Section 3: Barriers to Enterprise Risk Management (ERM) program implementation

According to Peter Kennedy (Kennedy, 2008) there are five steps to doing ERM correctly:

1. Establish governance and expect it to change.
2. Start the conversation inside and outside.
3. Use the same risk management tools and methods.
4. Keep line of sight from actions to root causes to risk.
5. Share findings across domains.

But, there are also pre-existing organisational conditions and mind-sets that create barriers to ERM program implementation. The list in the following question is based on the findings of an extensive literature review on the topic.

Question 3.1: Please rank the following barriers to ERM program implementation where 1 is the most important and 10 is the least important.

ERM Roadmap Building Block	Affected Deliverables	Barrier	Rank
II. Establish the tone of the organisation (BUILD IT)	Risk awareness program	Lack of Board or C-level or senior executive leadership.	

ERM Roadmap Building Block	Affected Deliverables	Barrier	Rank
II. Establish the tone of the organisation (BUILD IT)	Risk governance framework	Difficult to identify risk owners for particular risks and responses.	
II. Establish the tone of the organisation (BUILD IT)	Risk governance framework	Role confusion: lack of clarity with regards to risk roles and responsibilities in the organisation.	
II. Establish the tone of the organisation (BUILD IT)	Risk management plan	Insufficient resources (i.e. people, technology, budget) to manage risks.	
III. Design the rules of the game (BUILD IT)	Risk management framework	Lack of perceived value added by the enterprise risk management program.	
III. Design the rules of the game (BUILD IT)	Risk management framework Risk management process	Badly designed ERM program, e.g.: • Misalignment between the ERM program design and the design of the organisation. • A common view from management is that risk is intuitively managed, and therefore there is no need to deploy a formal approach. • Ignoring existing risk management activities. • Inadequate information to make risk-based decisions.	
III. Design the rules of the game (BUILD IT)	Risk management framework	Incentives do not reward making risk-based decisions.	
III. Design the rules of the game (BUILD IT)	Common risk language	Risk management criteria is not standardised throughout the organisation.	
V. Implement (DO IT)	Risk integration	Competing priorities between the risk owner's operational- (day-to-day) and risk responsibilities.	
VI. Monitor and review (CHECK IT)	Monitoring	Little or no monitoring regarding risk management plan execution.	

Thank you for your prompt response and enthusiastic participation.

References:

- Bates, L. 2010. Avoiding the pitfalls of enterprise risk management. *Journal of Risk Management in Financial Institutions*, 4(1):23-28.
- Beasley, M.S., Branson, B.C. & Hancock, B.V. 2009. ERM: Opportunities for Improvement. *Journal of Accountancy*, 208(3):28-32.
- Beaumier, C. & DeLoach, J. 2011. Ten Common Risk Management Failures and How to Avoid Them. *Business Credit*, 113(8):46.
- Board, C.E. 2008. Risk management effectiveness survey findings.
- Boultonwood, B. & Dominus, M. 2014. Developing an Effective Risk Culture. *Electric Perspectives*, 39(3):57.
- Burnaby, P. & Hass, S. 2009. Ten steps to enterprise-wide risk management. *Corporate Governance*, 9(5):539-550.
- COSO. 2010. Report on ERM: Coso.
- Deloitte. 2013. Exploring Strategic Risk: 300 executives around the world say their view of strategic risk is changing: Deloitte.
- FERMA. 2012. Keys to Understanding the Diversity of Risk Management in a Riskier World: Ferma.
- Fraser, J.R.S. & Simkins, B.J. 2007. Ten Common Misconceptions About Enterprise Risk Management. *Journal of Applied Corporate Finance*, 19(4):75-81.
- Frigo, M.L. & Anderson, R.J. 2011. Embracing Enterprise Risk Management. *Thought Leadership in ERM* Date of access: April 2015.
- Group, S.S. 2009. Risk management lessons from the global banking crisis of 2008.
- Hamill, M. 2007. The practical challenges of ERM. www.protiviti.com.au.
- Harner, M.M. 2010. Barriers to Effective Risk Management [article].1323.
- Hellings, S. 2014. The Trials and Tribulations of ERM. *Credit Control*, 35(6/7):51.
- Kennedy, P. 2008. Enterprise risk management: effective ERM practices. *Strategy & Leadership*, 36(3).
- Kerstin, D., Simone, O. & Nicole, Z. 2014. Challenges in implementing enterprise risk management. *ACRN Journal of Finance and Risk Perspectives*, 3(3):1-14.
- Lam, J. 2010. Enterprise risk management: back to the future: several challenges still need addressing before enterprise risk management can truly be called a success. *The RMA Journal*(9):16.
- Martin, D. & Power, M. 2007. The end of enterprise risk management. *Aei-Brookings Joint Center for Regulatory Studies*. August.
- Merchant, K.A. 2012. ERM: where to go from here: why new tools are needed to help companies properly assess risks and opportunities. *Journal of Accountancy*(3):32.
- Nocco, B.W. & Stulz, R.M. 2006. Enterprise risk management: Theory and practice. *Journal of Applied Corporate Finance*, 18(4):8-20.

Prodyot, S., Wolfe, S. & McCabe, K. 2013. Translating ERM from a Theoretical Perspective into Practical and Effective Actions that Impact Performance. *URMIA Journal*.

Protiviti. 2006. Guide to Enterprise Risk Management. Frequently Asked Questions: Protiviti.

RIMS, A. 2013. 2013 RIMS Enterprise Risk Management (ERM) Survey: Rims, A.

Schanfield, A. & Helming, D. 2008. 12 Top ERM Implementation Challenges. *Internal Auditor*, 65(6):41-44.

Addendum E: **Phase 2 – Round 1: Discuss the conceptual ERM implementation model**



PO Box 1174, Vanderbijlpark
South Africa 1900

Tel: 016 910-3111

Fax: 016 910-3116

Web: <http://www.nwu.ac.za>

Risk Management Department

Tel: 016 910-3403

Email: Diana.Viljoen@nwu.ac.za

ENTERPRISE RISK MANAGEMENT (ERM) PROGRAM IMPLEMENTATION MODEL VALIDATION INTERVIEW CONFIDENTIAL

Format: Semi-structured Interview

Ethics clearance number: ECONIT-2016-038

Student: Ms Hermie le Roux

Student number: 11112891

Contact number: 084 777 2803

Email: applyerm@gmail.com

Degree: PhD (Risk Management)

Promotor: Dr. Diana Viljoen

University: North-West University, Vaal Triangle Campus, Faculty of Economic Sciences and IT,
School of Economic Sciences

Interviewer: Hermie le Roux

Interviewee:

Job:

Company:

Date:

Duration:

OVERVIEW OF THE RESEARCH STUDY:

1. Title of the research study:

Development of an Enterprise risk management (ERM) program implementation model and - assessment tool

2. Research problem:

The notion that several barriers to ERM implementation prevent the successful implementation of an ERM program is supported by academic- and industry related research (Liebenberg & Hoyt, 2003; Beasley et al., 2005; Nocco & Stulz, 2006; Blaskovich & Taylor, 2011; Gates et al., 2012; Bromiley et al., 2014; Viscelli, 2014). This results in a lower adoption rate of ERM programs (Colquitt et al., 1999; Harrington et al., 2002; Kleffner et al., 2003; Liebenberg et al., 2003; Beasley et al., 2005).

This study will attempt to prioritise the barriers to ERM program implementation from a South African perspective, develop an ERM program implementation model, develop an ERM program implementation assessment tool, and position the risk facilitator as the linking pin in the ERM process in an effort to deduce the barriers to ERM program implementation.

BACKGROUND TO THE INTERVIEW:

1. Objective of the interview: to **VALIDATE** the components of the ERM program implementation model.

2. Participant selection criteria:

- a. Risk officers / managers / facilitators that are
 - i. viewed as leaders in ERM by their peers and by the researcher.
 - ii. involved with the development and / or implementation of ERM

3. **During** the interview we will discuss the following:

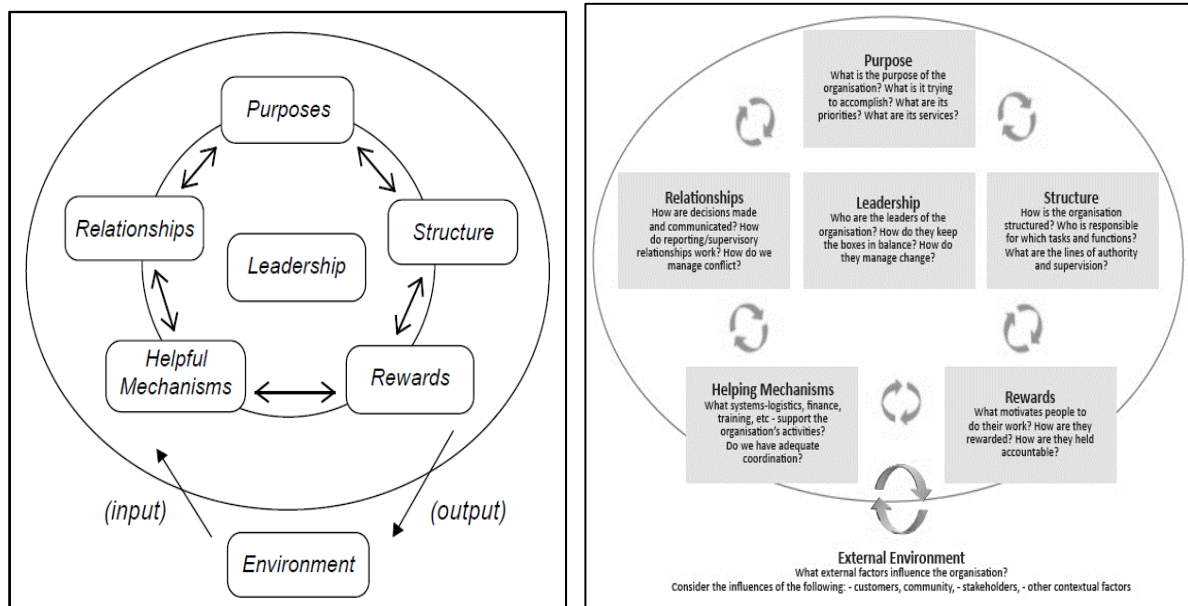
- Part 1: an overview of the ERM implementation model;
- Part 2: confirm the requirements, deliverables and purpose for the components in building blocks I – VII; and
- Part 3: comments and suggestions.

PART 1: OVERVIEW OF THE ENTERPRISE RISK MANAGEMENT (ERM) PROGRAM MODEL

WHY? Research gaps:

- Limited academic research on the “how to” of enterprise risk implementation, and
- Barrier to ERM implementation = misalignment between ERM program design and organisational design

To address the misalignment: Deming cycle (Plan-Do-Check_Adjust) & Marvin Weisbord's model



Purpose of the ERM program implementation model:

- To provide risk facilitators / risk role players with a standardised implementation model that they can use to facilitate the implementation of the ERM program
- To reduce the barriers to ERM program implementation
- To result in improved allocation of scarce risk resources
- To establish a common risk language.

The model:

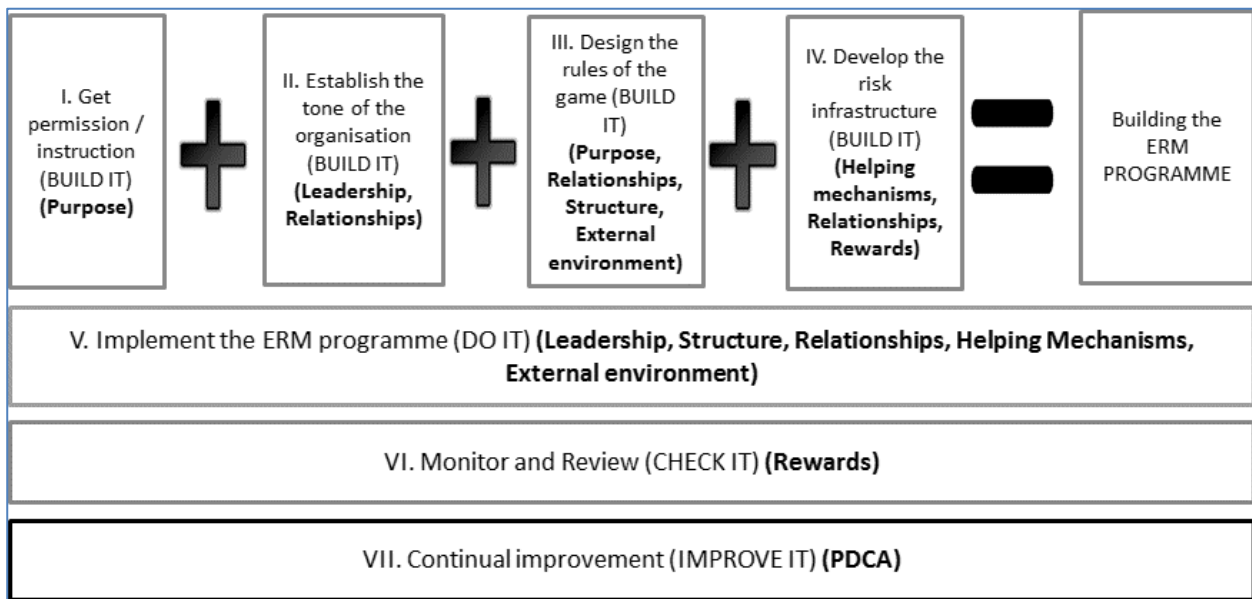


Diagram 1: Enterprise Risk Management (ERM) program: implementation model (based on ISO 31000, King III and ISO 31010)

The key question that should be addressed by each building block in the ERM program is as follows:

1. **Get permission:** does the organisation have to or want to implement ERM?
2. **Establish the tone of the organisation:** who is involved and how do we set the tone at each level of the organisation?
3. **Design the rules of the game:** what are the requirements of the risk management framework and risk management process?
4. **Develop the risk infrastructure:** Which resources do we need to design and implement an ERM program?
5. **Implement the ERM program:** how do we implement the ERM program?
6. **Monitor and review:** How do we ensure effective and efficient risk management?
7. **Continual improvement:** which elements of the risk management framework and risk management process can be improved?

INTERVIEWER NOTES:

General notes:

Suggestions:

INTERVIEW TRANSCRIPTION:

PART 2: ENTERPRISE RISK MANAGEMENT (ERM) PROGRAM – CONFIRM THE REQUIREMENTS AND THE DELIVERABLES

- | |
|--|
| <ul style="list-style-type: none">• Requirements: Source = ISO 31000 – Risk management principles and guidelines, ISO 31010 – risk assessment techniques and King III – code on corporate governance from South Africa. |
| <ul style="list-style-type: none">• Deliverables: derived from requirements and based on practical experience. |
| <ul style="list-style-type: none">• Purpose: based on requirements, best practice and academic research. |

Building block 1: Get permission

Question 1.1: Please confirm the requirements, deliverables and the purpose. If you would like to add or remove a component, then please explain.

1.1: **What.** The proposed requirements, deliverables and the purpose is detailed in the table below.

Requirements	Deliverables	Purpose
Ensure legal and regulatory compliance.	Compliance requirements (legal + regulatory + best practise frameworks)	To motivate the need for an ERM program.
	Agenda item for Board meeting	To ask for permission for the design and implementation of the ERM program.
	Minutes of the Board meeting	To record the permission received to design and implement an ERM program.
The risk committee or audit committee should assist the board in carrying out its risk responsibilities	Board risk committee (BRC) charter	To assist the board in carrying out its risk roles and responsibilities.
Define and endorse the risk management policy	Risk management policy	To document risk management scope, objectives and roles and responsibilities.

INTERVIEWER NOTES:

General notes:

Suggestions:

INTERVIEW TRANSCRIPTION:

Building block 2: Establish the tone of the organisation

Question 2.1: Please confirm the requirements, deliverables and the purpose. If you would like to add or remove a component, then please explain.

2.1: **What.** The proposed requirements, deliverables and the purpose is detailed in the table below.

Requirements	Deliverables	Purpose
Establishing the tone of the organisation: The introduction of risk management and ensuring its ongoing effectiveness require strong and sustained commitment by management of the organisation, as well as strategic and rigorous planning to achieve commitment at all levels.	CRO / Senior level project sponsor	A senior level ERM program sponsor / Chief Risk Officer should have clear authority over and accountability for oversight of risk across the enterprise.
(a) Ensure that the organisation's culture and risk management policy are aligned.	Risk management policy	To document risk management scope, objectives and roles and responsibilities.
(b) Determine risk management performance indicators that align with performance indicators of the organisation.	Performance indicators (Key risk indicators)	To measure risk management performance against indicators, which are periodically reviewed for appropriateness;
(c) Align risk management objectives with the objectives and strategies of the organisation.	Risk appetite & risk tolerance	To encourage a risk mind-set for decision making.
(d) Assign accountabilities and responsibilities at appropriate levels within the organisation.	Risk governance model: (incl. risk owners' matrix, roles & responsibilities, reporting & escalation process & incentives guidelines.)	To establish clear roles and responsibilities for risk activities. across businesses and risk types.
(e) Ensure that the necessary resources are allocated to risk management.	Risk management plan (People, Processes and Budget)	To ensure the effective and efficient implementation of the ERM program.
(f) Communicate the benefits of risk management to all stakeholders.	Benefits of risk management	To raise risk awareness and create excitement for the project.
The induction and ongoing training programs of the board should incorporate risk governance. (Note: apply to all the levels in the organisation)	Risk awareness gap analysis	To raise risk awareness and create excitement for the project.
	Risk maturity model	
	Risk awareness plan	

INTERVIEWER NOTES:

General notes:

Suggestions:

INTERVIEW TRANSCRIPTION:

Building block 3: Design the rules of the game

Question 3.1: Please confirm the requirements, deliverables and the purpose. If you would like to add or remove a component, then please explain.

3.1: **What.** The proposed requirements, deliverables and the purpose is detailed in the table below.

Requirements	Deliverables	Purpose
RISK MANAGEMENT FRAMEWORK		
Task: Understanding the organisation and its context (Know your organisation)		
External context of the organisation	Environmental scanning	To get an overall picture of the external environment based PESTLE and / or Porter's 5 forces.
	Key business drivers' analysis	
	External stakeholder analysis	
Internal context of the organisation	Environmental scanning of the INTERNAL value chain	To describe the internal value chain of the organisation and to identify areas that would create risks and opportunities
	SWOT analysis	
	Organisational organigram	
	Divisional organigram	
	Departmental organigram	
	Delegation of authority	
	Committee structure	
	Committee charters	
	List of policies	
	Copy of policies	
	Action plans (strategies)	
	Risk competency model	
	Job profiles / specification	
	Technical job specs	
	List of systems	
	Process maps	
	Escalation policy	
	Escalation process	
	Connected stakeholder analysis	
	Internal stakeholder analysis	
	Organisational culture survey results	
	List of standards, guidelines and models	
	Contracts register	

Requirements	Deliverables	Purpose
RISK MANAGEMENT FRAMEWORK		
Task: Understanding the organisation and its context (Know your organisation)		
Context of the risk management process	Risk management file / manual that includes:	To create ONE set of risk management rules for the organisation.
	• Risk management goals & - objectives	
	• Risk governance model	
	• Top-down & Bottom-up risk management activities	
	• Interconnectedness maps	
	• Risk assessment methodologies	
	• Key risk indicators	
	• Decision matrix	
	• Research to clarify context	
Risk criteria	Risk management file / manual that includes:	To create standardised risk assessment criteria for the organisation as a whole. To give risk owners and other risk stakeholders insight into risk management in their terms.
	• Examples of causes and consequences	
	• Impact guidelines and scale	
	• Probability guidelines and scale	
	• Risk tolerance levels	
	• Interconnectedness of risks	
Task: establishing the risk management policy	Risk management policy	To document risk management scope, objectives and roles and responsibilities.
Task: develop an accountability matrix / risk governance framework	Risk governance model: (incl. risk owners' matrix, roles & responsibilities, reporting & escalation process & incentives guidelines.)	To establish clear roles and responsibilities for risk activities across businesses and risk types.
Task: integration into organisational processes	Common risk language	To embed risk management in all the organisation's practices and processes in a way that it is relevant, effective and efficient.
	Strategic planning process	
	Risk owners	
	Business planning process	
	Financial planning process	
	Risk & incident escalation process	
Align risk management objectives with the objectives and strategies of the organisation.	Risk appetite & risk tolerance	To encourage a risk mind-set for decision making.
Determine risk management performance indicators that align with performance indicators of the organisation	Performance reporting metrics, i.e. key risk indicators	To measure risk management performance against indicators, which are periodically reviewed for appropriateness;
Task: establishing internal communication and reporting mechanisms	Internal reporting guidelines	To create one set of rules for risk communication and also to increase risk transparency.
	Internal reporting mechanisms	
Task: establishing external communication and reporting mechanisms	Integrated report: risks and opportunities section	To create one set of rules for risk communication and also to increase risk transparency.
	External communication guidelines	
	External reporting mechanisms	

Requirements	Deliverables	Purpose
RISK MANAGEMENT PROCESS		
Design the risk management process	Risk management process guidelines	To develop a standardised risk management process for the organisation.

INTERVIEWER NOTES:

General notes:

Suggestions:

INTERVIEW TRANSCRIPTION:

Building block 4: Develop the risk infrastructure

Question 4.1: Please confirm the requirements, deliverables and the purpose. If you would like to add or remove a component, then please explain.

4.1: **What.** The proposed requirements, deliverables and the purpose is detailed in the table below.

Requirements	Deliverables	Purpose
People (skills, experience and competence)	Risk governance model	To establish decision making structures, escalation protocol & identify risk stakeholders.
	Risk competency model	To identify competencies, skills levels and experience required by risk stakeholders.
	Risk training program (calendar, material, etc.)	To ensure proper training for risk stakeholders.
Committees: the board should delegate certain functions to well-structured committees but without abdicating its own responsibilities.	Board risk committee (part of the escalation structure)	To formalise decision making structures, escalation protocol & identify risk stakeholders.
	Audit committee (part of the escalation structure)	
	Executive risk committee (part of the escalation structure)	
	Departmental risk committee (part of the escalation structure)	
	Integrated assurance committee (part of the escalation structure)	
Models & tools: the organisation's processes, methods and tools to be used for managing risk	Risk identification tools	To assess and decide on standardised tools that should be used across the organisation.
	Risk analysis tools	
	Risk treatment tools	
	Risk monitoring tools	
	Models	
Templates: standardised recording, reporting and assessment templates	Examples:	To standardise recording, reporting and assessment templates.
	Risk management plan	
	Risk communication plan	
	Stakeholder maps	
	Stakeholder register	
	Risk register	
	Risk improvement report	
	Integrated assurance dashboard	
	Integrated report	
	Risk self-assessments	
	Stewardship report	
	Recording process	
Processes: documented processes and procedures;	Integration of risk process	To embed risk management in all the organisation's practices and processes in a way that it is relevant, effective and efficient.
Systems: information and knowledge management systems	Risk recording	To select the most appropriate risk management systems.
	Risk reporting	
	Risk monitoring	
	Risk review	

INTERVIEWER NOTES:

General notes:

Suggestions:

INTERVIEW TRANSCRIPTION:

Building block 5: Implement the ERM program

Question 5.1: Please confirm the requirements, deliverables and the purpose. If you would like to add or remove a component, then please explain.

5.1: **What.** The proposed requirements, deliverables and the purpose is detailed in the table below.

Requirements	Deliverables	Purpose
RISK MANAGEMENT FRAMEWORK		
Define the appropriate timing and strategy for implementing the framework;	Risk management plan (calendar)	To establish a time line for implementation.
Apply the risk management policy and process to the organisational processes;	Integration of the risk into organisational processes	To create an effective risk culture and to reduce role confusion with regards to risk implementation.
Comply with legal and regulatory requirements;	Legal, regulatory & best practice compliance register (pertaining to risk)	To communicate risk related compliance requirements.
Ensure that decision making, including the development and setting of objectives, is aligned with the outcomes of risk management processes;	Risk appetite statement & Risk tolerance levels	To encourage a risk mind-set for decision making.
Hold information and training sessions; and	Risk awareness gap analysis	To raise risk awareness and create excitement for the project.
	Risk maturity model	
	Risk awareness plan	
Communicate and consult with stakeholders to ensure that its risk management framework remains appropriate.	Risk improvement report	To improve the effectiveness of the ERM program.
RISK MANAGEMENT PROCESS		
Step 1: Communicate and consult	Stakeholder analysis	To identify the internal and external stakeholders for the organisation / division / department / project.
	Risk communication plan	To identify the most appropriate communication tools and establish timelines.
	Risk reports e.g. stress tests, risk & control self-assessments, incident reports, risk treatment plans, key risk indicator reports.	To ensure that the right information reaches the right people at the right time.
Step 2: Establish the context (Know your project / department / division)		
Establish the external context	External environment mind map	To describe the UNIQUE context for the risk management project.
	External stakeholder register	
	External stakeholder map	
Establish the internal context	Internal value chain mind map	
	Internal stakeholder register	
	Internal stakeholder map	
Establishing the context of the risk management process	Standardised risk management context (refer to building block III)	
Apply the risk criteria.	Standardised risk criteria (refer to building block III)	

Requirements	Deliverables	Purpose
RISK MANAGEMENT PROCESS		
Step 3: Risk identification	Key risk register (Top down)	Process of finding, recognising and describing risks.
	Divisional / Departmental / Project risk register (Bottom up)	
	Emerging risk register	
Step 4: Risk analysis	Key risk register (Top down)	Process to comprehend the nature of risk and to determine the level of risk (e.g. high, medium, low).
	Divisional / Departmental / Project risk register (Bottom up)	
Step 5: Risk evaluation	Key risk profile (Top down)	Process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable.
	Divisional / Departmental / Project risk profile (Bottom up)	
Step 6: Risk treatment	Risk treatment plans for KEY risks &	To identify the most appropriate risk treatment for the most significant risks.
	Risk treatment plans for divisional, departmental or project risks	
	List of controls	
	Risk treatment options	

INTERVIEWER NOTES:

General notes:

Suggestions:

INTERVIEW TRANSCRIPTION:

Building block 6: Monitor and review the ERM program performance

Question 6.1: Please confirm the requirements, deliverables and the purpose. If you would like to add or remove a component, then please explain.

6.1: **What.** The proposed requirements, deliverables and the purpose is detailed in the table below.

Requirements	Deliverables	Purpose
Monitoring activities by the Board		
The board should ensure continual risk monitoring by management	Risk governance framework	To ensure proper risk oversight.
	Risk management plan (monitoring roles and responsibilities)	To reduce role confusion and provide clear guidelines for risk monitoring.
	Status on risk management plan implementation	To periodically measure progress against, and deviation from, the risk management plan.
	Board risk committee performance evaluation	To ensure effectiveness and efficiency with regards to committee activities.
Review activities by the Board		
Review activities by the Board	Integrated report (risk and opportunities section)	To periodically review whether the risk management framework, policy and plan are still appropriate, given the organisations' external and internal context;
	Risk management plan implementation status report	To periodically measure progress against, and deviation from, the risk management plan.
	Risk improvement report	To periodically review whether the risk management framework, policy and plan are still appropriate, given the organisations' external and internal context;
Monitor the risk management framework		
The board should monitor that risks taken are within the tolerance and appetite levels.	Risk appetite status report	To ensure compliance with the risk appetite framework.
	Risk tolerance status report	To ensure compliance with the risk tolerance levels.
Measure risk management performance against indicators, which are periodically reviewed for appropriateness;	KRI performance report	To measure risk management performance against indicators, which are periodically reviewed for appropriateness;
Periodically measure progress against, and deviation from, the risk management plan;	Risk management plan implementation status report	To periodically measure progress against, and deviation from, the risk management plan.
Report on risk, progress with the risk management plan and how well the risk management policy is being followed;	Risk management policy compliance report	To report on risk, progress with the risk management plan and how well the risk management policy is being followed.
Monitor the level of risk awareness	Risk culture surveys	To track the improvement of risk awareness.

Requirements	Deliverables	Purpose
Review the risk management framework		
Periodically review whether the risk management framework, policy and plan are still appropriate, given the organizations' external and internal context;	Risk improvement report	To periodically review whether the risk management framework, policy and plan are still appropriate, given the organisations' external and internal context;
Review the effectiveness of the risk management framework.		
Monitor the risk management process		
Ensuring that controls are effective and efficient in both design and operation;	Risk treatment plans	To ensure that controls are effective and efficient in both design and operation.
Identifying emerging risks.	Emerging risk register	To identify emerging risks in the organisation's internal value chain and external environment.
Review the risk management process		
Analysing and learning lessons from events (including near-misses), changes, trends, successes and failures;	Variance and trend analysis	To analyse and learn lessons from events (including near-misses), changes, trends, successes and failures;
Detecting changes in the external and internal context, including changes to risk criteria and the risk itself which can require revision of risk treatments and priorities; and	Risk improvement report (List of internal, external, risk management process & risk criteria context changes)	To periodically review whether the risk management framework, policy and plan are still appropriate, given the organisations' external and internal context;
Obtaining further information to improve risk assessment.	Risk improvement report (risk assessment process & methodology)	To improve / change the risk assessment methodology based on practical experiences.

INTERVIEWER NOTES:

General notes:

Suggestions:

INTERVIEW TRANSCRIPTION:

Building block 7: Continual improvement of the ERM program

Question 7.1: Please confirm the requirements, deliverables and the purpose. If you would like to add or remove a component, then please explain

7.1: **What.** The proposed requirements, deliverables and the purpose is detailed in the table below.

Requirements	Deliverables	Purpose
Management should provide assurance to the board that the risk management plan is integrated in the daily activities of the company.	Integrated assurance report.	To inform the relevant committees and risk stakeholders of the level of assurance provided by assurance providers.
Internal audit should provide a written assessment of the effectiveness of the system of internal controls and risk management to the board.	Risk improvement report	To periodically review whether the risk management framework, policy and plan are still appropriate, given the organisations' external and internal context;

INTERVIEWER NOTES:

General notes:

Suggestions:

INTERVIEW TRANSCRIPTION:

MOVE FROM THE MODEL TO THE ERM PROGRAM IMPLEMENTATION BLUEPRINT



INTERVIEWER NOTES:

General notes:

Suggestions:

INTERVIEW TRANSCRIPTION:

PART 3: GENERAL COMMENTS OR SUGGESTIONS?

INTERVIEWER NOTES:

General notes:

Suggestions:

INTERVIEW TRANSCRIPTION:

THANK YOU!

ROUND 2 VALIDATION:
ADJUSTED ENTERPRISE RISK MANAGEMENT (ERM) IMPLEMENTATION MODEL
CONFIDENTIAL

Format: Questionnaire

Ethics clearance number: ECONIT-2016-038

Student: Ms Hermie le Roux

Student number: 11112891

Contact number: 084 777 2803

Email: applyerm@gmail.com

Degree: PhD (Risk Management)

Promotor: Dr Diana Viljoen

University: North-West University, Vaal Triangle Campus, Faculty of Economic Sciences and IT, School of Economic Sciences

PURPOSE OF ROUND 2 ERM IMPLEMENTATION MODEL CONFIRMATION PROCESS:

1. The ERM implementation model was adjusted with the comments and suggestions received from the experts during the 1st round of face-to-face semi-structured interviews.
2. The purpose of this document is to validate the components of the adjusted ERM implementation model.

OVERVIEW OF THE RESEARCH STUDY:

1. Title of the research study:

Development of an Enterprise risk management (ERM) program implementation model and - assessment tool

2. Contribution to the ERM body of knowledge:

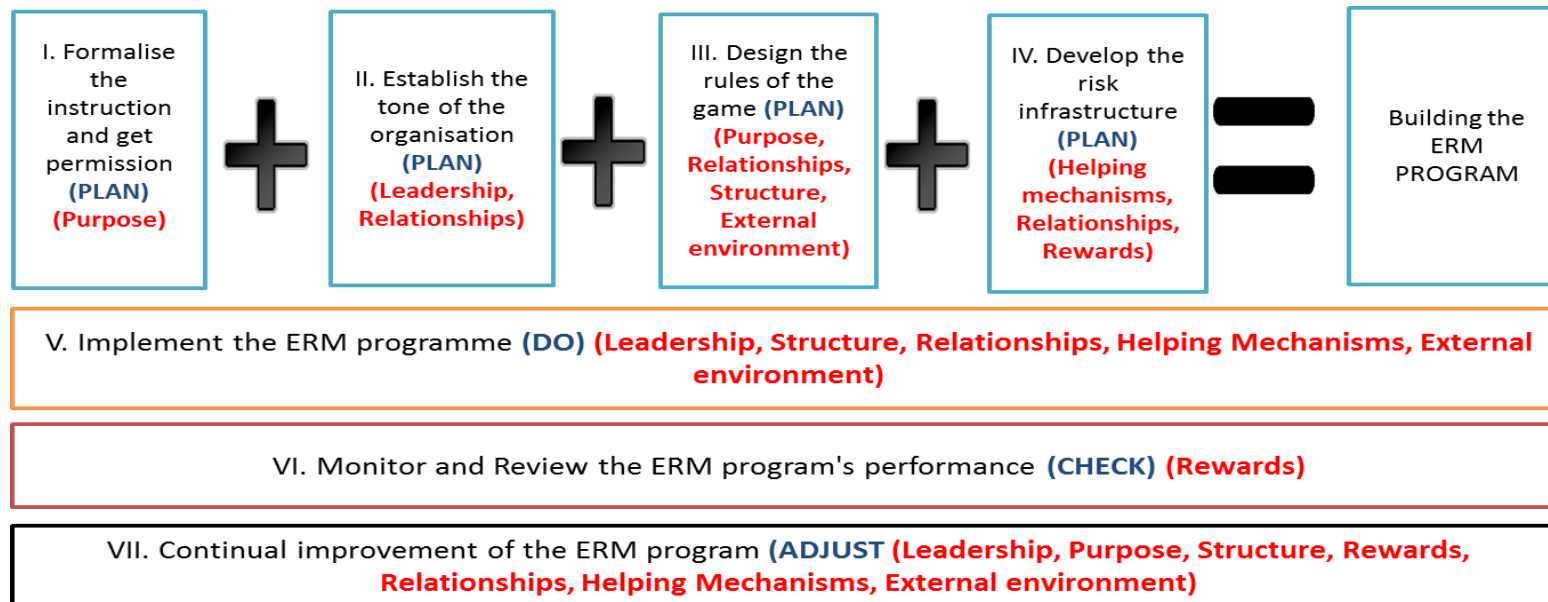
- There is limited academic research on how to implement enterprise risk management, and
- One of the barrier to ERM implementation is the misalignment between ERM program design and organisational design.

This research study is an attempt to improve the aforementioned gap and to address the barrier to ERM implementation.

3. Purpose of the ERM implementation model:

- To provide risk stakeholders with a standardised implementation model that can be used to determine the level of implementation of the ERM program;
- To reduce the barriers to ERM program implementation;
- To result in improved allocation of scarce risk resources; and
- To establish a common risk language.

The adjusted ERM implementation model:



Keys:

- Black font: ERM implementation model building blocks
- Blue font: Deming Cycle
- Red font: Weisbord's Six-box Model

Diagram 1: Adjusted Enterprise Risk Management (ERM) implementation model (based on ISO 31000, King III and ISO 31010)

The key question that should be addressed by each building block in the ERM program is as follows:

1. **Formalise the instruction and get permission:** does the organisation have to or want to implement ERM?
2. **Establish the tone of the organisation:** who is involved and how do we set the tone at each level of the organisation?
3. **Design the rules of the game:** what are the requirements of the risk management framework and risk management process?
4. **Develop the risk infrastructure:** which resources do we need to design and implement an ERM program?
5. **Implement the ERM program:** how do we implement the ERM program?
6. **Monitor and review:** how do we ensure effective and efficient risk management?
7. **Continual improvement:** which elements of the risk management framework and risk management process can be improved?

Building block I: Formalise the instruction and get permission

Task 1: Please confirm the adjusted ERM implementation model deliverables by marking agree / disagree column with an X. If you DISAGREE, then please explain in the comments column.

Building blocks		Best practice requirements				Proposed deliverables			Round 2		
Conceptual	Adjusted	Level 1		Level 2		Purpose	Conceptual ERM implementation model	Adjusted ERM implementation model	Agree	Dis-agree	Comments
		Conceptual ERM implementation model	Adjusted ERM implementation model	Conceptual ERM implementation model	Adjusted ERM implementation model						
I. Get permission.	I. Formalise the instruction and get permission.	Ensure legal and regulatory compliance.	Instruction / Trigger		Business trigger e.g. event, merger & acquisition due diligence requirement, peer pressure, etc.	To motivate the need for an ERM program.		Business case document			
					Ensure legal and regulatory compliance.	To motivate the need for an ERM program.	Compliance requirements (legal + regulatory + best practise frameworks)	Compliance register (legal + regulatory + best practise frameworks)			
		The board should delegate to management the responsibility to design, implement and monitor the risk management plan.	Permission / Mandate		The board should delegate to management the responsibility to design, implement and monitor the risk management plan.	To ask for permission / mandate to design and implement the ERM program.	Agenda item for Board meeting	Agenda item for the decision making forum e.g. Board meeting, Executive committee meeting.			
						To record the permission / mandate received to design and implement an ERM program.	Minutes of the Board meeting	Minutes of the decision making forum e.g. Board meeting, Executive committee meeting.			

Building blocks		Best practice requirements				Proposed deliverables			Round 2		
Conceptual	Adjusted	Level 1		Level 2		Purpose	Conceptual ERM implementation model	Adjusted ERM implementation model	Agree	Dis-agree	Comments
		Conceptual ERM implementation model	Adjusted ERM implementation model	Conceptual ERM implementation model	Adjusted ERM implementation model						
		The risk committee or audit committee should assist the board in carrying out its risk responsibilities	Oversight: the risk committee or audit committee should assist the board in carrying out its risk responsibilities	The board should appoint a committee responsible for risk.	The board should appoint a committee responsible for risk.	To assist the board in carrying out its risk roles and responsibilities.	Board risk committee (BRC) charter	Board risk committee (BRC) terms of reference / Audit committee charter / Audit and risk committee charter			
				The risk committee should:	The risk committee should:						
				consider the risk management policy and plan and monitor the risk management process;	consider the risk management policy and plan and monitor the risk management process;						
				have as its members executive and non-executive directors, members of senior management and independent risk management experts to be invited, if necessary;	have as its members executive and non-executive directors, members of senior management and independent risk management experts to be invited, if necessary;						
				have a minimum of three members; and	have a minimum of three members; and						

Building blocks		Best practice requirements				Proposed deliverables			Round 2		
Conceptual	Adjusted	Level 1		Level 2		Purpose	Conceptual ERM implementation model	Adjusted ERM implementation model	Agree	Dis-agree	Comments
		Conceptual ERM implementation model	Adjusted ERM implementation model	Conceptual ERM implementation model	Adjusted ERM implementation model						
				convene at least twice per year.	convene at least twice per year.						
				The board's responsibility for risk governance should be expressed in the board charter.	The board's responsibility for risk governance should be expressed in the board charter.						
		Define and endorse the risk management policy	Define and endorse the risk management policy	The board's responsibility for risk governance should manifest in a documented risk management policy and plan.	The board's responsibility for risk governance should manifest in a documented risk management policy and plan.	To document risk management scope, objectives and roles and responsibilities.					
				The board should approve the risk management policy and plan.	The board should approve the risk management policy and plan.		Risk management policy	Risk management policy			
				The risk management policy should be widely distributed throughout the company.	The risk management policy should be widely distributed throughout the company.						

Building block II: Establish the tone of the organisation

Task 2: Please confirm the adjusted ERM implementation model deliverables by marking agree / disagree column with an X. If you DISAGREE, then please explain in the comments column.

Building blocks		Best practice requirements				Proposed deliverables			Round 2		
Conceptual	Adjusted	Level 1		Level 2					Agree	Dis-agree	Comments
		Conceptual ERM implementation model	Adjusted ERM implementation model	Conceptual ERM implementation model	Adjusted ERM implementation model	Purpose	Conceptual ERM implementation model	Adjusted ERM implementation model			
II. Establish the tone of the organisation.	II. Establish the tone of the organisation.	Establishing the tone of the organisation: The introduction of risk management and ensuring its ongoing effectiveness require strong and sustained	Establishing the tone of the organisation: The introduction of risk management and ensuring its ongoing effectiveness require strong and sustained			A senior level ERM program sponsor / Chief Risk Officer should have clear authority over and accountability for oversight of risk across the enterprise	CRO / Senior level project sponsor	CRO / Senior level project sponsor			

Building blocks		Best practice requirements				Proposed deliverables			Round 2		
Conceptual	Adjusted	Level 1		Level 2					Agree	Dis-agree	Comments
		Conceptual ERM implementation model	Adjusted ERM implementation model	Conceptual ERM implementation model	Adjusted ERM implementation model	Purpose	Conceptual ERM implementation model	Adjusted ERM implementation model			
		commitment by management of the organisation, as well as strategic and rigorous planning to achieve commitment at all levels.	commitment by management of the organisation, as well as strategic and rigorous planning to achieve commitment at all levels.	(a) Ensure that the organisation's culture and risk management policy are aligned.	(a) Ensure that the organisation's culture and risk management policy are aligned.	To create risk awareness at all levels of the organisations and to encourage risk based decision making.	Risk management policy	Risk management policy / Risk requirements evident in business, project and HR requirements and standards / Strategic intent document / Risk communication strategy / Internal audit reports / External audit report / Insurance claims			
				(b) Determine risk management performance indicators that align with performance indicators of the organisation.	(b) Determine risk management performance indicators that align with performance indicators of the organisation.	To measure risk management performance against indicators, which are periodically reviewed for appropriateness;	Performance indicators (Key risk indicators)	Performance indicators (Key risk indicators)			
				(c) Align risk management objectives with the objectives	(c) Align risk management objectives with the objectives	To encourage a risk mind-set for decision making.	Risk appetite & risk tolerance	Strategic plan / Business plan / Risk plan / Risk management objectives / Risk			

Building blocks		Best practice requirements				Proposed deliverables			Round 2		
Conceptual	Adjusted	Level 1		Level 2					Agree	Dis-agree	Comments
		Conceptual ERM implementation model	Adjusted ERM implementation model	Conceptual ERM implementation model	Adjusted ERM implementation model	Purpose	Conceptual ERM implementation model	Adjusted ERM implementation model			
				and strategies of the organisation.	and strategies of the organisation.			appetite statement / Risk tolerance levels			
				(d) Assign accountabilities and responsibilities at appropriate levels within the organisation.	(d) Assign accountabilities and responsibilities at appropriate levels within the organisation.	To reduce role confusion by establishing clear roles and responsibilities for risk activities across businesses and risk types.	Risk governance model: (incl. risk owners' matrix, roles & responsibilities, reporting & escalation process & incentives guidelines.)	Risk governance model: (incl. risk owners' matrix, roles & responsibilities, reporting & escalation process & incentives guidelines & individual performance scorecard.)			
				(e) Ensure that the necessary resources are allocated to risk management.	(e) Ensure that the necessary resources are allocated to risk management.	To ensure the effective and efficient implementation of the ERM program.	Risk management plan (People, Processes and Budget)	Risk management plan (People, Processes and Budget) / Annual performance plan / Operational budget			
				(f) Communicate the benefits of risk management to all stakeholders.	(f) Communicate the benefits of risk management to all stakeholders.	To raise risk awareness and create excitement for the project.	Benefits of risk management	Risk training material / Business case / Risk management policy / Embedded in			

Building blocks		Best practice requirements				Proposed deliverables			Round 2		
Conceptual	Adjusted	Level 1		Level 2					Agree	Dis-agree	Comments
		Conceptual ERM implementation model	Adjusted ERM implementation model	Conceptual ERM implementation model	Adjusted ERM implementation model	Purpose	Conceptual ERM implementation model	Adjusted ERM implementation model			
								risk reports / Board risk report			
		The induction and ongoing training programs of the board should incorporate risk governance. (Note: apply to all the levels in the organisation)	The induction and ongoing training programs of the board should incorporate risk governance. (Note: apply to all the levels in the organisation)			To create a common risk language, improve risk awareness and encourage risk based decision making.	Risk awareness gap analysis	Risk awareness gap analysis			
							Risk maturity model	Risk maturity assessment			
							Risk awareness plan	Risk awareness strategy & plan			

Building block III: Design the rules of the game

Task 3: Please confirm the adjusted ERM implementation model deliverables by marking agree / disagree column with an X. If you DISAGREE, then please explain in the comments column.

Building blocks		Best practice requirements				Proposed deliverables			Round 2		
Conceptual	Adjusted	Level 1		Level 2					Agree	Dis-agree	Comments
		Conceptual ERM implementation model	Adjusted ERM implementation model	Conceptual ERM implementation model	Adjusted ERM implementation model	Purpose	Conceptual ERM implementation model	Adjusted ERM implementation model			
III. Design the rules of the game.	III. Design the rules of the game.	Design the risk management framework.	Design the risk management framework.	Task: Understanding the organisation and its context (Know your organisation)	Task: Understanding the organisation and its context (Know your organisation)						
				Establish the external context:	Establish the external context:	To get an overall picture of the external environment based PESTLE and / or Porter's 5 forces.					
				(a) the social and cultural, political, legal, regulatory, financial, technological, economic, natural and competitive environment, whether international, national, regional or local;	(a) the social and cultural, political, legal, regulatory, financial, technological, economic, natural and competitive environment, whether international, national, regional or local;		Environmental scanning report	Environmental scanning report			
				(b) key drivers and trends having impact on the objectives of the	(b) key drivers and trends having impact on the objectives of the		Key business drivers report	Key business drivers report			

Building blocks		Best practice requirements				Proposed deliverables			Round 2			
Conceptual	Adjusted	Level 1		Level 2					Agree	Dis-agree	Comments	
		Conceptual ERM implementation model	Adjusted ERM implementation model	Conceptual ERM implementation model	Adjusted ERM implementation model	Purpose	Conceptual ERM implementation model	Adjusted ERM implementation model				
				organisation; and	organisation; and							
				(c) External stakeholder analysis	(c) External stakeholder analysis		Stakeholder analysis	Stakeholder analysis				
				Establish the internal context:	Establish the internal context:	To describe the internal value chain of the organisation and to identify areas that would create risks and opportunities						
				(a) Governance, organisational structure, roles and accountabilities;	(a) Governance, organisational structure, roles and accountabilities;		Environmental scanning of the INTERNAL value chain	Environmental scanning of the INTERNAL value chain				
							SWOT analysis	SWOT analysis				
							Organisational organigram	Organisational organigram				
							Divisional organigram	Divisional organigram				
							Departmental organigram	Departmental organigram				
							Delegation of authority	Delegation of authority				
							Committee structure	Committee structure				
				Committee charters	Committee charters							
				(b) Policies, objectives, and the strategies that are in place to achieve them;	(b) Policies, objectives, and the strategies that are in place to achieve them;		List of policies	List of policies				
							Copy of policies	Copy of policies				
							Action plans (strategies)	Action plans (strategies)				
				(c) Capabilities, understood in terms of resources and knowledge (e.g.	(c) Capabilities, understood in terms of resources and knowledge (e.g.		Risk competency model	Risk competency model				
Job profiles / specification	Job profiles / specification											

Building blocks		Best practice requirements				Proposed deliverables			Round 2		
Conceptual	Adjusted	Level 1		Level 2					Agree	Dis-agree	Comments
		Conceptual ERM implementation model	Adjusted ERM implementation model	Conceptual ERM implementation model	Adjusted ERM implementation model	Purpose	Conceptual ERM implementation model	Adjusted ERM implementation model			
				capital, time, people, processes, systems and technologies);	capital, time, people, processes, systems and technologies);		Technical job specs	Technical job specs			
				(d) Information systems, information flows and decision making processes (both formal and informal)	(d) Information systems, information flows and decision making processes (both formal and informal)		List of systems	List of systems			
							Process maps	Process maps			
							Escalation policy	Escalation policy			
							Escalation process	Escalation process			
				Connected stakeholder analysis	Connected stakeholder analysis		Connected stakeholder analysis	Connected stakeholder analysis			
				(e) Internal stakeholder analysis	(e) Internal stakeholder analysis		Internal stakeholder analysis	Internal stakeholder analysis			
				(f) Temperature checks on organisational culture	(f) Temperature checks on organisational culture		Organisational culture survey results	Organisational culture survey results			
				(g) Standards, guidelines and models adopted by the organisation; and	(g) Standards, guidelines and models adopted by the organisation; and		List of standards, guidelines and models	List of standards, guidelines and models			
				(h) the form and extent of contractual relationships.	(h) the form and extent of contractual relationships.		Contracts register	Contracts register			
								Internal audit reports			

Building blocks		Best practice requirements				Proposed deliverables			Round 2		
Conceptual	Adjusted	Level 1		Level 2					Agree	Dis-agree	Comments
		Conceptual ERM implementation model	Adjusted ERM implementation model	Conceptual ERM implementation model	Adjusted ERM implementation model	Purpose	Conceptual ERM implementation model	Adjusted ERM implementation model			
								External audit reports			
								Strategic plan			
								Business plans			
				Establish the context of the risk management process (The context of the risk management process will vary according to the needs of an organisation. It can involve, but is not limited to:	Establish the context of the risk management process (The context of the risk management process will vary according to the needs of an organisation. It can involve, but is not limited to:	To create ONE set of risk management rules for the organisation.	Risk management file / manual that includes:	Risk management file / manual that includes:			
				(a) Defining the goals and objectives of the risk management activities;	(a) Defining the goals and objectives of the risk management activities;		Risk management goals & - objectives	Risk management goals & - objectives			
				(b) Defining responsibilities for and within the risk management process;	(b) Defining responsibilities for and within the risk management process;		Risk governance model	Risk governance model			
				(c) Defining the scope, as well as the depth and breadth of the risk	(c) Defining the scope, as well as the depth and breadth of the risk		Top-down & Bottom-up risk management activities	Top-down & Bottom-up risk management activities			

Building blocks		Best practice requirements				Proposed deliverables			Round 2		
Conceptual	Adjusted	Level 1		Level 2					Agree	Dis-agree	Comments
		Conceptual ERM implementation model	Adjusted ERM implementation model	Conceptual ERM implementation model	Adjusted ERM implementation model	Purpose	Conceptual ERM implementation model	Adjusted ERM implementation model			
				management activities to be carried out, including specific inclusions and exclusions;	management activities to be carried out, including specific inclusions and exclusions;						
				(e) Defining the activity, process, function, project, product, service or asset in terms of time and location;	(e) Defining the activity, process, function, project, product, service or asset in terms of time and location;						
				(f) Defining the relationships between a particular project, process or activity and other projects, processes or activities of the organisation;	(f) Defining the relationships between a particular project, process or activity and other projects, processes or activities of the organisation;						
				(g) Defining the risk assessment methodologies;	(g) Defining the risk assessment methodologies;						
				(h) Defining the way performance and effectiveness is evaluated in the management of risk;	(h) Defining the way performance and effectiveness is evaluated in the management of risk;						
							Interconnected-ness maps	Interconnected-ness maps			
							Risk assessment methodologies	Risk assessment methodologies			
							Key risk indicators	Key risk indicators			

Building blocks		Best practice requirements				Proposed deliverables			Round 2		
Conceptual	Adjusted	Level 1		Level 2					Agree	Dis-agree	Comments
		Conceptual ERM implementation model	Adjusted ERM implementation model	Conceptual ERM implementation model	Adjusted ERM implementation model	Purpose	Conceptual ERM implementation model	Adjusted ERM implementation model			
				(i) Identifying and specifying the decisions that have to be made; and	(i) Identifying and specifying the decisions that have to be made; and		Decision matrix	Decision matrix			
				(j) Identifying, scoping or framing studies needed, their extent and objectives, and the resources required for such studies.	(j) Identifying, scoping or framing studies needed, their extent and objectives, and the resources required for such studies.		Research to clarify context	Research to clarify context			
				Define the risk criteria (When defining risk criteria, factors to be considered should include the following:	Define the risk criteria (When defining risk criteria, factors to be considered should include the following:	To create standardised risk assessment criteria for the organisation as a whole. To give risk owners and other risk stakeholders insight into risk management in their terms.	Risk management file / manual that includes:	Risk management file / manual that includes:			
				(a) The nature and types of causes and consequences that can occur and how they will be measured;	(a) The nature and types of causes and consequences that can occur and how they will be measured;		Examples of causes and consequences	Examples of causes and consequences			
				(b) How likelihood will be defined;	(b) How likelihood will be defined;		Risk assessment tools and techniques	Risk assessment tools and techniques			
				(c) The timeframe(s) of the likelihood	(c) The timeframe(s) of the likelihood		Risk management plan	Risk management plan			

Building blocks		Best practice requirements				Proposed deliverables			Round 2		
Conceptual	Adjusted	Level 1		Level 2					Agree	Dis-agree	Comments
		Conceptual ERM implementation model	Adjusted ERM implementation model	Conceptual ERM implementation model	Adjusted ERM implementation model	Purpose	Conceptual ERM implementation model	Adjusted ERM implementation model			
				and/or consequence(s);	and/or consequence(s);						
				(d) How the level of risk is to be determined;	(d) How the level of risk is to be determined;		Risk appetite guidelines	Risk appetite guidelines			
				(e) The views of stakeholders;	(e) The views of stakeholders;		Risk tolerance levels guidelines	Risk tolerance levels guidelines			
				(f) The level at which risk becomes acceptable or tolerable; and	(f) The level at which risk becomes acceptable or tolerable; and						
				(g) Whether combinations of multiple risks should be taken into account and, if so, how and which combinations should be considered.	(g) Whether combinations of multiple risks should be taken into account and, if so, how and which combinations should be considered.						
				Task: establishing the risk management policy	Task: establishing the risk management policy	To document risk management scope, objectives and roles and responsibilities .	Risk management policy	Risk management policy			
				(a) A policy and plan for a system and process of risk management should be developed.	(a) A policy and plan for a system and process of risk management should be developed.						

Building blocks		Best practice requirements				Proposed deliverables			Round 2		
Conceptual	Adjusted	Level 1		Level 2							
		Conceptual ERM implementation model	Adjusted ERM implementation model	Conceptual ERM implementation model	Adjusted ERM implementation model	Purpose	Conceptual ERM implementation model	Adjusted ERM implementation model			
				(c) The board's responsibility for risk governance should manifest in a documented risk management policy and plan.	(c) The board's responsibility for risk governance should manifest in a documented risk management policy and plan.						
				(d) The board should approve the risk management policy and plan.	(d) The board should approve the risk management policy and plan.						
				The risk management policy should be widely distributed throughout the company.	The risk management policy should be widely distributed throughout the company.						
				Task: develop an accountability matrix / risk governance framework	Task: develop an accountability matrix / risk governance framework	To establish clear roles and responsibilities for risk activities across businesses and risk types.	Risk governance model: (incl. risk owners' matrix, roles & responsibilities, reporting & escalation process & incentives guidelines.)	Risk governance framework: (incl. risk owners' matrix, roles & responsibilities, reporting & escalation process & incentives guidelines & individual			
				(a) Identifying risk owners that have the accountability and authority to manage risks;	(a) Identifying risk owners that have the accountability and authority to manage risks;						

Building blocks		Best practice requirements				Proposed deliverables			Round 2		
Conceptual	Adjusted	Level 1		Level 2					Agree	Dis-agree	Comments
		Conceptual ERM implementation model	Adjusted ERM implementation model	Conceptual ERM implementation model	Adjusted ERM implementation model	Purpose	Conceptual ERM implementation model	Adjusted ERM implementation model			
				(b) Identifying who is accountable for the development, implementation and maintenance of the framework for managing risk;	(b) Identifying who is accountable for the development, implementation and maintenance of the framework for managing risk;			performance scorecards)			
				(c) Identifying other responsibilities of people at all levels in the organisation for the risk management process;	(c) Identifying other responsibilities of people at all levels in the organisation for the risk management process;						
				(d) Establishing performance measurement and external and/or internal reporting and escalation processes; and	(d) Establishing performance measurement and external and/or internal reporting and escalation processes; and						
				(e) Ensuring appropriate levels of recognition.	(e) Ensuring appropriate levels of recognition.						
				Task: integration into organisational processes	Task: integration into organisational processes	To embed risk management in all the organisation's					

Building blocks		Best practice requirements				Proposed deliverables			Round 2		
Conceptual	Adjusted	Level 1		Level 2					Agree	Dis-agree	Comments
		Conceptual ERM implementation model	Adjusted ERM implementation model	Conceptual ERM implementation model	Adjusted ERM implementation model	Purpose	Conceptual ERM implementation model	Adjusted ERM implementation model			
				Develop a common risk language	Develop a common risk language	practices and processes in a way that it is relevant, effective and efficient.	Common risk language	Common risk language			
				Risk management should be embedded in all the organisation's practices and processes in a way that it is relevant, effective and efficient.	Risk management should be embedded in all the organisation's practices and processes in a way that it is relevant, effective and efficient.		Risk owners	Risk owners			
							Strategic plan	Strategic plan			
							Business plan	Business plan			
							Financial plan	Financial plan			
							Risk & incident escalation process	Risk & incident escalation process			
								New products development			
								Operational processes			
								Investment decisions			
								Combined assurance			
								Performance management process			
								Change management process			
								Quality assurance process			
				Align risk management objectives with the objectives	Align risk management objectives with the objectives	To encourage a risk mind-set for decision making.	Risk appetite guidelines	Risk appetite guidelines			
							Risk tolerance levels guidelines	Risk tolerance levels guidelines			

Building blocks		Best practice requirements				Proposed deliverables			Round 2		
Conceptual	Adjusted	Level 1		Level 2					Agree	Dis-agree	Comments
		Conceptual ERM implementation model	Adjusted ERM implementation model	Conceptual ERM implementation model	Adjusted ERM implementation model	Purpose	Conceptual ERM implementation model	Adjusted ERM implementation model			
				and strategies of the organisation.	and strategies of the organisation.			Strategic plans			
								Business plans			
				Determine risk management performance indicators that align with performance indicators of the organisation.	Determine risk management performance indicators that align with performance indicators of the organisation.	To measure risk management performance against indicators, which are periodically reviewed for appropriateness;	Performance reporting metrics, i.e. key risk indicators	Performance reporting metrics, i.e. key risk indicators			
				Task: Establishing internal communication and reporting mechanisms	Task: Establishing internal communication and reporting mechanisms	To create one set of rules for risk communication and also to increase risk transparency.	Internal reporting guidelines	Internal reporting guidelines			
				(a) Key components of the risk management framework, and any subsequent modifications, are communicated appropriately;	(a) Key components of the risk management framework, and any subsequent modifications, are communicated appropriately;		Communication guidelines	Communication guidelines			
				(b) there is adequate internal reporting on the framework, its effectiveness	(b) there is adequate internal reporting on the framework, its effectiveness						

Building blocks		Best practice requirements				Proposed deliverables			Round 2		
Conceptual	Adjusted	Level 1		Level 2					Agree	Dis-agree	Comments
		Conceptual ERM implementation model	Adjusted ERM implementation model	Conceptual ERM implementation model	Adjusted ERM implementation model	Purpose	Conceptual ERM implementation model	Adjusted ERM implementation model			
				and the outcomes;	and the outcomes;						
				(c) relevant information derived from the application of risk management is available at appropriate levels and times; and	(c) relevant information derived from the application of risk management is available at appropriate levels and times; and						
				(d) there are processes for consultation with internal stakeholders.	(d) there are processes for consultation with internal stakeholders.						
				Task: Establishing external communication and reporting mechanisms	Task: Establishing external communication and reporting mechanisms	To create one set of rules for risk communication and also to increase risk transparency.	Integrated report: risks and opportunities section				
				(a) Engaging appropriate external stakeholders and ensuring an effective exchange of information;	(a) Engaging appropriate external stakeholders and ensuring an effective exchange of information;		External reporting guidelines	External reporting guidelines			
				(b) External reporting to comply with legal, regulatory,	(b) External reporting to comply with legal, regulatory,		Communication guidelines	Communication guidelines			

Building blocks		Best practice requirements				Proposed deliverables			Round 2		
Conceptual	Adjusted	Level 1		Level 2					Agree	Dis-agree	Comments
		Conceptual ERM implementation model	Adjusted ERM implementation model	Conceptual ERM implementation model	Adjusted ERM implementation model	Purpose	Conceptual ERM implementation model	Adjusted ERM implementation model			
				and governance requirements;	and governance requirements;						
				(c) Providing feedback and reporting on communication and consultation;	(c) Providing feedback and reporting on communication and consultation;						
		Design the risk management process.	Design the risk management process.	Step 1: Communication and consultation	Step 1: Communication and consultation	To develop a standardised risk management process for the organisation.	Risk management process guidelines	Risk management process guidelines			
				Step 2: Establish the context	Step 2: Establish the context						
				Step 3: Risk identification	Step 3: Risk identification						
				Step 4: Risk analysis	Step 4: Risk analysis						
				Step 5: Risk evaluation	Step 5: Risk evaluation						
				Step 6: Risk treatment	Step 6: Risk treatment						
				Step 7: Monitor and review	Step 7: Monitor and review						
Step 8: Continuous improvement	Step 8: Continuous improvement										

Building block IV: Develop the risk infrastructure

Task 4: Please confirm the adjusted ERM implementation model deliverables by marking agree / disagree column with an X. If you DISAGREE, then please explain in the comments column.

Building blocks		Best practice requirements				Proposed deliverables			Round 2		
Conceptual	Adjusted	Level 1		Level 2					Agree	Dis-agree	Comments
		Conceptual ERM implementation model	Adjusted ERM implementation model	Conceptual ERM implementation model	Adjusted ERM implementation model	Purpose	Conceptual ERM implementation model	Adjusted ERM implementation model			
IV. Develop the risk infrastructure.	IV. Develop the risk infrastructure.	Task: Allocate appropriate resources for risk management	Task: Allocate appropriate resources for risk management								
		People (skills, experience, competence & training programs).	People (skills, experience, competence & training programs).	People: skills, experience, competence & training programs	People: skills, experience, competence & training programs	To establish decision making structures, escalation protocol & identify risk stakeholders.	Risk governance models	Risk governance models			
								Performance management scorecards			
						To identify competencies, skills levels and experience required by risk stakeholders.	Risk competency model	Job profiles			
						To ensure proper training for risk stakeholders.	Risk training	Risk training: induction sessions and risk awareness sessions			
		Committees: the board should	Committees: the board should	Board committees:	Board committees:	To formalise decision					

Building blocks		Best practice requirements				Proposed deliverables			Round 2		
Conceptual	Adjusted	Level 1		Level 2					Agree	Dis-agree	Comments
		Conceptual ERM implementation model	Adjusted ERM implementation model	Conceptual ERM implementation model	Adjusted ERM implementation model	Purpose	Conceptual ERM implementation model	Adjusted ERM implementation model			
		delegate certain functions to well-structured committees but without abdicating its own responsibilities.	delegate certain functions to well-structured committees but without abdicating its own responsibilities.	Formal terms of reference should be established and approved for each committee of the board.	Formal terms of reference should be established and approved for each committee of the board.	making structures, escalation protocol & identify risk stakeholders.	Board committees' charter / terms of reference	Board committees' charter / terms of reference			
				The committees' terms of reference should be reviewed yearly.	The committees' terms of reference should be reviewed yearly.						
				The committees should be appropriately constituted and the composition and the terms of reference should be disclosed in the integrated report.	The committees should be appropriately constituted and the composition and the terms of reference should be disclosed in the integrated report.		Integrated report	Integrated report			
				The risk committee should:	The risk committee should:						
				consider the risk management policy and plan and monitor the risk	consider the risk management policy and plan and monitor the risk						
							Board risk committee charter	Board risk committee terms of reference			

Building blocks		Best practice requirements				Proposed deliverables			Round 2		
Conceptual	Adjusted	Level 1		Level 2					Agree	Dis-agree	Comments
		Conceptual ERM implementation model	Adjusted ERM implementation model	Conceptual ERM implementation model	Adjusted ERM implementation model	Purpose	Conceptual ERM implementation model	Adjusted ERM implementation model			
				management process;	management process;						
				have as its members' executive and non-executive directors, members of senior management and independent risk management experts to be invited, if necessary;	have as its members' executive and non-executive directors, members of senior management and independent risk management experts to be invited, if necessary;		Executive risk committee charter	Executive risk committee terms of reference			
				have a minimum of three members; and	have a minimum of three members; and		Departmental risk committee charter	Departmental risk committee terms of reference			
				convene at least twice per year.	convene at least twice per year.			Audit and risk committee			
				The audit committee should:	The audit committee should:						
				oversee integrated reporting.	oversee integrated reporting.						
				have regard to all factors and risks that may impact on the	have regard to all factors and risks that may impact on the		Audit committee charter	Audit committee charter			

Building blocks		Best practice requirements				Proposed deliverables			Round 2		
Conceptual	Adjusted	Level 1		Level 2					Agree	Dis-agree	Comments
		Conceptual ERM implementation model	Adjusted ERM implementation model	Conceptual ERM implementation model	Adjusted ERM implementation model	Purpose	Conceptual ERM implementation model	Adjusted ERM implementation model			
				integrity of the integrated report.	integrity of the integrated report.						
				review and comment on the financial statements included in the integrated report.	review and comment on the financial statements included in the integrated report.						
				review the disclosure of sustainability issues in the integrated report to ensure that it is reliable and does not conflict with the financial information.	review the disclosure of sustainability issues in the integrated report to ensure that it is reliable and does not conflict with the financial information.						
				recommend to the board to engage an external assurance provider on material sustainability issues.	recommend to the board to engage an external assurance provider on material sustainability issues.						
				consider the need to issue interim results.	consider the need to issue interim results.						
				review the content of the summarised information.	review the content of the summarised information.						

Building blocks		Best practice requirements				Proposed deliverables			Round 2		
Conceptual	Adjusted	Level 1		Level 2					Agree	Dis-agree	Comments
		Conceptual ERM implementation model	Adjusted ERM implementation model	Conceptual ERM implementation model	Adjusted ERM implementation model	Purpose	Conceptual ERM implementation model	Adjusted ERM implementation model			
				engage the external auditors to provide assurance on the summarised financial information.	engage the external auditors to provide assurance on the summarised financial information.						
				ensure that a combined assurance model is applied to provide a coordinated approach to all assurance activities.	ensure that a combined assurance model is applied to provide a coordinated approach to all assurance activities.						
				ensure that the combined assurance is received is appropriate to address all the significant risks facing the company.	ensure that the combined assurance is received is appropriate to address all the significant risks facing the company.						
				monitor the relationship between the external assurance providers and the company.	monitor the relationship between the external assurance providers and the company.						
				The audit committee should be an integral	The audit committee should be an integral						

Building blocks		Best practice requirements				Proposed deliverables			Round 2		
Conceptual	Adjusted	Level 1		Level 2					Agree	Dis-agree	Comments
		Conceptual ERM implementation model	Adjusted ERM implementation model	Conceptual ERM implementation model	Adjusted ERM implementation model	Purpose	Conceptual ERM implementation model	Adjusted ERM implementation model			
				component of the risk management process.	component of the risk management process.						
				The charter of the audit committee should set out its responsibilities regarding risk management.	The charter of the audit committee should set out its responsibilities regarding risk management.						
				The audit committee should specifically have oversight of:	The audit committee should specifically have oversight of:						
				financial reporting risks;	financial reporting risks;						
				internal financial controls;	internal financial controls;						
				fraud risks as it relates to financial reporting; and	fraud risks as it relates to financial reporting; and						
				IT risks as it relates to financial reporting.	IT risks as it relates to financial reporting.						
				The audit committee should also:	The audit committee should also:		Integrated assurance	Combined assurance			

Building blocks		Best practice requirements				Proposed deliverables			Round 2		
Conceptual	Adjusted	Level 1		Level 2					Agree	Dis-agree	Comments
		Conceptual ERM implementation model	Adjusted ERM implementation model	Conceptual ERM implementation model	Adjusted ERM implementation model	Purpose	Conceptual ERM implementation model	Adjusted ERM implementation model			
				ensure that a combined assurance model is applied to provide a coordinated approach to all assurance activities	ensure that a combined assurance model is applied to provide a coordinated approach to all assurance activities		committee charter	committee terms of reference			
				ensure that the combined assurance is received is appropriate to address all the significant risks facing the company.	ensure that the combined assurance is received is appropriate to address all the significant risks facing the company.						
		Models & tools: the organisation's processes, methods and tools to be used for managing risk	Models & tools: the organisation's processes, methods and tools to be used for managing risk			To assess and decide on standardised tools that should be used across the organisation.		Risk specific committee terms of reference e.g. Fraud risk committee			
							Risk identification tools	Risk identification tools			
							Risk analysis tools	Risk analysis tools			
							Risk evaluation tools	Risk evaluation tools			
							Risk treatment tools	Risk response tools			
							Risk monitoring tools	Risk monitoring tools			
							Risk reporting tools	Risk reporting tools			

Building blocks		Best practice requirements				Proposed deliverables			Round 2		
Conceptual	Adjusted	Level 1		Level 2					Agree	Dis-agree	Comments
		Conceptual ERM implementation model	Adjusted ERM implementation model	Conceptual ERM implementation model	Adjusted ERM implementation model	Purpose	Conceptual ERM implementation model	Adjusted ERM implementation model			
							Models	Risk quantification models			
		Templates: standardised recording, reporting and assessment templates	Templates: standardised recording, reporting and assessment templates			To standardise policy, framework, recording, reporting and assessment templates.	Examples:	Examples:			
							Risk management plan	Risk management plan			
							Risk communication plan	Risk communication plan			
							Stakeholder maps	Stakeholder maps			
							Stakeholder register	Stakeholder register			
							Risk register	Risk register			
							Risk improvement report	Risk improvement report			
							Integrated assurance dashboard	Integrated assurance dashboard			
							Integrated report	Integrated report			
							Risk self-assessments	Risk self-assessments			
							Stewardship report	Stewardship report			
							Recording process	Recording process			
								Risk acceptance form			

Building blocks		Best practice requirements				Proposed deliverables			Round 2		
Conceptual	Adjusted	Level 1		Level 2					Agree	Dis-agree	Comments
		Conceptual ERM implementation model	Adjusted ERM implementation model	Conceptual ERM implementation model	Adjusted ERM implementation model	Purpose	Conceptual ERM implementation model	Adjusted ERM implementation model			
								Risk retirement form			
								Reporting dashboards			
								Reporting scorecards			
								Risk policy			
								Risk management framework			
								Risk committee terms of reference			
		Processes: documented processes and procedures.	Processes: documented processes and procedures.			To embed risk management in all the organisation's practices and processes in a way that it is relevant, effective and efficient.	Common risk language	Common risk language			
							Risk owners' matrix	Risk owners' matrix			
							Strategic planning process	Strategic planning process			
							Business planning process	Business planning process			
							Financial planning process	Financial planning process			
							Change management process	Change management process			
							Quality assurance process	Quality assurance process			
							Risk management process	Risk management process			

Building blocks		Best practice requirements				Proposed deliverables			Round 2		
Conceptual	Adjusted	Level 1		Level 2					Agree	Dis-agree	Comments
		Conceptual ERM implementation model	Adjusted ERM implementation model	Conceptual ERM implementation model	Adjusted ERM implementation model	Purpose	Conceptual ERM implementation model	Adjusted ERM implementation model			
							Risk & incident escalation process	Risk & incident escalation process			
								External audit process			
								Performance management process			
		Systems: information and knowledge management systems	Systems: information and knowledge management systems			To select the most appropriate risk management systems.	Risk recording	Risk recording			
							Risk reporting	Risk reporting			
							Risk monitoring	Risk monitoring			
							Risk review	Risk review			

Building block V: Implement the ERM program

Task 5: Please confirm the adjusted ERM implementation model deliverables by marking agree / disagree column with an X. If you DISAGREE, then please explain in the comments column.

Building blocks		Best practice requirements				Proposed deliverables			Round 2		
Conceptual	Adjusted	Level 1		Level 2					Agree	Dis-agree	Comments
		Conceptual ERM implementation model	Adjusted ERM implementation model	Conceptual ERM implementation model	Adjusted ERM implementation model	Purpose	Conceptual ERM implementation model	Adjusted ERM implementation model			
V. Implementation.	V. Implement the ERM program.	Implementing the framework for managing risk.	Implementing the framework for managing risk.	Define the appropriate timing and strategy for implementing the framework;	Define the appropriate timing and strategy for implementing the framework;	To establish a time line for risk management activities.	Risk management plan (calendar)	Risk management plan (calendar)			
								Critical path analysis for key dependencies			
				Apply the risk management policy and process to the organisational processes;	Apply the risk management policy and process to the organisational processes;	To embed risk management in all the organisation's practices and processes in a way that it is relevant, effective and efficient.	Integration of the risk into organisational processes	Common risk language			
								Risk owners' matrix			
								Strategic planning process			
								Business planning process			
								Financial planning process			
								Change management process			
								Quality assurance process			

Building blocks		Best practice requirements				Proposed deliverables			Round 2		
Conceptual	Adjusted	Level 1		Level 2							
		Conceptual ERM implementation model	Adjusted ERM implementation model	Conceptual ERM implementation model	Adjusted ERM implementation model	Purpose	Conceptual ERM implementation model	Adjusted ERM implementation model			
								Risk management process			
								Risk & incident escalation process			
								Performance management process			
				Comply with legal and regulatory requirements;	Comply with legal and regulatory requirements;	To communicate risk related compliance requirements.	Legal, regulatory & best practice compliance register (pertaining to risk)	Legal, regulatory & best practice compliance register (pertaining to risk)			
				Ensure that decision making, including the development and setting of objectives, is aligned with the outcomes of risk management processes;	Ensure that decision making, including the development and setting of objectives, is aligned with the outcomes of risk management processes;	To encourage a risk mind-set for decision making.	Risk appetite statements	Risk appetite statements			
							Risk tolerance levels	Risk tolerance levels			
								Strategic plan			
								ERM framework & policy			
				Hold information and training sessions; and	Hold information and training sessions; and	To create a common risk language, improve risk awareness and encourage risk based decision making.	Risk awareness gap analysis	Risk awareness gap analysis			
							Risk maturity model	Risk maturity assessment			
							Risk awareness plan	Risk awareness strategy & -plan			

Building blocks		Best practice requirements				Proposed deliverables			Round 2		
Conceptual	Adjusted	Level 1		Level 2					Agree	Dis-agree	Comments
		Conceptual ERM implementation model	Adjusted ERM implementation model	Conceptual ERM implementation model	Adjusted ERM implementation model	Purpose	Conceptual ERM implementation model	Adjusted ERM implementation model			
				Communicate and consult with stakeholders to ensure that its risk management framework remains appropriate.		To ensure that the risk management framework remains appropriate.	Risk facilitation sessions	Risk facilitation sessions			
		Implementing the risk management process	Implementing the risk management process.	Step 1: Communication and consultation with external and internal stakeholders should take place during all stages of the risk management process.	Step 1: Communication and consultation with external and internal stakeholders should take place during all stages of the risk management process.	To identify the internal and external stakeholders for the organisation / division / department / project.	Stakeholder analysis	Stakeholder analysis			
						To identify the most appropriate communication tools and establish timelines.	Risk communication plan	Risk communication plan			
						To ensure that the right information reaches the right people at the right time.	Risk reports e.g. stress tests, risk & control self-assessments, incident reports, risk treatment plans, key risk indicator reports.	Risk reports e.g. stress tests, risk & control self-assessments, incident reports, risk treatment plans, key risk indicator reports.			

Building blocks		Best practice requirements				Proposed deliverables			Round 2		
Conceptual	Adjusted	Level 1		Level 2					Agree	Dis-agree	Comments
		Conceptual ERM implementation model	Adjusted ERM implementation model	Conceptual ERM implementation model	Adjusted ERM implementation model	Purpose	Conceptual ERM implementation model	Adjusted ERM implementation model			
				Step 2: Establish the context (Know your organisation / division / department / project / risk type)	Step 2: Establish the context (Know your organisation / division / department / project / risk type)	To describe the UNIQUE context for the risk management project.					
							External environment mind map	External environment mind map			
				Establish the external context	Establish the external context		External stakeholder register	External stakeholder register			
							External stakeholder map	External stakeholder map			
				Establish the internal context	Establish the internal context		Internal value chain mind map	Internal value chain mind map			
							Internal stakeholder register	Internal stakeholder register			
							Internal stakeholder map	Internal stakeholder map			
				Establishing the context of the risk management process	Establishing the context of the risk management process		Standardised risk management context (refer to building block III)	Standardised risk management context (refer to building block III)			
				Apply the risk criteria	Apply the risk criteria	Standardised risk criteria (refer to building block III)	Standardised risk criteria (refer to building block III)				

Building blocks		Best practice requirements				Proposed deliverables			Round 2		
Conceptual	Adjusted	Level 1		Level 2					Agree	Dis-agree	Comments
		Conceptual ERM implementation model	Adjusted ERM implementation model	Conceptual ERM implementation model	Adjusted ERM implementation model	Purpose	Conceptual ERM implementation model	Adjusted ERM implementation model			
				Step 3: Risk identification	Step 3: Risk identification	Process of finding, recognising and describing risks.	Key / Principle / Strategic risk register	Key / Principle / Strategic risk register			
							Divisional / departmental / business unit risk register	Divisional / departmental / business unit risk register			
							Emerging risk register	Emerging risk register			
								Risk library			
				Step 4: Risk analysis	Step 4: Risk analysis	Process to comprehend the nature of risk and to determine the level of risk (e.g. high, medium, low).					
							Key / Principle / Strategic risk register - risk ratings applied	Key / Principle / Strategic risk register - risk ratings applied			
							Divisional / departmental / business unit risk register - risk ratings applied	Divisional / departmental / business unit risk register - risk ratings applied			
								Root cause analysis			
				Step 5: Risk evaluation	Step 5: Risk evaluation	Process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is	Key / Principle / Strategic risk profile - risk ratings + current controls applied & risk owners identified	Key / Principle / Strategic risk profile - risk ratings + current controls applied & risk owners identified			
							Divisional / departmental / business unit	Divisional / departmental / business unit			

Building blocks		Best practice requirements				Proposed deliverables			Round 2		
Conceptual	Adjusted	Level 1		Level 2					Agree	Dis-agree	Comments
		Conceptual ERM implementation model	Adjusted ERM implementation model	Conceptual ERM implementation model	Adjusted ERM implementation model	Purpose	Conceptual ERM implementation model	Adjusted ERM implementation model			
						acceptable or tolerable.	risk register risk ratings + current controls applied & risk owners identified	risk register risk ratings + current controls applied & risk owners identified			
				Step 6: Risk treatment	Step 6: Risk response	To identify the most appropriate risk treatment for the most significant risks.	List of risk controls	Controls library			
							Risk treatment plans	Risk response plans / Action plans			
							Risk treatment options	Risk response options			

Building block VI: Monitor and review the ERM program performance

Task 6: Please confirm the adjusted ERM implementation model deliverables by marking agree / disagree column with an X. If you DISAGREE, then please explain in the comments column.

Building blocks		Best practice requirements				Proposed deliverables			Round 2		
Conceptual	Adjusted	Level 1		Level 2					Agree	Dis-agree	Comments
		Conceptual ERM implementation model	Adjusted ERM implementation model	Conceptual ERM implementation model	Adjusted ERM implementation model	Purpose	Conceptual ERM implementation model	Adjusted ERM implementation model			
VI. Monitor & review.	VI. Monitor and review the ERM program.	Monitoring activities by the Board	Monitoring activities by the Board	The board should ensure continual risk monitoring by management	The board should ensure continual risk monitoring by management	To ensure proper risk oversight.	Risk governance framework	Risk governance framework			
				The board should ensure that effective and continual monitoring of risk management takes place.	The board should ensure that effective and continual monitoring of risk management takes place.	To reduce role confusion and provide clear guidelines for risk monitoring.	Risk management plan (monitoring roles and responsibilities)	Risk management plan (monitoring roles and responsibilities)			
				The responsibility for monitoring should be defined in the risk management plan.	The responsibility for monitoring should be defined in the risk management plan.	To periodically measure progress against, and deviation from, the risk management plan.	Status on risk management plan implementation	Status report on risk management plan implementation			
		Review activities by the Board	Review activities by the Board	The board should comment in the integrated report on the effectiveness of the system and process of risk management.	The board should comment in the integrated report on the effectiveness of the system and process of risk management.	To periodically review whether the risk management framework, policy and plan are still appropriate,	Integrated report (risk and opportunities section)	Integrated report (risk and opportunities section)			
								Annual board risk report			

Building blocks		Best practice requirements				Proposed deliverables			Round 2		
Conceptual	Adjusted	Level 1		Level 2					Agree	Dis-agree	Comments
		Conceptual ERM implementation model	Adjusted ERM implementation model	Conceptual ERM implementation model	Adjusted ERM implementation model	Purpose	Conceptual ERM implementation model	Adjusted ERM implementation model			
						given the organisations' external and internal context;					
				The board should ensure that effective and continual monitoring of risk management takes place.	The board should ensure that effective and continual monitoring of risk management takes place.	To periodically measure progress against, and deviation from, the risk management plan.	Risk management plan implementation status report	Risk management plan implementation status report			
				The board should review the implementation of the risk management plan at least once a year.	The board should review the implementation of the risk management plan at least once a year.	To periodically review whether the risk management framework, policy and plan are still appropriate, given the organisations' external and internal context;	Risk improvement report	Risk improvement report			
								Internal audit report			
				The performance of the committee should be evaluated once a year by the board.	The performance of the committee should be evaluated once a year by the board.	To ensure effectiveness and efficiency with regards to committee activities.	Board risk committee performance evaluation	Board risk committee performance evaluation			
		Monitor the risk management framework	Monitor the risk management framework	The board should monitor that risks taken are within the	The board should monitor that risks taken are within the	To ensure compliance with the risk appetite framework.	Risk appetite status report	Risk appetite status report			

Building blocks		Best practice requirements				Proposed deliverables			Round 2		
Conceptual	Adjusted	Level 1		Level 2					Agree	Dis-agree	Comments
		Conceptual ERM implementation model	Adjusted ERM implementation model	Conceptual ERM implementation model	Adjusted ERM implementation model	Purpose	Conceptual ERM implementation model	Adjusted ERM implementation model			
				tolerance and appetite levels.	tolerance and appetite levels.	To ensure compliance with the risk tolerance levels.	Risk tolerance status report	Risk tolerance status report			
				Measure risk management performance against indicators, which are periodically reviewed for appropriateness;	Measure risk management performance against indicators, which are periodically reviewed for appropriateness;	To measure risk management performance against indicators, which are periodically reviewed for appropriateness;	KRI performance report	KRI performance report			
				Periodically measure progress against, and deviation from, the risk management plan;	Periodically measure progress against, and deviation from, the risk management plan;	To periodically measure progress against, and deviation from, the risk management plan.	Risk management plan implementation status report	Risk management plan implementation status report			
				Report on risk, progress with the risk management plan and how well the risk management policy is being followed;	Report on risk, progress with the risk management plan and how well the risk management policy is being followed;	To report on risk, progress with the risk management plan and how well the risk management policy is being followed.	Risk management policy compliance report	Risk management policy compliance report			
				Monitor the level of risk awareness	Monitor the level of risk awareness	To track the improvement of risk awareness.		Deviations from risk management policy report			
								Risk culture surveys	Risk culture surveys		

Building blocks		Best practice requirements				Proposed deliverables			Round 2		
Conceptual	Adjusted	Level 1		Level 2					Agree	Dis-agree	Comments
		Conceptual ERM implementation model	Adjusted ERM implementation model	Conceptual ERM implementation model	Adjusted ERM implementation model	Purpose	Conceptual ERM implementation model	Adjusted ERM implementation model			
		Review the risk management framework	Review the risk management framework	Periodically review whether the risk management framework, policy and plan are still appropriate, given the organizations' external and internal context;	Periodically review whether the risk management framework, policy and plan are still appropriate, given the organizations' external and internal context;	To periodically review whether the risk management framework, policy and plan are still appropriate, given the organisations' external and internal context.	Risk improvement report	Risk improvement report			
					Internal audit report						
					Risk calendar						
				Risk improvement report	Risk improvement report						
					Subject matter expert gap analysis						
					Internal audit reports						
					Risk calendar						
					ISO 9000 reports						
				Risk improvement report	Internal audit reports, risk committee effectiveness, qualitative conversations, risk appetite and risk tolerance level breaches, signed letters of representation.						

Building blocks		Best practice requirements				Proposed deliverables			Round 2					
Conceptual	Adjusted	Level 1		Level 2					Agree	Dis-agree	Comments			
		Conceptual ERM implementation model	Adjusted ERM implementation model	Conceptual ERM implementation model	Adjusted ERM implementation model	Purpose	Conceptual ERM implementation model	Adjusted ERM implementation model						
		Monitor the risk management process	Monitor the risk management process	Ensuring that controls are effective and efficient in both design and operation.	Ensuring that controls are effective and efficient in both design and operation.	To ensure that controls are effective and efficient in both design and operation.	Risk treatment plans	Subject matter expert gap analysis						
								Combined assurance reports						
								Risk profile status reports						
								Internal audit reports						
								External audit reports						
				Review the risk management process	Review the risk management process	Analysing and learning lessons from events (including near-misses), changes, trends, successes and failures;	Analysing and learning lessons from events (including near-misses), changes, trends, successes and failures;	To identify emerging risks in the organisation's internal value chain and external environment.	Emerging risk register	Emerging risk register				
		Variance and trend analysis	Variance and trend analysis								Variance and trend analysis			
											Post mortem sessions			
											Environmental scanning			
											Risk reconciliation reports			
											Post loss analysis			

Building block VII: Continual improvement of the ERM program

Task 7: Please confirm the adjusted ERM implementation model deliverables by marking agree / disagree column with an X. If you DISAGREE, then please explain in the comments column.

Building blocks		Best practice requirements				Proposed deliverables			Round 2		
Conceptual	Adjusted	Level 1		Level 2					Agree	Dis-agree	Comments
		Conceptual ERM implementation model	Adjusted ERM implementation model	Conceptual ERM implementation model	Adjusted ERM implementation model	Purpose	Conceptual ERM implementation model	Adjusted ERM implementation model			
VII. Continual improvement.	VII. Continual improvement of the ERM program.	Management should provide assurance to the board that the risk management plan is integrated in the daily activities of the company.	Management should provide assurance to the board that the risk management plan is integrated in the daily activities of the company.			To inform the relevant committees and risk stakeholders of the level of assurance provided by assurance providers.	Integrated assurance report.	Combined assurance report.			
								Risk reports to various committees			
								Risk maturity assessment			
								Benchmarking assessments (peer reviews & best practice)			
		Internal audit should:	Internal audit should:			To periodically review whether the risk management framework, policy and plan are still appropriate, given the organisations' external and internal context;					
		provide a written assessment of the effectiveness of the system of internal controls and risk management to the board.	provide a written assessment of the effectiveness of the system of internal controls and risk management to the board.				Risk improvement report	Risk improvement report			
								Internal audit report			

Building blocks		Best practice requirements				Proposed deliverables			Round 2		
Conceptual	Adjusted	Level 1		Level 2					Agree	Dis-agree	Comments
		Conceptual ERM implementation model	Adjusted ERM implementation model	Conceptual ERM implementation model	Adjusted ERM implementation model	Purpose	Conceptual ERM implementation model	Adjusted ERM implementation model			
		detect changes in the external and internal context, including changes to risk criteria and the risk itself which can require revision of risk treatments and priorities; and	detect changes in the external and internal context, including changes to risk criteria and the risk itself which can require revision of risk treatments and priorities; and	Detecting changes in the external and internal context, including changes to risk criteria and the risk itself which can require revision of risk treatments and priorities; and	Detecting changes in the external and internal context, including changes to risk criteria and the risk itself which can require revision of risk treatments and priorities; and		Risk improvement report (List of internal, external, risk management process & risk criteria context changes)	Risk improvement report (List of internal, external, risk management process & risk criteria context changes)			
		obtaining further information to improve risk assessment.	obtaining further information to improve risk assessment.	Obtaining further information to improve risk assessment.	Obtaining further information to improve risk assessment.		Risk improvement report (risk assessment process & methodology)	Risk improvement report (risk assessment process & methodology)			

THANK YOU!

Addendum G: Phase 2 – Round 3: Confirmation of the proposed ERM implementation assessment tools



NORTH-WEST UNIVERSITY[®]
YUNIBESITHI YA BOKONE-BOPHIRIMA
NOORDWES-UNIVERSITEIT
VAAL TRIANGLE CAMPUS

PO Box 1174, Vanderbijlpark
South Africa 1900

Tel: 016 910-3111
Fax: 016 910-3116
Web: <http://www.nwu.ac.za>

Risk Management Department
Tel: 016 910-3403
Email: Diana.Viljoen@nwu.ac.za

**ROUND 3:
PROPOSED ENTERPRISE RISK MANAGEMENT (ERM)
IMPLEMENTATION ASSESSMENT TOOLS
CONFIDENTIAL**

Ethics clearance number: ECONIT-2016-038

Student: Ms Hermie le Roux

Student number: 11112891

Contact number: 084 777 2803

Email: applyerm@gmail.com

Degree: PhD (Risk Management)

Promotor: Dr Diana Viljoen

University: North-West University, Vaal Triangle Campus, Faculty of Economic Sciences and IT,
School of Economic Sciences

Dear Participant,

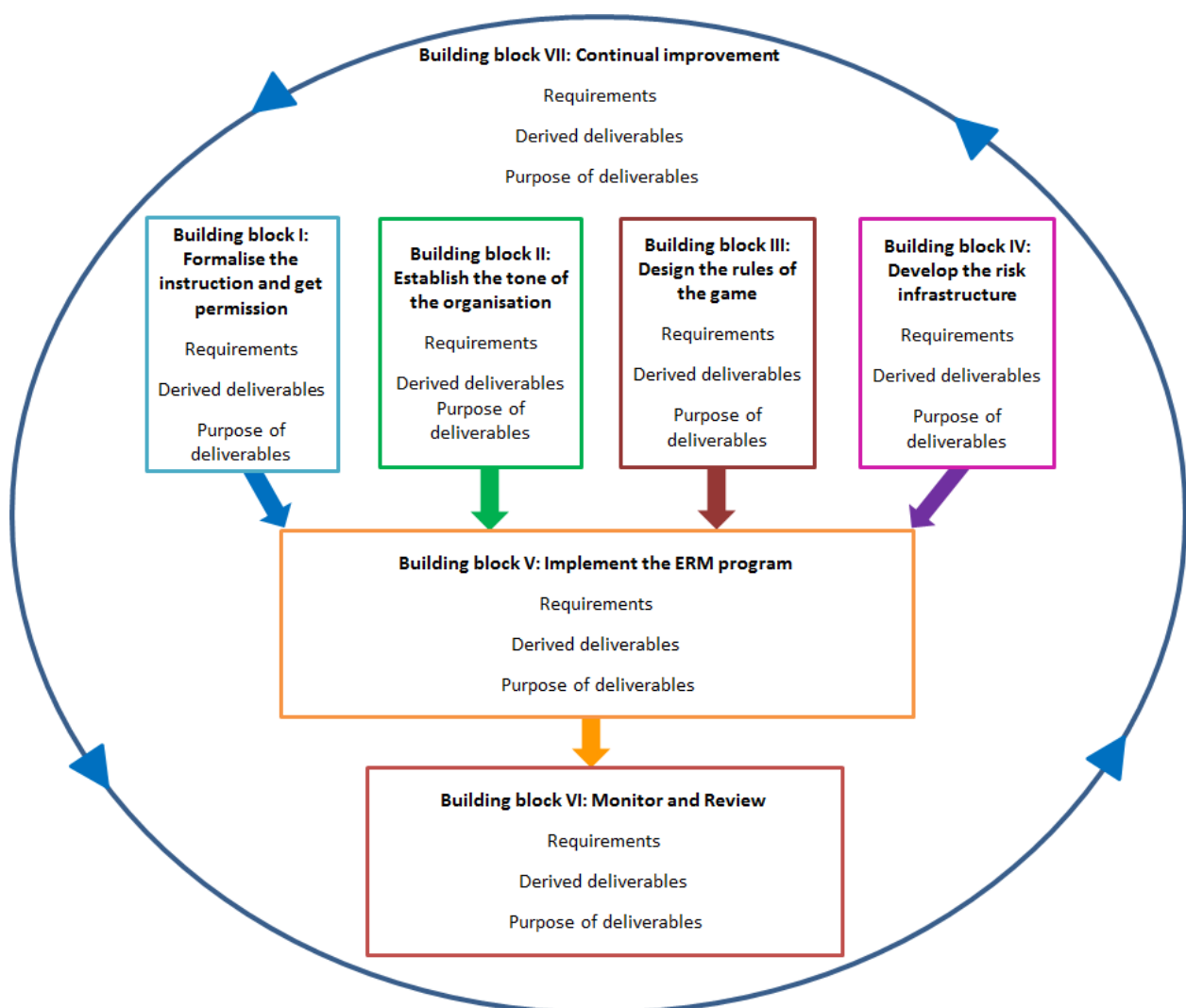
It is with gratitude that I send you this template for your final contribution to this research study.

Thank you so much for your valuable and much appreciated input during the first and second rounds of this process.

Adjusted ERM implementation model after round 1 and 2:

The adjusted and validated ERM implementation model, based on the results of the semi-structured interviews of round 1 and the e-mail confirmation during round 2, is as follows:

Figure 1: ERM implementation model



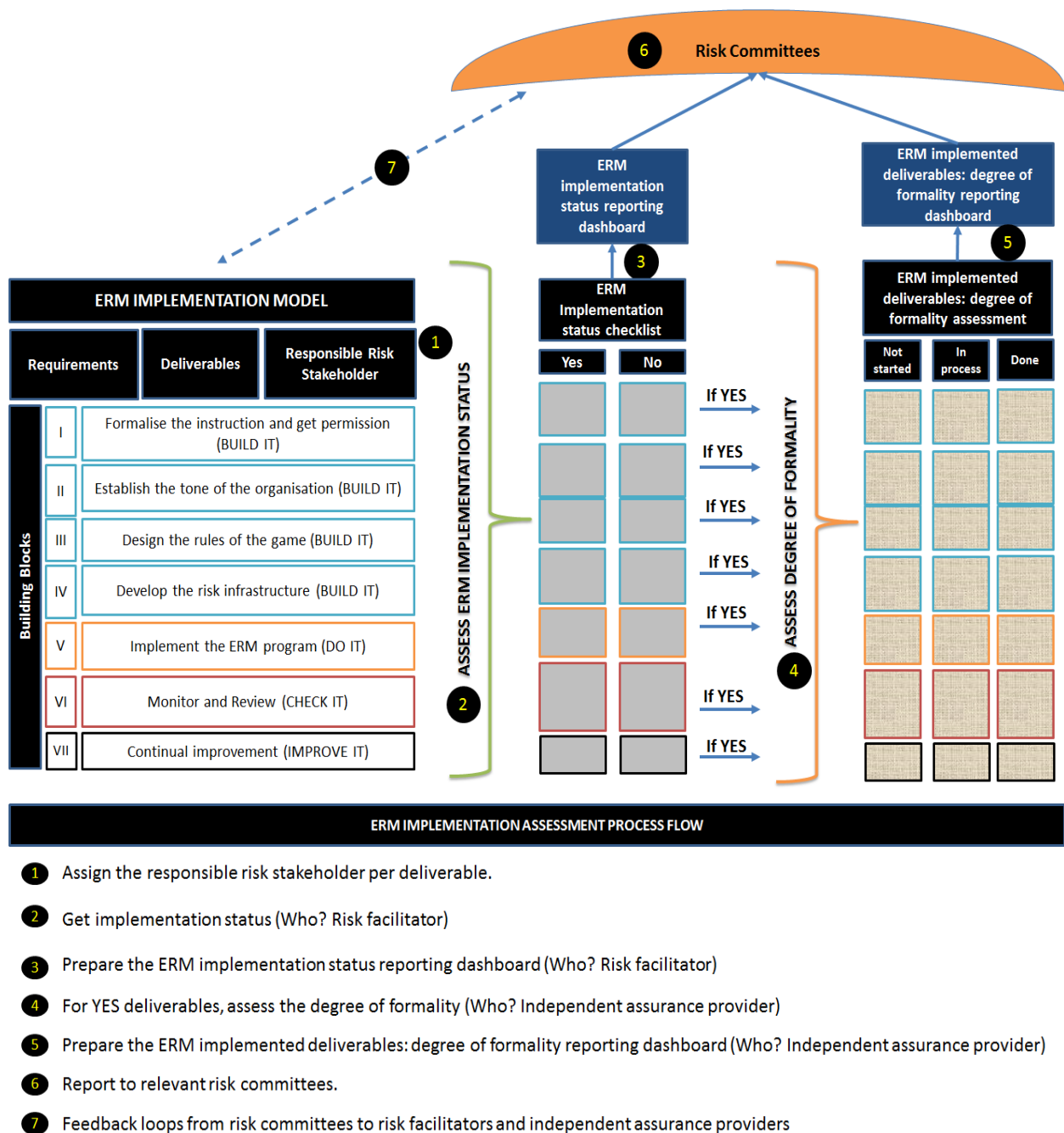
Source: Researcher's own compilation.

Purpose of round 3:

1. The purpose of round 3 of this study is to confirm the proposed overall process flow of the ERM implementation assessment checklist and the degree of formality reports from the responsible risk stakeholders to the independent risk function to the relevant risk committees.
2. The ERM implementation status checklist and the degree of formality assessment tool is based on the adjusted ERM implementation model (the building blocks, best practice requirements and the deliverables).
3. The researcher proposes two ERM implementation assessment tools:
 - a. **ERM implementation status checklist:** The checklist will be an extension of the ERM implementation model which consists of the building blocks, the associated requirements and the proposed deliverables. The first item to insert, is a column to pinpoint the responsible risk stakeholder(s) to design, develop and implement the respective deliverables. The appointment of these stakeholders will vary according to the organisational structure and design. For example, this could be the Chief Risk Officer (CRO), risk owners or the company secretary. The checklist uses a simple yes-no measurement scale. The measurement scale is used to determine the level of implementation of the ERM program, either per building block as per the conceptual ERM implementation model or per risk stakeholder. The coordination and facilitation of the completion of the checklist is the responsibility of the second line-of-defence (independent risk management and compliance) in the Protiviti risk governance model. The CRO will assign a risk facilitator to perform the task. The results of the checklists will be reported with an ERM implementation status reporting dashboard to the relevant risk committees.
 - b. **Degree of formality assessment tool:** The next step is to transfer all the implemented deliverables (the yes answers on the ERM implementation status checklist) to the degree of formality report. Degree of formality refers to the extent to which the different ERM implemented deliverables have been formalised. An independent assurer from the third line of defence of the risk governance model (Protiviti, 2013) will audit the implemented deliverables to confirm that it has been designed, developed and implemented by the relevant risk stakeholder. The degree of formality will be assessed with a (1) Not started, (2) In process and (3) Done measurement scale. This assessment tool is an attempt to reduce the bias involved when completing the ERM implementation status report in order to give assurance to the Board and senior management regarding the true status of the level of ERM implementation. The results will be reported with a degree of formality reporting dashboard to the relevant risk committees.

Part 1: Confirm the proposed ERM implementation status checklist and the degree of formality assessment tool

Figure 2: An overview of the proposed ERM implementation assessment tool



Source: Researcher's own compilation.

Question 1.1: Please confirm the proposed ERM assessment tools (i.e. ERM implementation status checklist and the ERM implemented deliverables: degree of formality assessment) in terms of the process flow and the implementation responsibilities.

Addendum H: Phase 2 - Round 1: Changes to the conceptual ERM implementation model suggested by the senior risk experts during the semi-structured interviews

Changes	Additions	Not accepted
---------	-----------	--------------

Theoretical frameworks		Building blocks		Best practice requirements								Proposed deliverables			Changes / additions suggested by:											Changes and additions			
Deming cycle	Weisbord organisational design model	Conceptual	Adjusted	Level 1				Level 2							IV1 (AdC)	IV2 (BG)	IV4 (EL)	IV6 (GS)	IV7 (GC)	IV8 (HG)	IV9 (HV)	IV13 (MF)	IV17 (SM)	IV18 (VP)	IV19 (WM)				
				Conceptual	Source	Ref.	Adjusted	Conceptual	Source	Ref.	Adjusted	Purpose	Conceptual	Adjusted															
Plan	Purpose, Leadership	I. Get permission.	I. Formalise the instruction and get permission.	Ensure legal and regulatory compliance.	ISO 31000	4.2	Instruction / Trigger				Business trigger e.g. event, merger & acquisition due diligence requirement, peer pressure, etc.	To motivate the need for an ERM program.		Business case document		x		x	x	x		x	x	x		IV1, IV4, IV6, IV7, IV9, IV13, IV17, IV18: The need for an ERM program can be triggered by any event such as a merger and acquisition. It can also originate from any level and a proper business case will then contain all the necessary details. Also include the benefits of risk management.			
											Ensure legal and regulatory compliance.	To motivate the need for an ERM program.	Compliance requirements (legal + regulatory + best practise frameworks)	Compliance register (legal + regulatory + best practise frameworks)		x		x			x			x			IV1, IV4, IV8, IV13 & IV17: Change compliance requirements to compliance register. IV2: For state owned enterprises (SOE's) the accounting officer is the accountable person.		
				The board should delegate to management the responsibility to design, implement and monitor the risk management plan.	King III	4.4	Permission / Mandate				The board should delegate to management the responsibility to design, implement and monitor the risk management plan.	To ask for permission / mandate to design and implement the ERM program.	Agenda item for Board meeting	Agenda item for the decision making body e.g. Board meeting, Executive committee meeting.							x						IV7: Add mandate to level 2 requirements. IV9: The decision making body for every type of organisation is different. By changing the words, the model becomes adaptable to each type of organisation and for each type of industry.		
												To record the permission / mandate received to design and implement an ERM program.	Minutes of the Board meeting	Minutes of the decision makingbody.g. Board meeting, Executive committee meeting.							x								
				The risk committee or audit committee should assist the board in carrying out its risk responsibilities	King III	4.3	Oversight: the risk committee or audit committee should assist the board in carrying out its risk responsibilities	The board should appoint a committee responsible for risk.	King III	4.3.1	The board should appoint a committee responsible for risk.	To assist the board in carrying out its risk roles and responsibilities.	Board risk committee (BRC) charter	Board risk committee (BRC) terms of reference / Audit committee charter / Audit and risk committee charter														IV4, IV8, IV19: The committee responsible for risk management can be a risk committee, audit committee or a board risk and audit committee. This will depend on the type of organisation and industry.	
								The risk committee should:		4.3.2	The risk committee should:																		
								consider the risk management policy and plan and monitor the risk management process;		4.3.2.1	consider the risk management policy and plan and monitor the risk management process;																		
								have as its members executive and non-executive directors, members of senior management and independent risk management experts to be invited, if necessary;		4.3.2.2	have as its members executive and non-executive directors, members of senior management and independent risk management experts to be invited, if necessary;							x		x									
								have a minimum of three members; and		4.3.2.3	have a minimum of three members; and																		
								convene at least twice per year.		4.3.2.4	convene at least twice per year.																		
				Define and endorse the risk management policy	King III	4.1.1	Define and endorse the risk management policy	The board's responsibility for risk governance should be expressed in the board charter.	King III	4.1.3	The board's responsibility for risk governance should be expressed in the board charter.	To document risk management scope, objectives and roles and responsibilities.	Risk management policy	Risk management policy															
								The board's responsibility for risk governance should manifest in a documented risk management policy and plan.		4.1.5	The board's responsibility for risk governance should manifest in a documented risk management policy and plan.																		
								The board should approve the risk management policy and plan.		4.1.6	The board should approve the risk management policy and plan.																		
	ISO 31000	4.2 & 4.3.2		The risk management policy should be widely distributed throughout the company.		4.1.7	The risk management policy should be widely distributed throughout the company.																						
Plan	Leadership, Relationships	II. Establish the tone of the organisation.	II. Establish the tone of the organisation.	Establishing the tone of the organisation: The introduction of risk management and ensuring its ongoing effectiveness require strong and sustained commitment by management of the organisation, as well as strategic and rigorous planning to achieve commitment at all levels.	ISO 31000	4.2	Establishing the tone of the organisation: The introduction of risk management and ensuring its ongoing effectiveness require strong and sustained commitment by management of the organisation, as well as strategic and rigorous planning to achieve commitment at all levels.		King III	4.4.3		A senior level ERM program sponsor / Chief Risk Officer should have clear authority over and accountability for oversight of risk across the enterprise	CRO / Senior level project sponsor	CRO / Senior level project sponsor															
								(a) Ensure that the organisation's culture and risk management policy are aligned.		ISO 31000	4.2	(a) Ensure that the organisation's culture and risk management policy are aligned.	To create risk awareness at all levels of the organisations and to encourage risk based decision making.	Risk management policy	Risk management policy / Risk requirements evident in business, project and HR requirements and standards / Strategic intent document / Risk communication strategy / Internal audit reports / External audit report / Insurance claims					x	x		x		x			IV6: Add risk management plan components: current key risk profile + current level of risk maturity + surveys wrt effectiveness of the risk management process + training program + budget & resources requirements. IV7: Risk requirements evident in business, project and HR requirements and standards. IV9: ARC uses the following reports to assess the tone of the organisation, i.e. Internal audit reports: indication of control weaknesses; Insurance claims: indicate failed controls; Financial losses: gives a sense of key risks; HR reports on	
								(b) Determine risk management performance indicators that align with performance indicators of the organisation.					(b) Determine risk management performance indicators that align with performance indicators of the organisation.	To measure risk management performance against indicators, which are periodically reviewed for appropriateness;	Performance indicators (Key risk indicators)	Performance indicators (Key risk indicators)													

Addendum H: Phase 2 - Round 1: Changes to the conceptual ERM implementation model suggested by the senior risk experts during the semi-structured interviews

Changes	Additions	Not accepted
---------	-----------	--------------

Theoretical frameworks		Building blocks		Best practice requirements								Proposed deliverables			Changes / additions suggested by:												Changes and additions	
Deming cycle	Weisbord organisational design model			Level 1				Level 2							IV1 (AdC)	IV2 (BG)	IV4 (EL)	IV6 (GS)	IV7 (GC)	IV8 (HG)	IV9 (HV)	IV13 (MF)	IV17 (SM)	IV18 (VP)	IV19 (WM)			
				Conceptual	Source	Ref.	Adjusted	Conceptual	Source	Ref.	Adjusted																	
Plan	Leadership, Relationships	II. Establish the tone of the organisation.	II. Establish the tone of the organisation.	Establishing the tone of the organisation: The introduction of risk management and ensuring its ongoing effectiveness require strong and sustained commitment by management of the organisation, as well as strategic and rigorous planning to achieve commitment at all levels.	ISO 31000	4.2	Establishing the tone of the organisation: The introduction of risk management and ensuring its ongoing effectiveness require strong and sustained commitment by management of the organisation, as well as strategic and rigorous planning to achieve commitment at all levels.	(c) Align risk management objectives with the objectives and strategies of the organisation.	ISO 31000	4.2	(c) Align risk management objectives with the objectives and strategies of the organisation.	To encourage a risk mind-set for decision making.	Risk appetite & risk tolerance	Strategic plan / Business plan / Risk plan / Risk management objectives / Risk appetite statement / Risk tolerance levels			x					x		x	x	IV4, IV9, IV17 & IV18: Add strategic plan / business plan / risk plan / risk management objectives.		
								(d) Assign accountabilities and responsibilities at appropriate levels within the organisation.			(d) Assign accountabilities and responsibilities at appropriate levels within the organisation.	To reduce role confusion by establishing clear roles and responsibilities for risk activities across businesses and risk types.	Risk governance model: (incl. risk owners' matrix, roles & responsibilities, reporting & escalation process & incentives guidelines.)	Risk governance model: (Incl. risk owners' matrix, roles & responsibilities, reporting & escalation process & incentives guidelines & individual performance scorecard.)								x		IV17: Add individual performance scorecard.				
								(e) Ensure that the necessary resources are allocated to risk management.			(e) Ensure that the necessary resources are allocated to risk management.	To ensure the effective and efficient implementation of the ERM program.	Risk management plan (People, Processes and Budget)	Risk management plan (People, Processes and Budget) / Annual performance plan / Operational budget		x		x							IV2: Add annual performance plan to proposed deliverables. IV7: Add operational budget.			
								(f) Communicate the benefits of risk management to all stakeholders.			(f) Communicate the benefits of risk management to all stakeholders.	To raise risk awareness and create excitement for the project.	Benefits of risk management	Risk training material / Business case / Risk management policy / Embedded in risk reports / Board risk report					x			x	x	x	IV7, IV17 & IV18: Add risk report to the board, training material, risk management policy. IV13: Make the benefits real by speaking the business' language and use case studies.			
						The induction and ongoing training programs of the board should incorporate risk governance. (Note: apply to all the levels in the organisation)	King III	4.1.4	The induction and ongoing training programs of the board should incorporate risk governance. (Note: apply to all the levels in the organisation)			To create a common risk language, improve risk awareness and encourage risk based decision making.	Risk awareness gap analysis	Risk awareness gap analysis						x				x	IV8 & IV19: Add risk culture assessment.			
													Risk maturity model	Risk maturity assessment			x		x									
													Risk awareness plan	Risk awareness strategy & plan	x	x										IV1 & IV2: Add risk awareness strategy.		
Plan	Purpose, Relationships, Structure, External environment	III. Design the rules of the game.	III. Design the rules of the game.	Design the risk management framework.	ISO 31000	4.3	Design the risk management framework.	Task: Understanding the organisation and its context (Know your organisation)		ISO 31000	4.3.1 & 5.3.2	Task: Understanding the organisation and its context (Know your organisation)	To get an overall picture of the external environment based PESTLE and / or Porter's 5 forces.		Environmental scanning report	Environmental scanning report												
								Establish the external context:				Establish the external context:																
								(a) the social and cultural, political, legal, regulatory, financial, technological, economic, natural and competitive environment, whether international, national, regional or local.				(a) the social and cultural, political, legal, regulatory, financial, technological, economic, natural and competitive environment, whether international, national, regional or local.																
								(b) key drivers and trends having impact on the objectives of the organisation; and				(b) key drivers and trends having impact on the objectives of the organisation; and																
								(c) External stakeholder analysis				(c) External stakeholder analysis																
								Establish the internal context:				Establish the internal context:																
								(a) Governance, organisational structure, roles and accountabilities;				(a) Governance, organisational structure, roles and accountabilities;				Environmental scanning of the INTERNAL value chain	Environmental scanning of the INTERNAL value chain											
																SWOT analysis	SWOT analysis											
																Organisational organigram	Organisational organigram											
																Divisional organigram	Divisional organigram											
																Departmental organigram	Departmental organigram											
																Delegation of authority	Delegation of authority											
																Committee structure	Committee structure											
																Committee charters	Committee charters											
																List of policies	List of policies											
																Copy of policies	Copy of policies											
																Action plans (strategies)	Action plans (strategies)											
																Risk competency model	Risk competency model											
																Job profiles / specification	Job profiles / specification											
																Technical job specs	Technical job specs											
																List of systems	List of systems											
																Process maps	Process maps											
																Escalation policy	Escalation policy											
																Escalation process	Escalation process											
																Connected stakeholder analysis	Connected stakeholder analysis											
																Internal stakeholder analysis	Internal stakeholder analysis											
																Organisational culture survey results	Organisational culture survey results											
																List of standards, guidelines and models adopted by the organisation; and	List of standards, guidelines and models adopted by the organisation; and											
																(h) the form and extent of contractual relationships.	(h) the form and extent of contractual relationships.											

Addendum H: Phase 2 - Round 1: Changes to the conceptual ERM implementation model suggested by the senior risk experts during the semi-structured interviews

Changes	Additions	Not accepted
---------	-----------	--------------

Theoretical frameworks		Building blocks		Best practice requirements								Proposed deliverables			Changes / additions suggested by:												Changes and additions																						
Deming cycle	Weisbord organisational design model	Conceptual	Adjusted	Level 1			Level 2				IV1 (AdC)				IV2 (BG)	IV4 (EL)	IV6 (GS)	IV7 (GC)	IV8 (HG)	IV9 (HV)	IV13 (MF)	IV17 (SM)	IV18 (VP)	IV19 (WM)																									
				Conceptual	Source	Ref.	Adjusted	Conceptual	Source	Ref.		Adjusted	Purpose	Conceptual											Adjusted																								
Plan	Purpose, Relationships, Structure, External environment	III. Design the rules of the game.	III. Design the rules of the game.	Design the risk management framework.	ISO 31000				ISO 31000	4.3.1 & 5.3.3		To describe the internal value chain of the organisation and to identify areas that would create risks and opportunities		Internal audit reports								x			x		IV9 & IV18: Add internal audit reports.																						
																														IV9 & IV 18: Add external audit reports.																			
																																IV17: Add strategic plans.																	
																																IV17: Add business plans.																	
								Design the risk management framework.	ISO 31000	4.3.1 & 5.3.4		Establish the context of the risk management process (The context of the risk management process will vary according to the needs of an organisation. It can involve, but is not limited to:		Establish the context of the risk management process (The context of the risk management process will vary according to the needs of an organisation. It can involve, but is not limited to:	To create ONE set of risk management rules for the organisation.		Risk management file / manual that includes:	Risk management file / manual that includes:																															
				(a) Defining the goals and objectives of the risk management activities;		(a) Defining the goals and objectives of the risk management activities;	Risk management goals & -objectives					Risk management goals & -objectives																																					
				(b) Defining responsibilities for and within the risk management process;		(b) Defining responsibilities for and within the risk management process;							Risk governance model	Risk governance model																																			
				(c) Defining the scope, as well as the depth and breadth of the risk management activities to be carried out, including specific inclusions and exclusions;		(c) Defining the scope, as well as the depth and breadth of the risk management activities to be carried out, including specific inclusions and exclusions;													Top-down & Bottom-up risk management activities	Top-down & Bottom-up risk management activities																													
				(e) Defining the activity, process, function, project, product, service or asset in terms of time and location;		(e) Defining the activity, process, function, project, product, service or asset in terms of time and location;															Interconnectedness maps	Interconnectedness maps																											
				(f) Defining the relationships between a particular project, process or activity and other projects, processes or activities of the organisation;		(f) Defining the relationships between a particular project, process or activity and other projects, processes or activities of the organisation;																	Risk assessment methodologies	Risk assessment methodologies																									
				(g) Defining the risk assessment methodologies;		(g) Defining the risk assessment methodologies;																			Key risk indicators	Key risk indicators																							
				(h) Defining the way performance and effectiveness is evaluated in the management of risk;		(h) Defining the way performance and effectiveness is evaluated in the management of risk;																					Decision matrix	Decision matrix																					
				(i) Identifying and specifying the decisions that have to be made; and		(i) Identifying and specifying the decisions that have to be made; and																							Research to clarify context	Research to clarify context																			
				(j) Identifying, scoping or framing studies needed, their extent and objectives, and the resources required for such studies;		(j) Identifying, scoping or framing studies needed, their extent and objectives, and the resources required for such studies;																																											
				Define the risk criteria (When defining risk criteria, factors to be considered should include the following:		Define the risk criteria (When defining risk criteria, factors to be considered should include the following:		To create standardised risk assessment criteria for the organisation as a whole. To give risk owners and other risk stakeholders insight into risk management in their terms.	Risk management file / manual that includes:	Risk management file / manual that includes:																																							
				(a) The nature and types of causes and consequences that can occur and how they will be managed;		(a) The nature and types of causes and consequences that can occur and how they will be managed;	Examples of causes and consequences				Examples of causes and consequences																																						
				(b) How likelihood will be defined;		(b) How likelihood will be defined;						Risk assessment tools and techniques	Risk assessment tools and techniques																																				
				(c) The timeframe(s) of the likelihood and/or risk is to be determined;		(c) The timeframe(s) of the likelihood and/or risk is to be determined;								Risk management plan	Risk management plan																																		
				(d) How the level of risk is to be determined;		(d) How the level of risk is to be determined;										Risk appetite guidelines	Risk appetite guidelines																																
				(e) The views of stakeholders;		(e) The views of stakeholders;												Risk tolerance levels guidelines	Risk tolerance levels guidelines			x																					IV4: Change risk tolerance levels guidelines to risk appetite statement.						
				(f) The level at which risk becomes acceptable or tolerable; and		(f) The level at which risk becomes acceptable or tolerable; and																																											
				(g) Whether combinations of multiple risks should be taken into account and, if so, how and which combinations should be considered.		(g) Whether combinations of multiple risks should be taken into account and, if so, how and which combinations should be considered.																																											

Changes	Additions	Not accepted
---------	-----------	--------------

Development of an enterprise risk management implementation model and assessment tool

Addendum H: Phase 2 - Round 1: Changes to the conceptual ERM implementation model suggested by the senior risk experts during the semi-structured interviews

Changes	Additions	Not accepted
---------	-----------	--------------

Theoretical frameworks		Building blocks		Best practice requirements								Proposed deliverables			Changes / additions suggested by:												Changes and additions																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																						
Deming cycle	Weisbord organisational design model	Conceptual	Adjusted	Level 1			Level 2				IV1 (AdC)				IV2 (BG)	IV4 (EL)	IV6 (GS)	IV7 (GC)	IV8 (HG)	IV9 (HV)	IV13 (MF)	IV17 (SM)	IV18 (VP)	IV19 (WM)																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																									
				Conceptual	Source	Ref.	Adjusted	Conceptual	Source	Ref.		Adjusted	Purpose	Conceptual											Adjusted																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																								
Plan	Purpose, Relationships, Structure, External environment	III. Design the rules of the game.	III. Design the rules of the game.	Design the risk management framework.	ISO 31000	4.3	Design the risk management framework.	Task: Establishing internal communication and reporting mechanisms	ISO 31000	4.3.6	Task: Establishing internal communication and reporting mechanisms	To create one set of rules for risk communication and also to increase risk transparency.	Internal reporting guidelines	Internal reporting guidelines																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																			
								(a) Key components of the risk management framework, and any subsequent modifications, are communicated appropriately;			(a) Key components of the risk management framework, and any subsequent modifications, are communicated appropriately;		Communication guidelines	Communication guidelines																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																			

Addendum H: Phase 2 - Round 1: Changes to the conceptual ERM implementation model suggested by the senior risk experts during the semi-structured interviews

Changes	Additions	Not accepted
---------	-----------	--------------

Theoretical frameworks		Building blocks		Best practice requirements								Proposed deliverables			Changes / additions suggested by:												Changes and additions							
Deming cycle	Weisbord organisational design model	Conceptual	Adjusted	Level 1				Level 2				Purpose	Conceptual	Adjusted	IV1 (AdC)	IV2 (BG)	IV4 (EL)	IV6 (GS)	IV7 (GC)	IV8 (HG)	IV9 (HV)	IV13 (MF)	IV17 (SM)	IV18 (VP)	IV19 (WM)									
				Conceptual	Source	Ref.	Adjusted	Conceptual	Source	Ref.	Adjusted																							
Plan	Helping mechanisms, Relationships, Rewards	IV. Develop the risk infrastructure.	IV. Develop the risk infrastructure.	Committees: the board should delegate certain functions to well-structured committees but without abdication of its own responsibilities.	King III	2.23	Committees: the board should delegate certain functions to well-structured committees but without abdication of its own responsibilities.	The risk committee should:	King III	4.3.2	The risk committee should:	To formalise decision making structures, escalation protocol & identify risk stakeholders.	Risk committees:	Risk committees:																				
								consider the risk management policy and plan and monitor the risk management process;			consider the risk management policy and plan and monitor the risk management process;		Board risk committee charter	Board risk committee terms of reference					x															
								have as its members executive and non-executive directors, members of senior management and independent risk management experts to be invited, if necessary;			have as its members executive and non-executive directors, members of senior management and independent risk management experts to be invited, if necessary;		Executive risk committee charter	Executive risk committee terms of reference					x								IV7 clarified that charter is used for legal and regulatory ordained committees and terms of reference for other types of committees required by best practice or the business.							
								have a minimum of three members; and			have a minimum of three members; and		Departmental risk committee charter	Departmental risk committee terms of reference				x																
								convene at least twice per year.			convene at least twice per year.			Audit and risk committee charter	x						x					IV1 & IV9: Could also be a audit and risk committee or a board risk and audit committee.								
								The audit committee should:	King III	3.4	The audit committee should:		Audit committee charter	Audit committee charter																				
								oversee integrated reporting.			oversee integrated reporting.																							
								have regard to all factors and risks that may impact on the integrity of the integrated report.			have regard to all factors and risks that may impact on the integrity of the integrated report.																							
								review and comment on the financial statements included in the integrated report.			review and comment on the financial statements included in the integrated report.																							
								review the disclosure of sustainability issues in the integrated report to ensure that it is reliable and does not conflict with the financial information.			review the disclosure of sustainability issues in the integrated report to ensure that it is reliable and does not conflict with the financial information.																							
								recommend to the board to engage an external assurance provider on material sustainability issues.			recommend to the board to engage an external assurance provider on material sustainability issues.																							
								consider the need to issue interim results.			consider the need to issue interim results.																							
								review the content of the summarised information.			review the content of the summarised information.																							
								engage the external auditors to provide assurance on the summarised financial information.			engage the external auditors to provide assurance on the summarised financial information.																							
								ensure that a combined assurance model is applied to provide a coordinated approach to all assurance activities.			ensure that a combined assurance model is applied to provide a coordinated approach to all assurance activities.																							
								ensure that the combined assurance is received is appropriate to address all the significant risks facing the company.			ensure that the combined assurance is received is appropriate to address all the significant risks facing the company.																							
								monitor the relationship between the external assurance providers and the company.			monitor the relationship between the external assurance providers and the company.																							
								The audit committee should be an integral component of the risk management process.		3.8	The audit committee should be an integral component of the risk management process.																							
								The charter of the audit committee should set out its responsibilities regarding risk management.			The charter of the audit committee should set out its responsibilities regarding risk management.																							
								The audit committee should specifically have oversight of:		3.8.2	The audit committee should specifically have oversight of:																							
								financial reporting			financial reporting																							
								internal financial controls;		3.8.2.2	internal financial controls;																							
								fraud risks as it relates to financial reporting; and			fraud risks as it relates to financial reporting; and																							
								IT risks as it relates to financial reporting.	3.8.2.4	IT risks as it relates to financial reporting.																								

Changes	Additions	Not accepted
---------	-----------	--------------

Development of an enterprise risk management implementation model and assessment tool 299

Addendum H: Phase 2 - Round 1: Changes to the conceptual ERM implementation model suggested by the senior risk experts during the semi-structured interviews

Changes	Additions	Not accepted
---------	-----------	--------------

Theoretical frameworks		Building blocks		Best practice requirements								Proposed deliverables			Changes / additions suggested by:												Changes and additions						
Deming cycle	Weisbord organisational design model	Conceptual	Adjusted	Level 1				Level 2							IV1 (AdC)	IV2 (BG)	IV4 (EL)	IV6 (GS)	IV7 (GC)	IV8 (HG)	IV9 (HV)	IV13 (MF)	IV17 (SM)	IV18 (VP)	IV19 (WM)								
				Conceptual	Source	Ref.	Adjusted	Conceptual	Source	Ref.	Adjusted	Purpose	Conceptual	Adjusted																			
Do	Leadership, Structure, Relationships, Helping Mechanisms, External environment	V. Implementation.	V. Implement the ERM program.	Implementing the framework for managing risk.	ISO 31000	4.4.1	Implementing the framework for managing risk.	Apply the risk management policy and process to the organisational processes;	ISO 31000	4.4.1	Apply the risk management policy and process to the organisational processes;	To embed risk management in all the organisation's practices and processes in a way that it is relevant, effective and efficient.	Integration of the risk into organisational processes	Performance management process											x		IV18 suggested that the detail processes should be added to the implementation model.						
								Comply with legal and regulatory requirements;			Comply with legal and regulatory requirements;	To communicate risk related compliance requirements.	Legal, regulatory & best practice compliance register (pertaining to risk)	Legal, regulatory & best practice compliance register (pertaining to risk)																			
								Ensure that decision making, including the development and setting of objectives, is aligned with the outcomes of risk management processes;			Ensure that decision making, including the development and setting of objectives, is aligned with the outcomes of risk management processes;	To encourage a risk mind-set for decision making.	Risk appetite statements	Risk appetite statements																			
								Hold information and training sessions; and			Hold information and training sessions; and	To create a common risk language, improve risk awareness and encourage risk based decision making.	Risk tolerance levels	Risk tolerance levels											x			IV18: Add strategic plan.					
													ERM framework & policy										x		IV19: Add ERM policy and process.								
								Hold information and training sessions; and	Hold information and training sessions; and	To create a common risk language, improve risk awareness and encourage risk based decision making.	Risk awareness gap analysis	Risk awareness gap analysis																					
											Risk maturity model	Risk maturity assessment																					
								Communicate and consult with stakeholders to ensure that its risk management framework remains appropriate.	ISO 31000	4.2 & 4.4.1		To ensure that the risk management framework remains appropriate.	Risk awareness plan	Risk awareness strategy & - plan																			
												To ensure that the risk management framework remains appropriate.	Risk facilitation sessions	Risk facilitation sessions																			
				Implementing the risk management process	ISO 31000	4.4.2	Implementing the risk management process.	Step 1: Communication and consultation with external and internal stakeholders should take place during all stages of the risk management process.	ISO 31000	5.2	Step 1: Communication and consultation with external and internal stakeholders should take place during all stages of the risk management process.	To identify the internal and external stakeholders for the organisation / division / department / project.	Stakeholder analysis	Stakeholder analysis																			
													To identify the most appropriate communication tools and establish timelines.	Risk communication plan	Risk communication plan																		
														To ensure that the right information reaches the right people at the right time.	Risk reports e.g. stress tests, risk & control self-assessments, incident reports, risk treatment plans, key risk indicator reports.	Risk reports e.g. stress tests, risk & control self-assessments, incident reports, risk treatment plans, key risk indicator reports.																	
								Step 2: Establish the context (Know your organisation / division / department / project / risk type)	ISO 31000	5.3	Step 2: Establish the context (Know your organisation / division / department / project / risk type)																						
								Establish the external context	ISO 31000	5.3.2 & 4.3.1	Establish the external context	To describe the UNIQUE context for the risk management project.	External environment mind map	External environment mind map																			
								Establish the internal context			Establish the internal context		External stakeholder register	External stakeholder register																			
													External stakeholder map	External stakeholder map																			
								Establishing the context of the risk management process			Establishing the context of the risk management process		Internal value chain mind map	Internal value chain mind map																			
								Apply the risk criteria	ISO 31000	5.3.4 & 4.3.1	Establishing the context of the risk management process		Internal stakeholder register	Internal stakeholder register																			
								Internal stakeholder map			Internal stakeholder map																						
								Step 3: Risk identification	ISO 31000	5.4.2	Step 3: Risk identification	Process of finding, recognising and describing risks.	Standardised risk management context (refer to building block III)	Standardised risk management context (refer to building block III)																			
													Key / Principle / Strategic risk register	Key / Principle / Strategic risk register																			
								Step 3: Risk identification	King III	4.5	Step 3: Risk identification		Divisional / departmental / business unit risk register	Divisional / departmental / business unit risk register																			
													Emerging risk register	Emerging risk register																			
								Step 3: Risk identification			Step 3: Risk identification		Risk library																x			IV19: Add risk library.	
								Step 4: Risk analysis	ISO 31000	5.4.3	Step 4: Risk analysis	Process to comprehend the nature of risk and to determine the level of risk (e.g. high, medium, low).																					
													Key / Principle / Strategic risk register - risk ratings applied	Key / Principle / Strategic risk register - risk ratings applied																			
								Step 4: Risk analysis	King III	4.5	Step 4: Risk analysis		Divisional / departmental / business unit risk register - risk ratings applied	Divisional / departmental / business unit risk register - risk ratings applied																			
													Root cause analysis																				
								Step 5: Risk evaluation	ISO 31000	5.4.4	Step 5: Risk evaluation	Process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable.	Key / Principle / Strategic risk profile - risk ratings + current controls applied & risk owners identified	Key / Principle / Strategic risk profile - risk ratings + current controls applied & risk owners identified																			
													Divisional / departmental / business unit risk register risk ratings + current controls applied & risk owners identified	Divisional / departmental / business unit risk register risk ratings + current controls applied & risk owners identified																			
				Step 6: Risk treatment	ISO 31000	5.5	Step 6: Risk response	To identify the most appropriate risk treatment for the most significant risks.	King III	4.7	Step 6: Risk response		List of risk controls	Controls library	x										x		x		IV1 & IV19: Change list of risk controls to controls library. IV17: replace list of risk controls with key controls framework.				
													Risk treatment plans	Risk response plans / Action plans			x		x											IV2 & IV6: Add action plans			
													Risk treatment options	Risk response options					x												IV7: Change risk treatment to risk response to comply with King III.		

Addendum H: Phase 2 - Round 1: Changes to the conceptual ERM implementation model suggested by the senior risk experts during the semi-structured interviews

Changes	Additions	Not accepted
---------	-----------	--------------

Theoretical frameworks		Building blocks		Best practice requirements								Proposed deliverables			Changes / additions suggested by:												Changes and additions								
Deming cycle	Weisbord organisational design model	Conceptual	Adjusted	Level 1				Level 2							Purpose	Conceptual	Adjusted	IV1	IV2	IV4	IV6	IV7	IV8	IV9	IV13	IV17			IV18	IV19					
				Conceptual	Source	Ref.	Adjusted	Conceptual	Source	Ref.	Adjusted	(AdC)	(BG)	(EL)				(GS)	(GC)	(HG)	(HV)	(MF)	(SM)	(VP)	(WM)										
Check	Rewards	VI. Monitor & review.	VI. Monitor and review the ERM program.	Monitoring activities by the Board			Monitoring activities by the Board	The board should ensure continual risk monitoring by management	King III	4.8	The board should ensure continual risk monitoring by management	To ensure proper risk oversight.	Risk governance framework	Risk governance framework																					
								The board should ensure that effective and continual monitoring of risk management takes place.		4.8.1	The board should ensure that effective and continual monitoring of risk management takes place.	To reduce role confusion and provide clear guidelines for risk monitoring.	Risk management plan (monitoring roles and responsibilities)	Risk management plan (monitoring roles and responsibilities)																					
								The responsibility for monitoring should be defined in the risk management plan.		4.8.2	The responsibility for monitoring should be defined in the risk management plan.	To periodically measure progress against, and deviation from, the risk management plan.	Status on risk management plan implementation	Status report on risk management plan implementation											x		IV17: Change status to status report.								
				Review activities by the Board	King III	4.1 & 4.3	Review activities by the Board	The board should comment in the integrated report on the effectiveness of the system and process of risk	King III	4.1.2	The board should comment in the integrated report on the effectiveness of the system and process of risk	To periodically review whether the risk management framework, policy and plan are still	Integrated report (risk and opportunities section)	Integrated report (risk and opportunities section)																					
								The board should ensure that effective and continual monitoring of risk management takes place.		King III	4.1.8	The board should ensure that effective and continual monitoring of risk management takes place.	To periodically measure progress against, and deviation from, the risk management plan.	Risk management plan implementation status report	Risk management plan implementation status report																				
								The board should review the implementation of the	King III	4.1.9	The board should review the implementation of the	To periodically review whether the risk	Risk improvement report	Risk improvement report																					
								The performance of the committee should be evaluated once a year by the board.	King III	4.3.3	The performance of the committee should be evaluated once a year by the board.	To ensure effectiveness and efficiency with regards to committee activities.	Board risk committee performance evaluation	Board risk committee performance evaluation																					
				Monitor the risk management framework			Monitor the risk management framework	The board should monitor that risks taken are within the tolerance and appetite levels.	King III	4.2.3	The board should monitor that risks taken are within the tolerance and appetite levels.	To ensure compliance with the risk appetite framework.	Risk appetite status report	Risk appetite status report																					
								Measure risk management performance against indicators, which are periodically reviewed for appropriateness;		ISO 31000	4.5	Measure risk management performance against indicators, which are periodically reviewed for appropriateness;	To measure risk management performance against indicators, which are periodically reviewed for appropriateness;	KRI performance report	KRI performance report																				
								Periodically measure progress against, and deviation from, the risk management plan;	To periodically measure progress against, and deviation from, the risk management plan.			Risk management plan implementation status report	Risk management plan implementation status report																						
								Report on risk, progress with the risk management plan and how well the risk management policy is being	To report on risk, progress with the risk management plan and how well the risk management policy is being			Risk management policy compliance report	Risk management policy compliance report																						
								Monitor the level of risk awareness	Researcher		Monitor the level of risk awareness	To track the improvement of risk awareness.	Risk culture surveys	Risk culture surveys																					
				Review the risk management framework			Review the risk management framework	Periodically review whether the risk management framework, policy and plan	ISO 31000	4.5	Periodically review whether the risk management framework, policy and plan	To periodically review whether the risk management framework, policy and plan are still appropriate, given the organisations' external and internal context.	Risk improvement report	Internal audit report	Risk improvement report																				
								Risk calendar																											
								Communicate and consult with stakeholders to ensure that its risk management framework remains appropriate.	ISO 31000	4.2 & 4.4.1	Communicate and consult with stakeholders to ensure that its risk management framework remains appropriate.			Subject matter expert gap analysis																					
								Internal audit reports																											
				Monitor the risk management process	ISO 31000	5.6	Monitor the risk management process	Ensuring that controls are effective and efficient in both design and operation.	ISO 31000	5.6	Ensuring that controls are effective and efficient in both design and operation.	To ensure that controls are effective and efficient in both design and operation.	Risk treatment plans	Subject matter expert gap analysis																					
								Combined assurance reports																											
								Risk profile status reports			x																								
								Internal audit reports																											
								Identifying emerging risks.	ISO 31000	5.6	Identifying emerging risks.	To identify emerging risks in the organisation's internal value chain and external environment.	Emerging risk register	Emerging risk register																					
				Review the risk management process	ISO 31000	5.6	Review the risk management process	Analysing and learning lessons from events (including near-misses), changes, trends, successes and failures;	ISO 31000	5.6	Analysing and learning lessons from events (including near-misses), changes, trends, successes and failures;	To analyse and learn lessons from events (including near-misses), changes, trends, successes and failures.	Variance and trend analysis	Variance and trend analysis																					
								Post mortem sessions			x																								
								Environmental scanning																											
Risk reconciliation reports																																			
Post loss analysis																																			

Addendum H: Phase 2 - Round 1: Changes to the conceptual ERM implementation model suggested by the senior risk experts during the semi-structured interviews

Changes	Additions	Not accepted
---------	-----------	--------------

Theoretical frameworks		Building blocks		Best practice requirements								Proposed deliverables			Changes / additions suggested by:												Changes and additions					
Deming cycle	Weisbord organisational design model	Conceptual	Adjusted	Level 1				Level 2							IV1 (AdC)	IV2 (BG)	IV4 (EL)	IV6 (GS)	IV7 (GC)	IV8 (HG)	IV9 (HV)	IV13 (MF)	IV17 (SM)	IV18 (VP)	IV19 (WM)							
				Conceptual	Source	Ref.	Adjusted	Conceptual	Source	Ref.	Adjusted	Purpose	Conceptual	Adjusted																		
Adjust	Leadership, Purposes, Structure, Relationships, Rewards, Helpful mechanisms, External environment	VII. Continual improvement.	VII. Continual improvement of the ERM program.	Management should provide assurance to the board that the risk management plan is integrated in the daily activities of the company.	King III	4.9	Management should provide assurance to the board that the risk management plan is integrated in the daily activities of the company.		King III	4.9.1		To inform the relevant committees and risk stakeholders of the level of assurance provided by assurance providers.	Integrated assurance report.	Combined assurance report.					x								IV7 advised that King IV will refer to combined assurance.					
																														IV7, IV17, IV18 & IV19: Add risk reports to various committees.		
																															IV4 & IV6: Add risk maturity assessment.	
																															IV6: Add benchmarking assessments.	
				Internal audit should:																												
				provide a written assessment of the effectiveness of the system of internal controls and risk management to the board.			King III	4.9	provide a written assessment of the effectiveness of the system of internal controls and risk management to the board.		King III	4.9.2		To periodically review whether the risk management framework, policy and plan are still appropriate, given the organisations' external and internal context;																		
			detect changes in the external and internal context, including changes to risk criteria and the risk itself which can require revision of risk treatments and priorities; and		ISO 31000	5.6	Detecting changes in the external and internal context, including changes to risk criteria and the risk itself which can require revision of risk treatments and priorities; and																									
			obtaining further information to improve risk assessment.				5.6	Obtaining further information to improve risk assessment.																								

Source: Researcher's own compilation

Phase 2 - Round 1: Changes to the conceptual ERM implementation model suggested by the senior risk experts structured interviews

Changes	Additions
---------	-----------

Building blocks		Best practice requirements								Proposed deliverables		Agreed with by (semi-structured interviews):												Comments
Conceptual	Adjusted	Level 1			Level 2				Purpose			Conceptual	IV1 (AdC)	IV2 (BC)	IV4 (EL)	IV6 (GS)	IV7 (GC)	IV8 (HG)	IV9 (HV)	IV13 (MF)	IV17 (SM)	IV18 (VP)	IV19 (WM)	
		Conceptual	Source	Ref.	Adjusted	Conceptual	Source	Ref.		Adjusted														
I. Get permission.	I. Formalise the instruction and get permission.	Ensure legal and regulatory compliance.	ISO 31000	4.2	Instruction / Trigger				Business trigger e.g. event, merger & acquisition due diligence requirement, peer pressure, etc.	To motivate the need for an ERM program.														
									Ensure legal and regulatory compliance.	To motivate the need for an ERM program.	Compliance requirements (legal + regulatory + best practise frameworks)													
		The board should delegate to management the responsibility to design, implement and monitor the risk management plan.	King III	4.4	Permission / Mandate				The board should delegate to management the responsibility to design, implement and monitor the risk management plan.	To ask for permission / mandate to design and implement the ERM program.	Agenda item for Board meeting													
										To record the permission / mandate received to design and implement an ERM program.	Minutes of the Board meeting													
		The risk committee or audit committee should assist the board in carrying out its risk responsibilities	King III	4.3	Oversight: the risk committee or audit committee should assist the board in carrying out its risk responsibilities		King III	4.3.1	The board should appoint a committee responsible for risk.	To assist the board in carrying out its risk roles and responsibilities.	Board risk committee (BRC) charter													
									The risk committee should: consider the risk management policy and plan and monitor the risk management process;															
									have as its members executive and non-executive directors, members of senior management and independent risk management experts to be invited, if necessary;															
									have a minimum of three members; and															
									convene at least twice per year.															
									The board's responsibility for risk governance should be expressed in the board charter.															
		Define and endorse the risk management policy	King III	4.1.1	Define and endorse the risk management policy		King III	4.1.5	The board's responsibility for risk governance should manifest in a documented risk management policy and plan.	To document risk management scope, objectives and roles and responsibilities.	Risk management policy	x	x	x	x	x	x	x	x	x	x	x	x	
								4.1.6	The board should approve the risk management policy and plan.															
			ISO 31000	4.2 & 4.3.2				4.1.7	The risk management policy should be widely distributed throughout the company.															
II. Establish the tone of the organisation.	II. Establish the tone of the organisation.	Establishing the tone of the organisation: The introduction of risk management and ensuring its ongoing effectiveness require strong and sustained commitment by management of the organisation, as well as strategic and rigorous planning to achieve commitment at all levels.	ISO 31000	4.2	Establishing the tone of the organisation: The introduction of risk management and ensuring its ongoing effectiveness require strong and sustained commitment by management of the organisation, as well as strategic and rigorous planning to achieve commitment at all levels.		King III	4.4.3		A senior level ERM program sponsor / Chief Risk Officer should have clear authority over and accountability for oversight of risk across the enterprise	CRO / Senior level project sponsor	x	x	x	x	x	x	x	x	x	x			
							ISO 31000	4.2	(a) Ensure that the organisation's culture and risk management policy are aligned.	To create risk awareness at all levels of the organisations and to encourage risk based decision making.	Risk management policy													
									(b) Determine risk management performance indicators that align with performance indicators of the organisation.	To measure risk management performance against indicators, which are periodically reviewed for appropriateness;	Performance indicators (Key risk indicators)	x	x	x	x	x	x	x	x	x	x			

Phase 2 - Round 1: Changes to the conceptual ERM implementation model suggested by the senior risk experts structured interviews

Changes	Additions
---------	-----------

Building blocks		Best practice requirements								Proposed deliverables		Agreed with by (semi-structured interviews):														Comments	
Conceptual	Adjusted	Level 1			Level 2				Purpose			Conceptual	IV1 (AdC)	IV2 (BC)	IV4 (EL)	IV6 (GS)	IV7 (GC)	IV8 (HG)	IV9 (HV)	IV13 (MF)	IV17 (SM)	IV18 (VP)	IV19 (WM)				
		Conceptual	Source	Ref.	Adjusted	Conceptual	Source	Ref.		Adjusted																	
II. Establish the tone of the organisation.	II. Establish the tone of the organisation.	Establishing the tone of the organisation: The introduction of risk management and ensuring its ongoing effectiveness require strong and sustained commitment by management of the organisation, as well as strategic and rigorous planning to achieve commitment at all levels.	ISO 31000	4.2	Establishing the tone of the organisation: The introduction of risk management and ensuring its ongoing effectiveness require strong and sustained commitment by management of the organisation, as well as strategic and rigorous planning to achieve commitment at all levels.	(c) Align risk management objectives with the objectives and strategies of the organisation.	ISO 31000	4.2	(c) Align risk management objectives with the objectives and strategies of the organisation.	To encourage a risk mind-set for decision making.	Risk appetite & risk tolerance																
						(d) Assign accountabilities and responsibilities at appropriate levels within the organisation.			(d) Assign accountabilities and responsibilities at appropriate levels within the organisation.	To reduce role confusion by establishing clear roles and responsibilities for risk activities across businesses and risk types.	Risk governance model: (incl. risk owners' matrix, roles & responsibilities, reporting & escalation process & incentives guidelines.)																
						(e) Ensure that the necessary resources are allocated to risk management.			(e) Ensure that the necessary resources are allocated to risk management.	To ensure the effective and efficient implementation of the ERM program.	Risk management plan (People, Processes and Budget)																
						(f) Communicate the benefits of risk management to all stakeholders.			(f) Communicate the benefits of risk management to all stakeholders.	To raise risk awareness and create excitement for the project.	Benefits of risk management																
		The induction and ongoing training programs of the board should incorporate risk governance. (Note: apply to all the levels in the organisation)	King III	4.1.4	The induction and ongoing training programs of the board should incorporate risk governance. (Note: apply to all the levels in the organisation)			To create a common risk language, improve risk awareness and encourage risk based decision making.	Risk awareness gap analysis	x	x	x	x	x	x	x	x	x	x	x							
									Risk maturity model																		
											Risk awareness plan																
III. Design the rules of the game.	III. Design the rules of the game.	Design the risk management framework.	ISO 31000	4.3	Design the risk management framework.	Task: Understanding the organisation and its context (Know your organisation)			Task: Understanding the organisation and its context (Know your organisation)																		
						Establish the external context:	ISO 31000	4.3.1 & 5.3.2	Establish the external context:	To get an overall picture of the external environment based PESTLE and / or Porter's 5 forces.																	
						(a) the social and cultural, political, legal, regulatory, financial, technological, economic, natural and competitive environment, whether international, national, regional or local;			(a) the social and cultural, political, legal, regulatory, financial, technological, economic, natural and competitive environment, whether international, national, regional or local;		Environmental scanning report	x	x	x	x	x	x	x	x	x	x						
						(b) key drivers and trends having impact on the objectives of the organisation; and			(b) key drivers and trends having impact on the objectives of the organisation; and		Key business drivers report	x	x	x	x	x	x	x	x	x	x						
						(c) External stakeholder analysis			(c) External stakeholder analysis		Stakeholder analysis	x	x	x	x	x	x	x	x	x	x						
						Establish the internal context:	ISO 31000	4.3.1 & 5.3.3	Establish the internal context:	To describe the internal value chain of the organisation and to identify areas that would create risks and opportunities																	
						(a) Governance, organisational structure, roles and accountabilities;			(a) Governance, organisational structure, roles and accountabilities;		Environmental scanning of the INTERNAL value chain	x	x	x	x	x	x	x	x	x	x	x	x				
											SWOT analysis	x	x	x	x	x	x	x	x	x	x	x	x				
											Organisational organigram	x	x	x	x	x	x	x	x	x	x	x	x				
											Divisional organigram	x	x	x	x	x	x	x	x	x	x	x	x				
											Departmental organigram	x	x	x	x	x	x	x	x	x	x	x	x				
											Delegation of authority	x	x	x	x	x	x	x	x	x	x	x	x				
											Committee structure	x	x	x	x	x	x	x	x	x	x	x	x				
											Committee charters	x	x	x	x	x	x	x	x	x	x	x	x				
											List of policies	x	x	x	x	x	x	x	x	x	x	x	x				
											Copy of policies	x	x	x	x	x	x	x	x	x	x	x	x				
											Action plans (strategies)	x	x	x	x	x	x	x	x	x	x	x	x				
											Risk competency model	x	x	x	x	x	x	x	x	x	x	x	x				
						Job profiles / specification			x		x	x	x	x	x	x	x	x	x	x	x						
						Technical job specs			x		x	x	x	x	x	x	x	x	x	x	x						
						List of systems			x		x	x	x	x	x	x	x	x	x	x	x						
						Process maps			x		x	x	x	x	x	x	x	x	x	x	x						
						Escalation policy			x		x	x	x	x	x	x	x	x	x	x	x						
						Escalation process			x		x	x	x	x	x	x	x	x	x	x	x						
						Connected stakeholder analysis			x		x	x	x	x	x	x	x	x	x	x	x						
						Internal stakeholder analysis	x	x	x	x	x	x	x	x	x	x	x	x									
						Organisational culture survey results	x	x	x	x	x	x	x	x	x	x	x	x									
						List of standards, guidelines and models	x	x	x	x	x	x	x	x	x	x	x	x									
						Contracts register	x	x	x	x	x	x	x	x	x	x	x	x									

Phase 2 - Round 1: Changes to the conceptual ERM implementation model suggested by the senior risk experts structured interviews

Changes	Additions
---------	-----------

Building blocks		Best practice requirements								Proposed deliverables		Agreed with by (semi-structured interviews):														Comments			
Conceptual	Adjusted	Level 1			Level 2				Purpose			Conceptual	IV1 (AdC)	IV2 (BC)	IV4 (EL)	IV6 (GS)	IV7 (GC)	IV8 (HG)	IV9 (HV)	IV13 (MF)	IV17 (SM)	IV18 (VP)	IV19 (VM)						
		Conceptual	Source	Ref.	Adjusted	Conceptual	Source	Ref.		Adjusted																			
III. Design the rules of the game.	III. Design the rules of the game.	Design the risk management framework.	ISO 31000	4.3	Design the risk management framework.		ISO 31000	4.3.1 & 5.3.3		To describe the internal value chain of the organisation and to identify areas that would create risks and opportunities																			
						Establish the context of the risk management process (The context of the risk management process will vary according to the needs of an organisation. It can involve, but is not limited to:				Establish the context of the risk management process (The context of the risk management process will vary according to the needs of an organisation. It can involve, but is not limited to:				To create ONE set of risk management rules for the organisation.	Risk management file / manual that includes:														
						(a) Defining the goals and objectives of the risk management activities;				(a) Defining the goals and objectives of the risk management activities;					Risk management goals & -objectives	x	x	x	x	x	x	x	x	x	x	x	x		
						(b) Defining responsibilities for and within the risk management process;				(b) Defining responsibilities for and within the risk management process;					Risk governance model	x	x	x	x	x	x	x	x	x	x	x	x		
						(c) Defining the scope, as well as the depth and breadth of the risk management activities to be carried out, including specific inclusions and exclusions;				(c) Defining the scope, as well as the depth and breadth of the risk management activities to be carried out, including specific inclusions and exclusions;					Top-down & Bottom-up risk management activities	x	x	x	x	x	x	x	x	x	x	x			
						(e) Defining the activity, process, function, project, product, service or asset in terms of time and location;				(e) Defining the activity, process, function, project, product, service or asset in terms of time and location;					Interconnectedness maps	x	x	x	x	x	x	x	x	x	x	x			
						(f) Defining the relationships between a particular project, process or activity and other projects, processes or activities of the organisation;				(f) Defining the relationships between a particular project, process or activity and other projects, processes or activities of the organisation;					Risk assessment methodologies	x	x	x	x	x	x	x	x	x	x	x			
						(g) Defining the risk assessment methodologies;				(g) Defining the risk assessment methodologies;					Key risk indicators	x	x	x	x	x	x	x	x	x	x	x			
						(h) Defining the way performance and effectiveness is evaluated in the management of risk;				(h) Defining the way performance and effectiveness is evaluated in the management of risk;					Decision matrix	x	x	x	x	x	x	x	x	x	x	x			
						(i) Identifying and specifying the decisions that have to be made; and				(i) Identifying and specifying the decisions that have to be made; and					Research to clarify context	x	x	x	x	x	x	x	x	x	x	x			
						(j) Identifying, scoping or framing studies needed, their extent and objectives, and the resources required for such studies;				(j) Identifying, scoping or framing studies needed, their extent and objectives, and the resources required for such studies;																			
						Define the risk criteria (When defining risk criteria, factors to be considered should include the following:				Define the risk criteria (When defining risk criteria, factors to be considered should include the following:				To create standardised risk assessment criteria for the organisation as a whole. To give risk owners and other risk stakeholders insight into risk management in their terms.	Risk management file / manual that includes:														
						(a) The nature and types of causes and consequences that can occur and how they will be measured;				(a) The nature and types of causes and consequences that can occur and how they will be measured;					Examples of causes and consequences	x	x	x	x	x	x	x	x	x	x	x			
						(b) How likelihood will be defined;				(b) How likelihood will be defined;					Risk assessment tools and techniques	x	x	x	x	x	x	x	x	x	x	x			
						(c) The timeframe(s) of the likelihood and/or				(c) The timeframe(s) of the likelihood and/or					Risk management plan	x	x	x	x	x	x	x	x	x	x	x			
						(d) How the level of risk is to be determined;				(d) How the level of risk is to be determined;					Risk appetite guidelines	x	x	x	x	x	x	x	x	x	x	x			
						(e) The views of stakeholders;				(e) The views of stakeholders;					Risk tolerance levels guidelines	x	x		x	x	x	x	x	x	x	x			
						(f) The level at which risk becomes acceptable or tolerable; and				(f) The level at which risk becomes acceptable or tolerable; and																			
						(g) Whether combinations of multiple risks should be taken into account and, if so, how and which combinations should be considered.				(g) Whether combinations of multiple risks should be taken into account and, if so, how and which combinations should be considered.																			

Phase 2 - Round 1: Changes to the conceptual ERM implementation model suggested by the senior risk experts structured interviews

Changes	Additions
---------	-----------

[illegible]

Phase 2 - Round 1: Changes to the conceptual ERM implementation model suggested by the senior risk experts structured interviews

Changes	Additions
---------	-----------

Building blocks		Best practice requirements								Proposed deliverables		Agreed with by (semi-structured interviews):												Comments	
Conceptual	Adjusted	Level 1			Level 2				Purpose			Conceptual	IV1 (AdC)	IV2 (BG)	IV4 (EL)	IV6 (GS)	IV7 (GC)	IV8 (HG)	IV9 (HV)	IV13 (MF)	IV17 (SM)	IV18 (VP)	IV19 (WM)		
		Conceptual	Source	Ref.	Adjusted	Conceptual	Source	Ref.		Adjusted															
III. Design the rules of the game.	III. Design the rules of the game.	Design the risk management framework.	ISO 31000	4.3	Design the risk management framework.	Task: Establishing internal communication and reporting mechanisms	ISO 31000	4.3.6	Task: Establishing internal communication and reporting mechanisms	To create one set of rules for risk communication and also to increase risk transparency.	Internal reporting guidelines	x	x	x	x	x	x	x	x	x	x	x			
						(a) Key components of the risk management framework, and any subsequent modifications, are communicated appropriately;			(a) Key components of the risk management framework, and any subsequent modifications, are communicated appropriately;		Communication guidelines	x	x	x	x	x	x	x	x	x					
						(b) there is adequate internal reporting on the framework, its effectiveness and the outcomes;			(b) there is adequate internal reporting on the framework, its effectiveness and the outcomes;																
						(c) relevant information derived from the application of risk management is available at appropriate levels and times; and			(c) relevant information derived from the application of risk management is available at appropriate levels and times; and																
						(d) there are processes for consultation with internal stakeholders.			(d) there are processes for consultation with internal stakeholders.																
						Task: Establishing external communication and reporting mechanisms			Task: Establishing external communication and reporting mechanisms		Integrated report: risks and opportunities section														
		(a) Engaging appropriate external stakeholders and ensuring an effective exchange of information;	(a) Engaging appropriate external stakeholders and ensuring an effective exchange of information;	External reporting guidelines	x	x	x	x	x	x	x	x	x	x	x										
		(b) External reporting to comply with legal, regulatory, and governance requirements;	(b) External reporting to comply with legal, regulatory, and governance requirements;	Communication guidelines	x	x	x	x	x	x	x	x	x	x	x										
		(c) Providing feedback and reporting on communication and consultation;	(c) Providing feedback and reporting on communication and consultation;																						
		Design the risk management process.	ISO 31000	5	Design the risk management process.	Step 1: Communication and consultation	ISO 31000	5.2	Step 1: Communication and consultation	To develop a standardised risk management process for the organisation.	Risk management process guidelines	x	x	x	x	x	x	x	x	x	x	x	x		
						Step 2: Establish the context			4.3.1 & 5.3																Step 2: Establish the context
						Step 3: Risk identification			5.4.2																Step 3: Risk identification
Step 4: Risk analysis	5.4.3					Step 4: Risk analysis																			
Step 5: Risk evaluation	5.4.4					Step 5: Risk evaluation																			
Step 6: Risk treatment	5.5					Step 6: Risk treatment																			
Step 7: Monitor and review	5.6	Step 7: Monitor and review																							
Step 8: Continuous improvement	4.6	Step 8: Continuous improvement																							
IV. Develop the risk infrastructure.	IV. Develop the risk infrastructure.	Task: Allocate appropriate resources for risk management			Task: Allocate appropriate resources for risk management																				
		People (skills, experience, competence & training programs).	ISO 31000	4.3.5	People (skills, experience, competence & training programs).	People: skills, experience, competence & training programs	ISO 31000	4.3.5	People: skills, experience, competence & training programs	To establish decision making structures, escalation protocol & identify risk stakeholders.	Risk governance models	x	x	x	x	x	x	x	x	x	x	x			
										To identify competencies, skills levels and experience required by risk stakeholders.	Risk competency model														
										To ensure proper training for risk stakeholders.	Risk training														
		Committees: the board should delegate certain functions to well-structured committees but without abdicating its own responsibilities.	King III	2.23	Committees: the board should delegate certain functions to well-structured committees but without abdicating its own responsibilities.	Board committees:	King III	2.23	Board committees:	To formalise decision making structures, escalation protocol & identify risk stakeholders.	Board committees charter / terms of reference	x	x	x	x	x	x	x	x	x	x	x			
						Formal terms of reference should be established and approved for each committee of the board.		2.23.1	Formal terms of reference should be established and approved for each committee of the board.																
						The committees' terms of reference should be reviewed yearly.		2.23.2	The committees' terms of reference should be reviewed yearly.																
						The committees should be appropriately constituted and the composition and the terms of reference should be disclosed in the integrated report.		2.23.3	The committees should be appropriately constituted and the composition and the terms of reference should be disclosed in the integrated report.																

Phase 2 - Round 1: Changes to the conceptual ERM implementation model suggested by the senior risk experts structured interviews

Changes	Additions
---------	-----------

Building blocks		Best practice requirements								Proposed deliverables		Agreed with by (semi-structured interviews):													Comments				
Conceptual	Adjusted	Level 1			Level 2				Purpose			Conceptual	IV1 (AdC)	IV2 (BC)	IV4 (EL)	IV6 (GS)	IV7 (GC)	IV8 (HG)	IV9 (HV)	IV13 (MF)	IV17 (SM)	IV18 (VP)	IV19 (WM)						
		Conceptual	Source	Ref.	Adjusted	Conceptual	Source	Ref.		Adjusted																			
IV. Develop the risk infrastructure.	IV. Develop the risk infrastructure.	Committees: the board should delegate certain functions to well-structured committees but without abdicating its own responsibilities.	King III	2.23	Committees: the board should delegate certain functions to well-structured committees but without abdicating its own responsibilities.	The risk committee should:	King III	4.3.2	The risk committee should:	To formalise decision making structures, escalation protocol & identify risk stakeholders.	Risk committees:																		
						consider the risk management policy and plan and monitor the risk management process;			consider the risk management policy and plan and monitor the risk management process;		Board risk committee charter																		
						have as its members executive and non-executive directors, members of senior management and independent risk management experts to be invited, if necessary;			have as its members executive and non-executive directors, members of senior management and independent risk management experts to be invited, if necessary;		Executive risk committee charter																		
						have a minimum of three members; and			have a minimum of three members; and		Departmental risk committee charter																		
						convene at least twice per year.			convene at least twice per year.																				
						The audit committee should:	King III	3.4	The audit committee should:		Audit committee charter																		
						oversee integrated reporting.			oversee integrated reporting.																				
						have regard to all factors and risks that may impact on the integrity of the integrated report.			have regard to all factors and risks that may impact on the integrity of the integrated report.																				
						review and comment on the financial statements included in the integrated report.			review and comment on the financial statements included in the integrated report.																				
						review the disclosure of sustainability issues in the integrated report to ensure that it is reliable and does not conflict with the financial information.			review the disclosure of sustainability issues in the integrated report to ensure that it is reliable and does not conflict with the financial information.																				
						recommend to the board to engage an external assurance provider on material sustainability issues.			recommend to the board to engage an external assurance provider on material sustainability issues.																				
						consider the need to issue interim results.			consider the need to issue interim results.																				
						review the content of the summarised information.			review the content of the summarised information.																				
						engage the external auditors to provide assurance on the summarised financial information.			engage the external auditors to provide assurance on the summarised financial information.																				
						ensure that a combined assurance model is applied to provide a coordinated approach to all assurance activities.			ensure that a combined assurance model is applied to provide a coordinated approach to all assurance activities.			x	x	x	x	x	x	x	x	x									
						ensure that the combined assurance is received is appropriate to address all the significant risks facing the company.			ensure that the combined assurance is received is appropriate to address all the significant risks facing the company.																				
						monitor the relationship between the external assurance providers and the company.			monitor the relationship between the external assurance providers and the company.																				
						The audit committee should be an integral component of the risk management process.		3.8	The audit committee should be an integral component of the risk management process.																				
						The charter of the audit committee should set out its responsibilities regarding risk management.			The charter of the audit committee should set out its responsibilities regarding risk management.																				
						The audit committee should specifically have oversight of:		3.8.2	The audit committee should specifically have oversight of:																				
						financial reporting			financial reporting																				
						internal financial controls;		3.8.2.2	internal financial controls;																				
						fraud risks as it relates to financial reporting; and			fraud risks as it relates to financial reporting; and																				
						IT risks as it relates to financial reporting.		3.8.2.4	IT risks as it relates to financial reporting.																				

Phase 2 - Round 1: Changes to the conceptual ERM implementation model suggested by the senior risk experts structured interviews

Changes	Additions
---------	-----------

Building blocks		Best practice requirements								Proposed deliverables		Agreed with by (semi-structured interviews):												Comments	
Conceptual	Adjusted	Level 1			Level 2				Purpose			Conceptual	IV1 (AdC)	IV2 (BG)	IV4 (EL)	IV6 (GS)	IV7 (GC)	IV8 (HG)	IV9 (HV)	IV13 (MF)	IV17 (SM)	IV18 (VP)	IV19 (VM)		
		Conceptual	Source	Ref.	Adjusted	Conceptual	Source	Ref.		Adjusted															
IV. Develop the risk infrastructure.	IV. Develop the risk infrastructure.	Committees: the board should delegate certain functions to well-structured committees but without abdication of its own responsibilities.	King III	2.23	Committees: the board should delegate certain functions to well-structured committees but without abdication of its own responsibilities.	The audit committee should also:	King III	3.5	The audit committee should also:	To formalise decision making structures, escalation protocol & identify risk stakeholders.	Integrated assurance committee charter														
						ensure that a combined assurance model is applied to provide a coordinated approach to all assurance activities		3.5.1	ensure that a combined assurance model is applied to provide a coordinated approach to all assurance activities																
						ensure that the combined assurance is received is appropriate to address all the significant risks facing the company.		3.5.2	ensure that the combined assurance is received is appropriate to address all the significant risks facing the company.																
							Round 1 Delphi																		
		Models & tools: the organisation's processes, methods and tools to be used for managing risk	ISO 31000	4.3.5 & 5.7	Models & tools: the organisation's processes, methods and tools to be used for managing risk		Round 1 Delphi		To assess and decide on standardised tools that should be used across the organisation.	Risk identification tools	x	x	x	x	x	x	x	x	x	x	x	x	x		
		Templates: standardised recording, reporting and assessment templates	Researcher		Templates: standardised recording, reporting and assessment templates		Round 1 Delphi		To standardise policy, framework, recording, reporting and assessment templates.	Risk analysis tools	x	x	x	x	x	x	x	x	x	x	x	x	x		
		Processes: documented processes and procedures.	ISO 31000 / King III	4.3.4 & 4.3.5 / 4.4.1	Processes: documented processes and procedures.		Round 1 Delphi		To embed risk management in all the organisation's practices and processes in a way that it is relevant, effective and efficient.	Risk evaluation tools	x	x	x	x	x	x	x	x	x	x	x	x	x		
Systems: information and knowledge management systems	ISO 31000 / King III	4.3.5 & 5.7 / 4.4.1	Systems: information and knowledge management systems		Round 1 Delphi		To select the most appropriate risk management systems.	Risk treatment tools	x	x	x	x	x	x	x	x	x	x	x	x					
V. Implementation.	V. Implement the ERM program.	Implementing the framework for managing risk.	ISO 31000	4.4.1	Implementing the framework for managing risk.	Define the appropriate timing and strategy for implementing the framework;	ISO 31000	4.4.1	Define the appropriate timing and strategy for implementing the framework;	To establish a time line for risk management activities.	Risk management plan (calendar)														
						Apply the risk management policy and process to the organisational processes;			Apply the risk management policy and process to the organisational processes;																

Phase 2 - Round 1: Changes to the conceptual ERM implementation model suggested by the senior risk experts structured interviews

Changes	Additions
---------	-----------

Building blocks		Best practice requirements								Proposed deliverables		Agreed with by (semi-structured interviews):													Comments
Conceptual	Adjusted	Level 1			Level 2				Purpose			Conceptual	IV1 (AdC)	IV2 (BC)	IV4 (EL)	IV6 (GS)	IV7 (GC)	IV8 (HG)	IV9 (HV)	IV13 (MF)	IV17 (SM)	IV18 (VP)	IV19 (VM)		
		Conceptual	Source	Ref.	Adjusted	Conceptual	Source	Ref.		Adjusted	IV1 (AdC)		IV2 (BC)	IV4 (EL)	IV6 (GS)	IV7 (GC)	IV8 (HG)	IV9 (HV)	IV13 (MF)	IV17 (SM)	IV18 (VP)	IV19 (VM)			
V. Implementation.	V. Implement the ERM program.	Implementing the framework for managing risk.	ISO 31000	4.4.1	Implementing the framework for managing risk.	Apply the risk management policy and process to the organisational processes;	ISO 31000	4.4.1	Apply the risk management policy and process to the organisational processes;	To embed risk management in all the organisation's practices and processes in a way that it is relevant, effective and efficient.	Integration of the risk into organisational processes	x	x	x	x	x	x	x	x	x	x	x			
						Comply with legal and regulatory requirements;			Comply with legal and regulatory requirements;	To communicate risk related compliance requirements.	Legal, regulatory & best practice compliance register (pertaining to risk)	x	x	x	x	x	x	x	x	x	x				
						Ensure that decision making, including the development and setting of objectives, is aligned with the outcomes of risk management processes;			Ensure that decision making, including the development and setting of objectives, is aligned with the outcomes of risk management processes;	To encourage a risk mind-set for decision making.	Risk appetite statements	x	x	x	x	x	x	x	x	x					
						Hold information and training sessions; and			Hold information and training sessions; and	To create a common risk language, improve risk awareness and encourage risk based decision making.	Risk tolerance levels	x	x	x	x	x	x	x	x	x					
						Communicate and consult with stakeholders to ensure that its risk management framework remains appropriate.			ISO 31000	4.2 & 4.4.1		To ensure that the risk management framework remains appropriate.	Risk awareness gap analysis	x	x	x	x	x	x	x	x	x	x	x	
		Implementing the risk management process	ISO 31000	4.4.2	Implementing the risk management process.	Step 1: Communication and consultation with external and internal stakeholders should take place during all stages of the risk management process.	ISO 31000	5.2	Step 1: Communication and consultation with external and internal stakeholders should take place during all stages of the risk management process.	To identify the internal and external stakeholders for the organisation / division / department / project.	Stakeholder analysis	x	x	x	x	x	x	x	x	x	x	x			
										To identify the most appropriate communication tools and establish timelines.	Risk communication plan	x	x	x	x	x	x	x	x	x	x				
										To ensure that the right information reaches the right people at the right time.	Risk reports e.g. stress tests, risk & control self-assessments, incident reports, risk treatment plans, key risk indicator reports.	x	x	x	x	x	x	x	x	x					
						Step 2: Establish the context (Know your organisation / division / department / project / risk type)	ISO 31000	5.3	Step 2: Establish the context (Know your organisation / division / department / project / risk type)	To describe the UNIQUE context for the risk management project.															
											Establish the external context	5.3.2 & 4.3.1	Establish the external context	External environment mind map	x	x	x	x	x	x	x	x	x		
											Establish the internal context	5.3.3 & 4.3.1	Establish the internal context	External stakeholder register	x	x	x	x	x	x	x	x	x		
						External stakeholder map	x	x	x					x	x	x	x	x	x	x					
						Internal value chain mind map	x	x	x					x	x	x	x	x	x	x					
						Establishing the context of the risk management process	5.3.4 & 4.3.1	Establishing the context of the risk management process	Internal stakeholder register		x	x	x	x	x	x	x	x	x	x	x				
									Internal stakeholder map		x	x	x	x	x	x	x	x	x	x					
									Standardised risk management context (refer to building block III)		x	x	x	x	x	x	x	x	x	x					
						Apply the risk criteria	5.3.5 & 4.3.1	Apply the risk criteria	Standardised risk criteria (refer to building block III)		x	x	x	x	x	x	x	x	x	x	x				
									Step 3: Risk identification	ISO 31000	5.4.2	Step 3: Risk identification	Process of finding, recognising and describing risks.	Key / Principle / Strategic risk register	x	x	x	x	x	x	x	x	x	x	
										King III	4.5			Divisional / departmental / business unit risk register	x	x	x	x	x	x	x	x	x		
								Emerging risk register		x	x			x	x	x	x	x	x	x					
						Step 4: Risk analysis	ISO 31000	5.4.3	Step 4: Risk analysis	Process to comprehend the nature of risk and to determine the level of risk (e.g. high, medium, low).															
											King III	4.5	Key / Principle / Strategic risk register - risk ratings applied	x	x	x	x	x	x	x	x	x	x		
													Divisional / departmental / business unit risk register - risk ratings applied	x	x	x	x	x	x	x	x	x			
						Step 5: Risk evaluation	ISO 31000	5.4.4	Step 5: Risk evaluation	Process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable.															
											King III	4.5	Key / Principle / Strategic risk profile - risk ratings + current controls applied & risk owners identified	x	x	x	x	x	x	x	x	x	x		
													Divisional / departmental / business unit risk register risk ratings + current controls applied & risk owners identified	x	x	x	x	x	x	x	x	x			
						Step 6: Risk treatment	ISO 31000	5.5	Step 6: Risk response	To identify the most appropriate risk treatment for the most significant risks.															
											King III	4.7	List of risk controls												
													Risk treatment plans												

Phase 2 - Round 1: Changes to the conceptual ERM implementation model suggested by the senior risk experts structured interviews

Changes	Additions
---------	-----------

Building blocks		Best practice requirements								Proposed deliverables		Agreed with by (semi-structured interviews):													Comments
Conceptual	Adjusted	Level 1			Level 2				Purpose			Conceptual	IV1 (AdC)	IV2 (BG)	IV4 (EL)	IV6 (GS)	IV7 (GC)	IV8 (HG)	IV9 (HV)	IV13 (MF)	IV17 (SM)	IV18 (VP)	IV19 (WM)		
		Conceptual	Source	Ref.	Adjusted	Conceptual	Source	Ref.		Adjusted															
VI. Monitor & review.	VI. Monitor and review the ERM program.	Monitoring activities by the Board			Monitoring activities by the Board	King III	4.8	The board should ensure continual risk monitoring by management	To ensure proper risk oversight.	Risk governance framework	x	x	x	x	x	x	x	x	x	x	x				
							4.8.1	The board should ensure that effective and continual monitoring of risk management takes place.	To reduce role confusion and provide clear guidelines for risk monitoring.	Risk management plan (monitoring roles and responsibilities)	x	x	x	x	x	x	x	x	x	x					
							4.8.2	The responsibility for monitoring should be defined in the risk management plan.	To periodically measure progress against, and deviation from, the risk management plan.	Status on risk management plan implementation	x	x	x	x	x	x	x	x	x	x					
		Review activities by the Board	King III	4.1 & 4.3	Review activities by the Board	King III	4.1.2	The board should comment in the integrated report on the effectiveness of the system and process of risk	To periodically review whether the risk management framework, policy and plan are still	Integrated report (risk and opportunities section)	x	x	x	x	x	x	x	x	x	x	x				
							4.1.8	The board should ensure that effective and continual monitoring of risk management takes place.	To periodically measure progress against, and deviation from, the risk management plan.	Risk management plan implementation status report	x	x	x	x	x	x	x	x	x						
						King III	4.1.9	The board should review the implementation of the	To periodically review whether the risk	Risk improvement report	x	x	x	x	x	x	x	x	x	x					
							4.3.3	The performance of the committee should be evaluated once a year by the board.	To ensure effectiveness and efficiency with regards to committee activities.	Board risk committee performance evaluation	x	x	x	x	x	x	x	x	x	x					
		Monitor the risk management framework			Monitor the risk management framework	King III	4.2.3	The board should monitor that risks taken are within the tolerance and appetite levels.	To ensure compliance with the risk appetite framework.	Risk appetite status report	x	x	x	x	x	x	x	x	x	x	x				
									To ensure compliance with the risk tolerance levels.	Risk tolerance status report	x	x	x	x	x	x	x	x	x	x					
						ISO 31000	4.5	Measure risk management performance against indicators, which are periodically reviewed for appropriateness;	To measure risk management performance against indicators, which are periodically reviewed for appropriateness;	KRI performance report	x	x		x	x	x	x	x	x	x					
								Periodically measure progress against, and deviation from, the risk management plan;	To periodically measure progress against, and deviation from, the risk management plan.	Risk management plan implementation status report	x	x	x	x	x	x	x	x	x	x					
								Report on risk, progress with the risk management plan and how well the risk management policy is being	To report on risk, progress with the risk management plan and how well the risk management policy is being	Risk management policy compliance report	x	x	x	x	x	x	x	x	x						
								Monitor the level of risk awareness	To track the improvement of risk awareness.	Risk culture surveys	x	x	x	x	x	x	x	x	x	x					
						Review the risk management framework			Review the risk management framework	ISO 31000	4.5	Periodically review whether the risk management framework, policy and plan	To periodically review whether the risk management framework, policy and plan are still appropriate, given the organisations' external and internal context.	Risk improvement report	x	x	x	x	x	x	x	x	x	x	
		ISO 31000	4.2 & 4.4.1	Communicate and consult with stakeholders to ensure that its risk management framework remains appropriate.																					
			ISO 31000	4.5	Review the effectiveness of the risk management framework.																				
		Monitor the risk management process	ISO 31000	5.6	Monitor the risk management process					ISO 31000	5.6	Ensuring that controls are effective and efficient in both design and operation.		To ensure that controls are effective and efficient in both design and operation.	Risk treatment plans										
						ISO 31000	5.6	Identifying emerging risks.	To identify emerging risks in the organisation's internal value chain and external environment.		Emerging risk register	x	x	x	x	x	x	x	x	x	x				
		Review the risk management process	ISO 31000	5.6	Review the risk management process	ISO 31000	5.6	Analysing and learning lessons from events (including near-misses), changes, trends, successes and failures;	To analyse and learn lessons from events (including near-misses), changes, trends, successes and failures.	Variance and trend analysis	x	x	x	x	x	x	x	x	x	x	x				

Phase 2 - Round 1: Changes to the conceptual ERM implementation model suggested by the senior risk experts structured interviews

Changes	Additions
---------	-----------

Building blocks		Best practice requirements								Proposed deliverables		Agreed with by (semi-structured interviews):												Comments
Conceptual	Adjusted	Level 1			Level 2				Purpose			Conceptual	IV1	IV2	IV4	IV6	IV7	IV8	IV9	IV13	IV17	IV18	IV19	
		Conceptual	Source	Ref.	Adjusted	Conceptual	Source	Ref.		Adjusted	(AdC)		(BG)	(EL)	(GS)	(GC)	(HG)	(HV)	(MF)	(SM)	(VP)	(WM)		
VII. Continual improvement.	VII. Continual improvement of the ERM program.	Management should provide assurance to the board that the risk management plan is integrated in the daily activities of the company.	King III	4.9	Management should provide assurance to the board that the risk management plan is integrated in the daily activities of the company.		King III	4.9.1		To inform the relevant committees and risk stakeholders of the level of assurance provided by assurance providers.	Integrated assurance report.	x	x	x	x	x	x	x	x	x	x	x		
		Internal audit should: provide a written assessment of the effectiveness of the system of internal controls and risk management to the board.				Internal audit should: provide a written assessment of the effectiveness of the system of internal controls and risk management to the board.		King III	4.9.2		To periodically review whether the risk management framework, policy and plan are still appropriate, given the organisations' external and internal context;	Risk improvement report	x	x	x	x	x	x	x	x	x	x	x	
										ISO 31000		5.6	Detecting changes in the external and internal context, including changes to risk criteria and the risk itself which can require revision of risk treatments and priorities; and	Risk improvement report (List of internal, external, risk management process & risk criteria context changes)	x	x	x	x	x	x	x	x	x	x
					5.6	Obtaining further information to improve risk assessment.	Risk improvement report (risk assessment process & methodology)	x	x			x	x	x	x	x	x	x	x					

own compilation

Addendum I: Adjusted ERM implementation model: theoretical frameworks, building blocks, best practice requirements and proposed deliverables

Key: Changes and additions from the conceptual to the adjusted model						
Theoretical frameworks		Building blocks	Best practice requirements		Proposed deliverables	
Deming cycle	Weisbord organisational design model		Level 1	Level 2	Purpose	Deliverables
Plan	Purpose, Leadership	I. Formalise the instruction and get permission.	Instruction / Trigger	Business trigger e.g. event, merger & acquisition due diligence requirement, peer pressure, etc.	To motivate the need for an ERM program.	Business case document
				Ensure legal and regulatory compliance.	To motivate the need for an ERM program.	Compliance register (legal + regulatory + best practise frameworks)
			Permission / Mandate	The board should delegate to management the responsibility to design, implement and monitor the risk management plan.	To ask for permission / mandate to design and implement the ERM program.	Agenda item for the decision making forum e.g. Board meeting, Executive committee meeting.
					To record the permission / mandate received to design and implement an ERM program.	Minutes of the decision making forum e.g. Board meeting, Executive committee meeting.
			Oversight: the risk committee or audit committee should assist the board in carrying out its risk responsibilities	The board should appoint a committee responsible for risk.	To assist the board in carrying out its risk roles and responsibilities.	Board risk committee (BRC) terms of reference / Audit committee charter / Audit and risk committee charter
				The risk committee should:		
				consider the risk management policy and plan and monitor the risk management process;		
				have as its members executive and non-executive directors, members of senior management and independent risk management experts to be invited, if necessary;		
				have a minimum of three members; and		
				convene at least twice per year.		
				The board's responsibility for risk governance should be expressed in the board charter.		

Addendum I: Adjusted ERM implementation model: theoretical frameworks, building blocks, best practice requirements and proposed deliverables

Key: Changes and additions from the conceptual to the adjusted model						
Theoretical frameworks		Building blocks	Best practice requirements		Proposed deliverables	
Deming cycle	Weisbord organisational design model		Level 1	Level 2	Purpose	Deliverables
Plan	Purpose	I. Formalise the instruction and get permission.	Define and endorse the risk management policy	The board's responsibility for risk governance should manifest in a documented risk management policy and plan. The board should approve the risk management policy and plan. The risk management policy should be widely distributed throughout the company.	To document risk management scope, objectives and roles and responsibilities.	Risk management policy
Plan	Leadership, Relationships	II. Establish the tone of the organisation.	Establishing the tone of the organisation: The introduction of risk management and ensuring its ongoing effectiveness require strong and sustained commitment by management of the organisation, as well as strategic and rigorous planning to achieve commitment at all levels.	The CRO should be a suitably experienced person who should have access and interact regularly on strategic matters with the board and/or appropriate board committee and executive management. (a) Ensure that the organisation's culture and risk management policy are aligned. (b) Determine risk management performance indicators that align with performance indicators of the organisation. (c) Align risk management objectives with the objectives and strategies of the organisation. (d) Assign accountabilities and responsibilities at appropriate levels within the organisation.	A senior level ERM program sponsor / Chief Risk Officer should have clear authority over and accountability for oversight of risk across the enterprise To create risk awareness at all levels of the organisations and to encourage risk based decision making. To measure risk management performance against indicators, which are periodically reviewed for appropriateness; To encourage a risk mind-set for decision making. To reduce role confusion by establishing clear roles and responsibilities for risk activities across businesses and risk types.	CRO / Senior level project sponsor Risk management policy / Risk requirements evident in business, project and HR requirements and standards / Strategic intent document / Risk communication strategy / Internal audit reports / External audit report / Insurance claims Performance indicators (Key risk indicators) Strategic plan / Business plan / Risk plan / Risk management objectives / Risk appetite statement / Risk tolerance levels Risk governance model: (incl. risk owners' matrix, roles & responsibilities, reporting & escalation process & incentives guidelines & individual performance scorecard.)

Addendum I: Adjusted ERM implementation model: theoretical frameworks, building blocks, best practice requirements and proposed deliverables

Key: Changes and additions from the conceptual to the adjusted model						
Theoretical frameworks		Building blocks	Best practice requirements		Proposed deliverables	
Deming cycle	Weisbord organisational design model				Purpose	Deliverables
Plan	Leadership, Relationships	II. Establish the tone of the organisation.	Establishing the tone of the organisation: introduction of risk management and ensuring its ongoing effectiveness require strong and sustained commitment by management of the organisation, as well as strategic and rigorous planning to achieve commitment at all levels.	(e) Ensure that the necessary resources are allocated to risk management.	To ensure the effective and efficient implementation of the ERM program.	Risk management plan (People, Processes and Budget) / Annual performance plan / Operational budget
				(f) Communicate the benefits of risk management to all stakeholders.	To raise risk awareness and create excitement for the project.	Risk training material / Business case / Risk management policy / Embedded in risk reports / Board risk report
			The induction and ongoing training programs of the board should incorporate risk governance. (Note: apply to all the levels in the		To create a common risk language, improve risk awareness and encourage risk based decision making.	Risk awareness gap analysis
						Risk maturity assessment
					Risk awareness strategy & plan	
Plan	Purpose, Relationships, Structure, External environment	III. Design the rules of the game.	Design the risk management framework.	Task: Understanding the organisation and its context (Know your organisation)		
				Establish the external context:		
				(a) the social and cultural, political, legal, regulatory, financial, technological, economic, natural and competitive environment, whether international, national, regional or local;	To get an overall picture of the external environment based PESTLE and / or Porter's 5 forces.	Environmental scanning report
				(b) key drivers and trends having impact on the objectives of the organisation; and		Key business drivers report
				(c) External stakeholder analysis		Stakeholder analysis
				Establish the internal context:	To describe the internal value chain of the organisation and to identify areas that would create risks and opportunities	
				(a) Governance, organisational structure, roles and accountabilities;		Environmental scanning of the INTERNAL value chain
						SWOT analysis
						Organisational organigram
						Divisional organigram
						Departmental organigram
				(b) Policies, objectives, and the strategies that are in place to achieve them;		Delegation of authority
						Committee structure
						Committee charters
				(c) Capabilities, understood in terms of resources and knowledge (e.g. capital, time, people, processes, systems and technologies);		List of policies
						Copy of policies
						Action plans (strategies)
						Risk competency model
						Job profiles / specification

Addendum I: Adjusted ERM implementation model: theoretical frameworks, building blocks, best practice requirements and proposed deliverables

Key: Changes and additions from the conceptual to the adjusted model									
Theoretical frameworks		Building blocks	Best practice requirements		Proposed deliverables				
Deming cycle	Weisbord organisational design model				Purpose	Deliverables			
Plan	Purpose, Relationships, Structure, External environment	III. Design the rules of the game.	Level 1	(d) Information systems, information flows and decision making processes (both formal and informal)	To describe the internal value chain of the organisation and to identify areas that would create risks and opportunities	List of systems			
						Process maps			
						Escalation policy			
						Escalation process			
						Connected stakeholder analysis			
						Internal stakeholder analysis			
						Organisational culture survey results			
						List of standards, guidelines and models			
						Contracts register			
						Internal audit reports			
						External audit reports			
						Strategic plan			
						Business plans			
						Level 2	Establish the context of the risk management process (The context of the risk management process will vary according to the needs of an organisation. It can involve, but is not limited to:	To create ONE set of risk management rules for the organisation.	Risk management file / manual that includes:
									Risk management goals & -objectives
									Risk governance model
									Top-down & Bottom-up risk management activities
			Interconnectedness maps						
			Risk assessment methodologies						
			Level 1	(e) Internal stakeholder analysis	To create ONE set of risk management rules for the organisation.	Key risk indicators			
						Decision matrix			
						Research to clarify context			
						Level 2	(f) Temperature checks on organisational culture	To create ONE set of risk management rules for the organisation.	Risk management file / manual that includes:
Risk management goals & -objectives									
Risk governance model									
Level 2	(g) Standards, guidelines and models adopted by the organisation; and	To create ONE set of risk management rules for the organisation.	Top-down & Bottom-up risk management activities						
				Interconnectedness maps					
				Risk assessment methodologies					
Level 2	(h) the form and extent of contractual relationships.	To create ONE set of risk management rules for the organisation.	Key risk indicators						
				Decision matrix					
				Research to clarify context					

Addendum I: Adjusted ERM implementation model: theoretical frameworks, building blocks, best practice requirements and proposed deliverables

Key: Changes and additions from the conceptual to the adjusted model										
Theoretical frameworks		Building blocks	Best practice requirements		Proposed deliverables					
Deming cycle	Weisbord organisational design model				Purpose	Deliverables				
Plan	Purpose, Relationships, Structure, External environment	III. Design the rules of the game.	Level 1	Level 2	To create standardised risk assessment criteria for the organisation as a whole. To give risk owners and other risk stakeholders insight into risk management in their terms.	Risk management file / manual that includes:				
						Examples of causes and consequences				
						Risk assessment tools and techniques				
						Risk management plan				
						Risk appetite guidelines				
						Risk tolerance levels guidelines				
				Task: establishing the risk management policy	To document risk management scope, objectives and roles and responsibilities.	Risk management policy				
							(a) A policy and plan for a system and process of risk management should be developed.			
							(c) The board's responsibility for risk governance should manifest in a documented risk management policy and plan.			
							(d) The board should approve the risk management policy and plan.			
							The risk management policy should be widely distributed throughout the company.			
							Task: develop an accountability matrix / risk governance framework	To establish clear roles and responsibilities for risk activities across businesses and risk types.	Risk governance framework: (incl. risk owners' matrix, roles & responsibilities, reporting & escalation process & incentives guidelines & individual performance scorecards)	
										(a) Identifying risk owners that have the accountability and authority to manage risks;
										(b) Identifying who is accountable for the development, implementation and maintenance of the framework for managing risk;
										(c) Identifying other responsibilities of people at all levels in the organisation for the risk management process;
				(d) Establishing performance measurement and external and/or internal reporting and escalation processes; and						
(e) Ensuring appropriate levels of recognition.										

Addendum I: Adjusted ERM implementation model: theoretical frameworks, building blocks, best practice requirements and proposed deliverables

Key: Changes and additions from the conceptual to the adjusted model							
Theoretical frameworks		Building blocks	Best practice requirements		Proposed deliverables		
Deming cycle	Weisbord organisational design model				Purpose	Deliverables	
Plan	Purpose, Relationships, Structure, External environment	III. Design the rules of the game.	Design the risk management framework.	Task: integration into organisational processes	To embed risk management in all the organisation's practices and processes in a way that it is relevant, effective and efficient.		
				Develop a common risk language		Common risk language	
				Risk management should be embedded in all the organisation's practices and processes in a way that it is relevant, effective and efficient.		To embed risk management in all the organisation's practices and processes in a way that it is relevant, effective and efficient.	Risk owners
							Strategic plan
							Business plan
							Financial plan
							Risk & incident escalation process
							New products development
							Operational processes
							Investment decisions
							Combined assurance
							Performance management process
			Change management process				
			Quality assurance process				
			Align risk management objectives with the objectives and strategies of the organisation.	To encourage a risk mind-set for decision making.	Risk appetite guidelines		
					Risk tolerance levels guidelines		
				Determine risk management performance indicators that align with performance indicators of the organisation.	To measure risk management performance against indicators, which are periodically reviewed for appropriateness;	Strategic plans	
						Business plans	
						Performance reporting metrics, i.e. key risk indicators	
			Task: Establishing internal communication and reporting mechanisms	To create one set of rules for risk communication and also to increase risk transparency.	Internal reporting guidelines		
					Communication guidelines		
	(a) Key components of the risk management framework, and any subsequent modifications, are communicated appropriately;	To create one set of rules for risk communication and also to increase risk transparency.					
	(b) there is adequate internal reporting on the framework, its effectiveness and the outcomes;						
	(c) relevant information derived from the application of risk management is available at appropriate levels and times; and						
(d) there are processes for consultation with internal stakeholders.							

Addendum I: Adjusted ERM implementation model: theoretical frameworks, building blocks, best practice requirements and proposed deliverables

Key: Changes and additions from the conceptual to the adjusted model

Theoretical frameworks		Building blocks	Best practice requirements		Proposed deliverables	
Deming cycle	Weisbord organisational design model		Level 1	Level 2	Purpose	Deliverables
Plan	Purpose, Relationships, Structure, External environment	III. Design the rules of the game.	Design the risk management framework.	Task: Establishing external communication and reporting mechanisms	To create one set of rules for risk communication and also to increase risk transparency.	
				(a) Engaging appropriate external stakeholders and ensuring an effective exchange of information;		External reporting guidelines
				(b) External reporting to comply with legal, regulatory, and governance requirements;		Communication guidelines
				(c) Providing feedback and reporting on communication and consultation;		
			Design the risk management process.	Step 1: Communication and consultation	To develop a standardised risk management process for the organisation.	Risk management process guidelines
				Step 2: Establish the context		
				Step 3: Risk identification		
				Step 4: Risk analysis		
				Step 5: Risk evaluation		
				Step 6: Risk treatment		
				Step 7: Monitor and review		
				Step 8: Continuous improvement		
Plan	Helping mechanisms, Relationships, Rewards	IV. Develop the risk infrastructure.	Task: Allocate appropriate resources for risk management			
			People (skills, experience, competence & training programs).	People: skills, experience, competence & training programs	To establish decision making structures, escalation protocol & identify risk stakeholders.	Risk governance models
						Performance management scorecards
					To identify competencies, skills levels and experience required by risk stakeholders.	Job profiles
					To ensure proper training for risk stakeholders.	Risk training: induction sessions and risk awareness sessions
			Committees: the board should delegate certain functions to well-structured committees but without abdicating its own responsibilities.	Board committees:	To formalise decision making structures, escalation protocol & identify risk stakeholders.	
				Formal terms of reference should be established and approved for each committee of the board.		Board committees charter / terms of reference
				The committees' terms of reference should be reviewed yearly.		
				The committees should be appropriately constituted and the composition and the terms of reference should be disclosed in the integrated report.		Integrated report
				The risk committee should:		Risk committees:
				consider the risk management policy and plan and monitor the risk management process;		Board risk committee terms of reference
				have as its members executive and non-executive directors, members of senior management and independent risk management experts to be invited, if necessary;		Executive risk committee terms of reference
				have a minimum of three members; and		Departmental risk committee terms of reference

Addendum I: Adjusted ERM implementation model: theoretical frameworks, building blocks, best practice requirements and proposed deliverables

Key: Changes and additions from the conceptual to the adjusted model						
Theoretical frameworks		Building blocks	Best practice requirements		Proposed deliverables	
Deming cycle	Weisbord organisational design model				Purpose	Deliverables
Plan	Helping mechanisms, Relationships, Rewards	IV. Develop the risk infrastructure.	Level 1 			

Addendum I: Adjusted ERM implementation model: theoretical frameworks, building blocks, best practice requirements and proposed deliverables

Key: Changes and additions from the conceptual to the adjusted model

Theoretical frameworks		Building blocks	Best practice requirements		Proposed deliverables	
Deming cycle	Weisbord organisational design model		Level 1	Level 2	Purpose	Deliverables
Plan	Helping mechanisms, Relationships, Rewards	IV. Develop the risk infrastructure.	Committees: the board should delegate certain functions to well-structured committees but without abdicating its own responsibilities.		To formalise decision making structures, escalation protocol & identify risk stakeholders.	Risk specific committee terms of reference e.g. Fraud risk committee
			Models & tools: the organisation's processes, methods and tools to be used for managing risk		To assess and decide on standardised tools that should be used across the organisation.	Risk identification tools
						Risk analysis tools
						Risk evaluation tools
						Risk response tools
						Risk monitoring tools
						Risk reporting tools
						Risk quantification models
			Templates: standardised recording, reporting and assessment templates		To standardise policy, framework, recording, reporting and assessment templates.	Examples:
						Risk management plan
						Risk communication plan
						Stakeholder maps
						Stakeholder register
						Risk register
						Risk improvement report
						Integrated assurance dashboard
						Integrated report
						Risk self-assessments
						Stewardship report
						Recording process
						Risk acceptance form
						Risk retirement form
						Reporting dashboards
						Reporting scorecards
						Risk policy
						Risk management framework
						Risk committee terms of reference
			Processes: documented processes and procedures.		To embed risk management in all the organisation's practices and processes in a way that it is relevant, effective and efficient.	Common risk language
						Risk owners matrix
						Strategic planning process
						Business planing process
						Financial planning process
						Change management process
						Quality assurance process
						Risk management process
						Risk & incident escalation process
						External audit process
						Performance management process
			Systems: information and knowledge management systems		To select the most appropriate risk management systems.	Risk recording
						Risk reporting
						Risk monitoring
						Risk review

Addendum I: Adjusted ERM implementation model: theoretical frameworks, building blocks, best practice requirements and proposed deliverables

Key: Changes and additions from the conceptual to the adjusted model

Theoretical frameworks		Building blocks	Best practice requirements		Proposed deliverables	
Deming cycle	Weisbord organisational design model		Level 1	Level 2	Purpose	Deliverables
Do	Leadership, Structure, Relationships, Helping Mechanisms, External environment	V. Implement the ERM program.	Implementing the framework for managing risk.	Define the appropriate timing and strategy for implementing the framework;	To establish a time line for risk management activities.	Risk management plan (calendar)
						Critical path analysis for key dependencies
				Apply the risk management policy and process to the organisational processes;	To embed risk management in all the organisation's practices and processes in a way that it is relevant, effective and efficient.	Common risk language
						Risk owners matrix
						Strategic planning process
						Business planning process
						Financial planning process
						Change management process
						Quality assurance process
						Risk management process
						Risk & incident escalation process
						Performance management process
			Implementing the risk management process.	Comply with legal and regulatory requirements;	To communicate risk related compliance requirements.	Legal, regulatory & best practice compliance register (pertaining to risk)
				Ensure that decision making, including the development and setting of objectives, is aligned with the outcomes of risk management processes;	To encourage a risk mind-set for decision making.	Risk appetite statements
						Risk tolerance levels
				Hold information and training sessions; and	To create a common risk language, improve risk awareness and encourage risk based decision making.	Strategic plan
						ERM framework & policy
				Communicate and consult with stakeholders to ensure that its risk management framework remains appropriate.	To ensure that the risk management framework remains appropriate.	Risk awareness gap analysis
						Risk maturity assessment
				Step 1: Communication and consultation with external and internal stakeholders should take place during all stages of the risk management process.	To identify the internal and external stakeholders for the organisation / division / department / project.	Risk awareness strategy & -plan
						Stakeholder analysis
						Risk communication plan
				Step 2: Establish the context (Know your organisation / division / department / project / risk type)	To identify the most appropriate communication tools and establish timelines.	Risk reports e.g. stress tests, risk & control self-assessments, incident reports, risk treatment plans, key risk indicator reports.
				Establish the external context	To describe the UNIQUE context for the risk management project.	External environment mind map
						External stakeholder register
				Establish the internal context		External stakeholder map
						Internal value chain mind map
				Establishing the context of the risk management process		Internal stakeholder register
				Apply the risk criteria		Internal stakeholder map
						Standardised risk management context (refer to building block III)
						Standardised risk criteria (refer to building block III)

Addendum I: Adjusted ERM implementation model: theoretical frameworks, building blocks, best practice requirements and proposed deliverables

Key: Changes and additions from the conceptual to the adjusted model						
Theoretical frameworks		Building blocks	Best practice requirements		Proposed deliverables	
Deming cycle	Weisbord organisational design model		Level 1	Level 2	Purpose	Deliverables
Do	Leadership, Structure, Relationships, Helping Mechanisms, External environment	V. Implement the ERM program.	Implementing the risk management process.	Step 3: Risk identification	Process of finding, recognising and describing risks.	Key / Principle / Strategic risk register
						Divisional / departmental / business unit risk register
						Emerging risk register
						Risk library
				Step 4: Risk analysis	Process to comprehend the nature of risk and to determine the level of risk (e.g. high, medium, low).	Key / Principle / Strategic risk register - risk ratings applied
						Divisional / departmental / business unit risk register - risk ratings applied
						Root cause analysis
						Key / Principle / Strategic risk profile - risk ratings + current controls applied & risk owners identified
						Divisional / departmental / business unit risk register risk ratings + current controls applied & risk owners identified
						Controls library
						Risk response plans / Action plans
Check	Rewards	VI. Monitor and review the ERM program.	Monitoring activities by the Board	Step 6: Risk response	To identify the most appropriate risk treatment for the most significant risks.	Risk response options
				The board should ensure continual risk monitoring by management	To ensure proper risk oversight.	Risk governance framework
						Risk management plan (monitoring roles and responsibilities)
						Status report on risk management plan implementation
			Review activities by the Board	The board should ensure that effective and continual monitoring of risk management takes place.	To reduce role confusion and provide clear guidelines for risk monitoring.	Integrated report (risk and opportunities section)
				The responsibility for monitoring should be defined in the risk management plan.	To periodically measure progress against, and deviation from, the risk management plan.	
				The board should comment in the integrated report on the effectiveness of the system and process of risk management.	To periodically review whether the risk management framework, policy and plan are still appropriate, given the organisations' external and internal context;	Annual board risk report
				The board should ensure that effective and continual monitoring of risk management takes place.	To periodically measure progress against, and deviation from, the risk management plan.	Risk management plan implementation status report
				The board should review the implementation of the risk management plan at least once a year.	To periodically review whether the risk management framework, policy and plan are still appropriate, given the organisations' external and internal context;	Risk improvement report
				The performance of the committee should be evaluated once a year by the board.	To ensure effectiveness and efficiency with regards to committee activities.	Internal audit report
			Monitor the risk management framework	The board should monitor that risks taken are within the tolerance and appetite levels.	To ensure compliance with the risk appetite framework.	Board risk committee performance evaluation
					To ensure compliance with the risk tolerance levels.	Risk appetite status report
				Measure risk management performance against indicators, which are periodically reviewed for appropriateness;	To ensure compliance with the risk tolerance levels.	Risk tolerance status report
						KRI performance report
				Periodically measure progress against, and deviation from, the risk management plan;	To periodically measure progress against, and deviation from, the risk management plan.	Risk management plan implementation status report

Addendum I: Adjusted ERM implementation model: theoretical frameworks, building blocks, best practice requirements and proposed deliverables

Key: Changes and additions from the conceptual to the adjusted model						
Theoretical frameworks		Building blocks	Best practice requirements		Proposed deliverables	
Deming cycle	Weisbord organisational design model		Level 1	Level 2	Purpose	Deliverables
Check	Rewards	VI. Monitor and review the ERM program.	Monitor the risk management framework	Report on risk, progress with the risk management plan and how well the risk management policy is being followed;	To report on risk, progress with the risk management plan and how well the risk management policy is being followed.	Risk management policy compliance report
						Deviations from risk management policy report
				Monitor the level of risk awareness	To track the improvement of risk awareness.	Risk culture surveys
			Review the risk management framework	Periodically review whether the risk management framework, policy and plan are still appropriate, given the organizations' external and internal context;	To periodically review whether the risk management framework, policy and plan are still appropriate, given the organisations' external and internal context.	Risk improvement report
						Internal audit report
						Risk calendar
						Risk improvement report
				Communicate and consult with stakeholders to ensure that its risk management framework remains appropriate.		Subject matter expert gap analysis
						Internal audit reports
						Risk calendar
						ISO 9000 reports
				Review the effectiveness of the risk management framework.		Internal audit reports, risk committee effectiveness, qualitative conversations, risk appetite and risk tolerance level breaches, signed letters of representation.
			Monitor the risk management process	Ensuring that controls are effective and efficient in both design and operation.	To ensure that controls are effective and efficient in both design and operation.	Subject matter expert gap analysis
						Combined assurance reports
						Risk profile status reports
						Internal audit reports
						External audit reports
				Identifying emerging risks.	To identify emerging risks in the organisation's internal value chain and external environment.	Emerging risk register
			Review the risk management process	Analysing and learning lessons from events (including near-misses), changes, trends, successes and failures;	To analyse and learn lessons from events (including near-misses), changes, trends, successes and failures.	Variance and trend analysis
						Post mortem sessions
						Environmental scanning
						Risk reconciliation reports
						Post loss analysis

Addendum I: Adjusted ERM implementation model: theoretical frameworks, building blocks, best practice requirements and proposed deliverables

Key: Changes and additions from the conceptual to the adjusted model						
Theoretical frameworks		Building blocks	Best practice requirements		Proposed deliverables	
Deming cycle	Weisbord organisational design model		Level 1	Level 2	Purpose	Deliverables
Adjust	Leadership, Purposes, Structure, Relationships, Rewards, Helpful mechanisms, External environment	VII. Continual improvement of the ERM program.	The board should receive assurance regarding the effectiveness of the risk management process	Management should provide assurance to the board that the risk management plan is integrated in the daily activities of the company.	To inform the relevant committees and risk stakeholders of the level of assurance provided by assurance providers.	Combined assurance report.
						Risk reports to various committees
						Risk maturity assessment
						Benchmarking assessments (peer reviews & best practice)
				Internal audit should:	To periodically review whether the risk management framework, policy and plan are still appropriate, given the organisations' external and internal context;	
				provide a written assessment of the effectiveness of the system of internal controls		Risk improvement report
				detect changes in the external and internal context, including changes to risk criteria and the risk itself which can require revision of risk treatments and priorities; and		Internal audit report
				obtaining further information to improve risk assessment.		Risk improvement report (List of internal, external, risk management process & risk criteria context changes)
		Risk improvement report (risk assessment process & methodology)				

Source: Researcher's own compilation

Addendum J: Phase 2 - Round 2: Validate the adjusted ERM implementation model: theoretical frameworks, building blocks, best practice requirements and proposed deliverables

Theoretical frameworks		Building blocks	Best practice requirements		Proposed deliverables		IV1		IV2		IV4		IV6		IV7	
Deming cycle	Weisbord organisational design model		Level 1	Level 2	Purpose	Deliverables	Agree	Dis-agree	Agree	Dis-agree	Agree	Dis-agree	Agree	Dis-agree	Agree	Dis-agree
Plan	Purpose, Leadership	I. Formalise the instruction and get permission.	Instruction / Trigger	Business trigger e.g. event, merger & acquisition due diligence requirement, peer pressure, etc.	To motivate the need for an ERM program.	Business case document	x		x		x		x		x	
				Ensure legal and regulatory compliance.	To motivate the need for an ERM program.	Compliance register (legal + regulatory + best practise frameworks)	x		x		x		x		x	
			Permission / Mandate	The board should delegate to management the responsibility to design, implement and monitor the risk management plan.	To ask for permission / mandate to design and implement the ERM program.	Agenda item for the decision making forum e.g. Board meeting, Executive committee meeting.	x		x		x		x		x	
					To record the permission / mandate received to design and implement an ERM program.	Minutes of the decision making forum e.g. Board meeting, Executive committee meeting.	x		x		x		x		x	
			Oversight: the risk committee or audit committee should assist the board in carrying out its risk responsibilities	The board should appoint a committee responsible for risk.	To assist the board in carrying out its risk roles and responsibilities.	Board risk committee (BRC) terms of reference / Audit committee charter / Audit and risk committee charter	x				x		x		x	
				The risk committee should:												
				consider the risk management policy and plan and monitor the risk management process;												
				have as its members executive and non-executive directors, members of senior management and independent risk management experts to be invited, if necessary;												
				have a minimum of three members; and												
				convene at least twice per year.												
				The board's responsibility for risk governance should be expressed in the board charter.												
			Define and endorse the risk management policy	The board's responsibility for risk governance should manifest in a documented risk management policy and plan.	To document risk management scope, objectives and roles and responsibilities.	Risk management policy	x				x		x		x	
				The board should approve the risk management policy and plan.												
				The risk management policy should be widely distributed throughout the company.												

Addendum J: Phase 2 - Round 2: Validate the adjusted ERM implementation model: theoretical frameworks, building blocks, best practice requirements and proposed deliverables

Theoretical frameworks		Building blocks	Best practice requirements		Proposed deliverables		IV1		IV2		IV4		IV6		IV7					
Deming cycle	Weisbord organisational design model				Purpose	Deliverables	Agree	Dis-agree	Agree	Dis-agree	Agree	Dis-agree	Agree	Dis-agree	Agree	Dis-agree				
Plan	Leadership, Relationships	II. Establish the tone of the organisation.	Establishing the tone of the organisation: The introduction of risk management and ensuring its ongoing effectiveness require strong and sustained commitment by management of the organisation, as well as strategic and rigorous planning to achieve commitment at all levels.		A senior level ERM program sponsor / Chief Risk Officer should have clear authority over and accountability for oversight of risk across the enterprise	CRO / Senior level project sponsor	x		x		x		x		x					
				(a) Ensure that the organisation's culture and risk management policy are aligned.	To create risk awareness at all levels of the organisations and to encourage risk based decision making.	Risk management policy / Risk requirements evident in business, project and HR requirements and standards / Strategic intent document / Risk communication strategy / Internal audit reports / External audit report / Insurance claims	x		x		x		x		x					
				(b) Determine risk management performance indicators that align with performance indicators of the organisation.	To measure risk management performance against indicators, which are periodically reviewed for appropriateness;	Performance indicators (Key risk indicators)	x		x		x		x		x					
				(c) Align risk management objectives with the objectives and strategies of the organisation.	To encourage a risk mind-set for decision making.	Strategic plan / Business plan / Risk plan / Risk management objectives / Risk appetite statement / Risk tolerance levels	x		x		x		x		x					
				(d) Assign accountabilities and responsibilities at appropriate levels within the organisation.	To reduce role confusion by establishing clear roles and responsibilities for risk activities across businesses and risk types.	Risk governance model: (incl. risk owners' matrix, roles & responsibilities, reporting & escalation process & incentives guidelines & individual performance scorecard.)	x		x		x		x		x					
				(e) Ensure that the necessary resources are allocated to risk management.	To ensure the effective and efficient implementation of the ERM program.	Risk management plan (People, Processes and Budget) / Annual performance plan / Operational budget	x		x		x		x		x					
				(f) Communicate the benefits of risk management to all stakeholders.	To raise risk awareness and create excitement for the project.	Risk training material / Business case / Risk management policy / Embedded in risk reports / Board risk report	x		x		x		x		x					
			The induction and ongoing training programs of the board should incorporate risk governance. (Note: apply to all the levels in the organisation)		To create a common risk language, improve risk awareness and encourage risk based decision making.	Risk awareness gap analysis	x		x		x		x		x					
						Risk maturity assessment	x		x		x		x		x					
						Risk awareness strategy & plan	x		x		x		x		x					
Plan	Purpose, Relationships, Structure, External environment	III. Design the rules of the game.	Design the risk management framework.	Task: Understanding the organisation and its context (Know your organisation)																
				Establish the external context:																
				(a) the social and cultural, political, legal, regulatory, financial, technological, economic, natural and competitive environment, whether international, national, regional or local;	To get an overall picture of the external environment based PESTLE and / or Porter's 5 forces.	Environmental scanning report	x		x		x		x		x		x			
				(b) key drivers and trends having impact on the objectives of the organisation; and		Key business drivers report	x		x		x		x		x		x			
				(c) External stakeholder analysis		Stakeholder analysis	x		x		x		x		x		x			
				Establish the internal context:																
				(a) Governance, organisational structure, roles and accountabilities;	To describe the internal value chain of the organisation and to identify areas that would create risks and opportunities	Environmental scanning of the INTERNAL value chain	x		x		x		x		x		x		x	
						SWOT analysis	x		x		x		x		x		x		x	
						Organisational organigram	x		x		x		x		x		x		x	
						Divisional organigram	x		x		x		x		x		x		x	
						Departmental organigram	x		x		x		x		x		x		x	
						Delegation of authority	x		x		x		x		x		x		x	
						Committee structure	x		x		x		x		x		x		x	
						Committee charters	x		x		x		x		x		x		x	
						List of policies	x		x		x		x		x		x		x	
						Copy of policies	x		x		x		x		x		x		x	
				(b) Policies, objectives, and the strategies that are in place to achieve them;	Action plans (strategies)	x		x		x		x		x		x		x		
					(c) Capabilities, understood in terms of resources and knowledge (e.g. capital, time, people, processes, systems and technologies);	Risk competency model	x		x		x		x		x		x		x	
						Job profiles / specification	x		x		x		x		x		x		x	
						Technical job specs	x		x		x		x		x		x		x	

Addendum J: Phase 2 - Round 2: Validate the adjusted ERM implementation model: theoretical frameworks, building blocks, best practice requirements and proposed deliverables

Theoretical frameworks		Building blocks	Best practice requirements		Proposed deliverables		IV1		IV2		IV4		IV6		IV7	
Deming cycle	Weisbord organisational design model		Level 1	Level 2	Purpose	Deliverables	Agree	Dis-agree	Agree	Dis-agree	Agree	Dis-agree	Agree	Dis-agree	Agree	Dis-agree
Plan	Purpose, Relationships, Structure, External environment	III. Design the rules of the game.		(d) Information systems, information flows and decision making processes (both formal and informal)	To describe the internal value chain of the organisation and to identify areas that would create risks and opportunities	List of systems	x		x		x		x		x	
						Process maps	x		x		x		x		x	
						Escalation policy	x		x		x		x		x	
						Escalation process	x		x		x		x		x	
				Connected stakeholder analysis		Connected stakeholder analysis	x		x		x		x		x	
				(e) Internal stakeholder analysis		Internal stakeholder analysis	x		x		x		x		x	
				(f) Temperature checks on organisational culture		Organisational culture survey results	x		x		x		x		x	
				(g) Standards, guidelines and models adopted by the organisation; and		List of standards, guidelines and models	x		x		x		x		x	
				(h) the form and extent of contractual relationships.		Contracts register	x		x		x		x		x	
						Internal audit reports	x		x		x		x		x	
						External audit reports	x		x		x		x		x	
						Strategic plan	x		x		x		x		x	
						Business plans	x		x		x		x		x	
			Design the risk management framework.	Establish the context of the risk management process (The context of the risk management process will vary according to the needs of an organisation. It can involve, but is not limited to:	To create ONE set of risk management rules for the organisation.	Risk management file / manual that includes:										
				(a) Defining the goals and objectives of the risk management activities;		Risk management goals & -objectives	x		x		x		x		x	
				(b) Defining responsibilities for and within the risk management process;		Risk governance model	x		x		x		x		x	
				(c) Defining the scope, as well as the depth and breadth of the risk management activities to be carried out, including specific		Top-down & Bottom-up risk management activities	x		x		x		x		x	
				(e) Defining the activity, process, function, project, product, service or asset in terms of time and location;		Interconnectedness maps	x		x		x		x		x	
				(f) Defining the relationships between a particular project, process or activity and other projects, processes or activities of the organisation;		Risk assessment methodologies	x		x		x		x		x	
				(g) Defining the risk assessment methodologies;		Key risk indicators	x		x		x		x		x	
				(h) Defining the way performance and effectiveness is evaluated in the management of risk;		Decision matrix	x		x		x		x		x	
				(i) Identifying and specifying the decisions that have to be made; and		Research to clarify context	x		x		x		x		x	
				(j) Identifying, scoping or framing studies needed, their extent and objectives, and the resources required for such studies.												
				Define the risk criteria (When defining risk criteria, factors to be considered should include the following:	To create standardised risk assessment criteria for the organisation as a whole. To give risk owners and other risk stakeholders insight into risk management in their terms.	Risk management file / manual that includes:										
				(a) The nature and types of causes and consequences that can occur and how they will be measured;		Examples of causes and consequences	x		x		x		x		x	
				(b) How likelihood will be defined;		Risk assessment tools and techniques	x		x		x		x		x	
				(c) The timeframe(s) of the likelihood and/or consequence(s);		Risk management plan	x		x		x		x		x	
				(d) How the level of risk is to be determined;		Risk appetite guidelines	x		x		x		x		x	
				(e) The views of stakeholders;		Risk tolerance levels guidelines	x		x		x		x		x	
				(f) The level at which risk becomes acceptable or tolerable; and												
				(g) Whether combinations of multiple risks should be taken into account and, if so, how and which combinations should be considered.												
				Task: establishing the risk management policy	To document risk management scope, objectives and roles and responsibilities.	Risk management policy	x	x	x	x	x	x	x	x	x	x
				(a) A policy and plan for a system and process of risk management should be developed.												

Addendum J: Phase 2 - Round 2: Validate the adjusted ERM implementation model: theoretical frameworks, building blocks, best practice requirements and proposed deliverables

Theoretical frameworks		Building blocks	Best practice requirements		Proposed deliverables		IV1		IV2		IV4		IV6		IV7			
Deming cycle	Weisbord organisational design model				Purpose	Deliverables	Agree	Dis-agree	Agree	Dis-agree	Agree	Dis-agree	Agree	Dis-agree	Agree	Dis-agree		
Plan	Purpose, Relationships, Structure, External environment	III. Design the rules of the game.	Level 1	(c) The board's responsibility for risk governance should manifest in a documented risk management policy and plan.	To document risk management scope, objectives and roles and responsibilities.	Risk management policy												
				(d) The board should approve the risk management policy and plan.														
				The risk management policy should be widely distributed throughout the company.														
				Task: develop an accountability matrix / risk governance framework	To establish clear roles and responsibilities for risk activities across businesses and risk types.	Risk governance framework: (incl. risk owners' matrix, roles & responsibilities, reporting & escalation process & incentives guidelines & individual performance scorecards)												
				(a) Identifying risk owners that have the accountability and authority to manage risks;														
				(b) Identifying who is accountable for the development, implementation and maintenance of the framework for managing risk;														
				(c) Identifying other responsibilities of people at all levels in the organisation for the risk management process;														
				(d) Establishing performance measurement and external and/or internal reporting and escalation processes; and														
				(e) Ensuring appropriate levels of recognition.														
				Task: integration into organisational processes														
				Develop a common risk language														
				Risk management should be embedded in all the organisation's practices and processes in a way that it is relevant, effective and efficient.	To embed risk management in all the organisation's practices and processes in a way that it is relevant, effective and efficient.													
						Common risk language	x		x		x		x		x		x	
						Risk owners	x		x		x		x		x		x	
						Strategic plan	x		x		x		x		x		x	
						Business plan	x		x		x		x		x		x	
						Financial plan	x		x		x		x		x		x	
						Risk & incident escalation process	x		x		x		x		x		x	
						New products development	x		x		x		x		x		x	
						Operational processes	x		x		x		x		x		x	
						Investment decisions	x		x		x		x		x		x	
						Combined assurance	x		x		x		x		x		x	
						Performance management process	x		x		x		x		x		x	
				Change management process	x		x		x		x		x		x			
				Quality assurance process	x		x		x		x		x		x			
				Align risk management objectives with the objectives and strategies of the organisation.	To encourage a risk mind-set for decision making.	Risk appetite guidelines	x		x		x		x		x		x	
						Risk tolerance levels guidelines	x		x		x		x		x		x	
						Strategic plans	x		x		x		x		x		x	
						Business plans	x		x		x		x		x		x	
				Determine risk management performance indicators that align with performance indicators of the organisation.	To measure risk management performance against indicators, which are periodically reviewed for appropriateness;	Performance reporting metrics, i.e. key risk indicators	x		x		x		x		x		x	
				Task: Establishing internal communication and reporting mechanisms	To create one set of rules for risk communication and also to increase risk transparency.	Internal reporting guidelines	x		x		x		x		x		x	
				Communication guidelines		x		x		x		x		x		x		
(a) Key components of the risk management framework, and any subsequent modifications, are communicated appropriately;																		
(b) there is adequate internal reporting on the framework, its effectiveness and the outcomes;																		
(c) relevant information derived from the application of risk management is available at appropriate levels and times; and																		
(d) there are processes for consultation with internal stakeholders.																		

Addendum J: Phase 2 - Round 2: Validate the adjusted ERM implementation model: theoretical frameworks, building blocks, best practice requirements and proposed deliverables

Theoretical frameworks		Building blocks	Best practice requirements		Proposed deliverables		IV1		IV2		IV4		IV6		IV7	
Deming cycle	Weisbord organisational design model		Level 1	Level 2	Purpose	Deliverables	Agree	Dis-agree	Agree	Dis-agree	Agree	Dis-agree	Agree	Dis-agree	Agree	Dis-agree
Plan	Purpose, Relationships, Structure, External environment	III. Design the rules of the game.	Design the risk management framework.	Task: Establishing external communication and reporting mechanisms	To create one set of rules for risk communication and also to increase risk transparency.											
				(a) Engaging appropriate external stakeholders and ensuring an effective exchange of information;		External reporting guidelines	x		x		x		x		x	
				(b) External reporting to comply with legal, regulatory, and governance requirements;		Communication guidelines	x		x		x		x		x	
				(c) Providing feedback and reporting on communication and consultation;												
			Design the risk management process.	Step 1: Communication and consultation	To develop a standardised risk management process for the organisation.	Risk management process guidelines	x		x		x		x		x	
				Step 2: Establish the context												
				Step 3: Risk identification												
				Step 4: Risk analysis												
				Step 5: Risk evaluation												
				Step 6: Risk treatment												
				Step 7: Monitor and review												
				Step 8: Continuous improvement												
			Task: Allocate appropriate resources for risk management													
			People (skills, experience, competence & training programs).	People: skills, experience, competence & training programs	To establish decision making structures, escalation protocol & identify risk stakeholders.	Risk governance models	x		x		x		x		x	
						Performance management scorecards	x		x		x		x		x	
					To identify competencies, skills levels and experience required by risk stakeholders.	Job profiles	x		x		x		x		x	
						Risk training: induction sessions and risk awareness sessions	x		x		x		x		x	
			Committees: the board should delegate certain functions to well-structured committees but without abdicating its own responsibilities.	Board committees:	To formalise decision making structures, escalation protocol & identify risk stakeholders.											
				Formal terms of reference should be established and approved for each committee of the board.		Board committees charter / terms of reference	x		x		x		x		x	
				The committees' terms of reference should be reviewed yearly.												
				The committees should be appropriately constituted and the composition and the terms of reference should be disclosed in the integrated report.		Integrated report	x		x		x		x		x	
				The risk committee should:		Risk committees:										
				consider the risk management policy and plan and monitor the risk management process;		Board risk committee terms of reference	x		x		x		x		x	
				have as its members executive and non-executive directors, members of senior management and independent risk management experts to be invited, if necessary;		Executive risk committee terms of reference	x		x		x		x		x	
				have a minimum of three members; and		Departmental risk committee terms of reference	x		x		x		x		x	
				convene at least twice per year.		Audit and risk committee	x		x		x		x		x	
				The audit committee should:		Audit committee charter	x	x	x	x	x	x	x	x	x	x
				oversee integrated reporting.												
				have regard to all factors and risks that may impact on the integrity of the integrated report.												
				review and comment on the financial statements included in the integrated report.												
				review the disclosure of sustainability issues in the integrated report to ensure that it is reliable and does not conflict with the financial information.												
				recommend to the board to engage an external assurance provider on material sustainability issues.												
				consider the need to issue interim results.												

Addendum J: Phase 2 - Round 2: Validate the adjusted ERM implementation model: theoretical frameworks, building blocks, best practice requirements and proposed deliverables

Theoretical frameworks		Building blocks	Best practice requirements		Proposed deliverables		IV1		IV2		IV4		IV6		IV7	
Deming cycle	Weisbord organisational design model		Level 1	Level 2	Purpose	Deliverables	Agree	Dis-agree	Agree	Dis-agree	Agree	Dis-agree	Agree	Dis-agree	Agree	Dis-agree
Plan	Helping mechanisms, Relationships, Rewards	IV. Develop the risk infrastructure.	Committees: the board should delegate certain functions to well-structured committees but without abdication of its own responsibilities.	review the content of the summarised information.	To formalise decision making structures, escalation protocol & identify risk stakeholders.	Audit committee charter										
				engage the external auditors to provide assurance on the summarised financial information.												
				ensure that a combined assurance model is applied to provide a coordinated approach to all assurance activities.												
				ensure that the combined assurance is received is appropriate to address all the significant risks facing the company.												
				monitor the relationship between the external assurance providers and the company.												
				The audit committee should be an integral component of the risk management process.												
				The charter of the audit committee should set out its responsibilities regarding risk management.												
				The audit committee should specifically have oversight of:												
				financial reporting risks;												
				internal financial controls;												
				fraud risks as it relates to financial reporting; and												
				IT risks as it relates to financial reporting.												
				The audit committee should also:		Combined assurance committee terms of reference										
				ensure that a combined assurance model is applied to provide a coordinated approach to all assurance activities			x		x		x		x		x	
				ensure that the combined assurance is received is appropriate to address all the significant risks facing the company.												
			Models & tools: the organisation's processes, methods and tools to be used for managing risk		To assess and decide on standardised tools that should be used across the organisation.	Risk specific committee terms of reference e.g. Fraud risk committee	x		x		x		x		x	
						Risk identification tools	x		x		x		x		x	
						Risk analysis tools	x		x		x		x		x	
						Risk evaluation tools	x		x		x		x		x	
						Risk response tools	x		x		x		x		x	
						Risk monitoring tools	x		x		x		x		x	
			Templates: standardised recording, reporting and assessment templates		To standardise policy, framework, recording, reporting and assessment templates.	Risk reporting tools	x		x		x		x		x	
						Risk quantification models	x		x		x		x		x	
						Examples:										
						Risk management plan	x		x		x		x		x	
						Risk communication plan	x		x		x		x		x	
						Stakeholder maps	x		x		x		x		x	
						Stakeholder register	x		x		x		x		x	
						Risk register	x		x		x		x		x	
						Risk improvement report	x		x		x		x		x	
						Integrated assurance dashboard	x		x		x		x		x	
						Integrated report	x		x		x		x		x	
						Risk self-assessments	x		x		x		x		x	
						Stewardship report	x		x		x		x		x	
						Recording process	x		x		x		x		x	
						Risk acceptance form	x		x		x		x		x	
						Risk retirement form	x		x		x		x		x	
						Reporting dashboards	x		x		x		x		x	
						Reporting scorecards	x		x		x		x		x	
						Risk policy	x		x		x		x		x	
						Risk management framework	x		x		x		x		x	
						Risk committee terms of reference	x		x		x		x		x	

Addendum J: Phase 2 - Round 2: Validate the adjusted ERM implementation model: theoretical frameworks, building blocks, best practice requirements and proposed deliverables

Theoretical frameworks		Building blocks	Best practice requirements		Proposed deliverables		IV1		IV2		IV4		IV6		IV7				
Deming cycle	Weisbord organisational design model								Agree	Dis-agree			Agree	Dis-agree			Agree	Dis-agree	
			Level 1	Level 2	Purpose	Deliverables	Agree	Dis-agree	Agree	Dis-agree	Agree	Dis-agree	Agree	Dis-agree	Agree	Dis-agree			
			Processes: documented processes and procedures.		To embed risk management in all the organisation's practices and processes in a way that it is relevant, effective and efficient.	Common risk language	x		x		x		x		x				
						Risk owners matrix	x		x		x		x		x				
						Strategic planning process	x		x		x		x		x				
						Business planing process	x		x		x		x		x				
						Financial planning process	x		x		x		x		x				
						Change management process	x		x		x		x		x				
						Quality assurance process	x		x		x		x		x				
						Risk management process	x		x		x		x		x				
						Risk & incident escalation process	x		x		x		x		x				
						External audit process	x		x		x		x		x				
						Performance management process	x		x		x		x		x				
			Systems: information and knowledge management systems		To select the most appropriate risk management systems.	Risk recording	x		x		x		x		x				
						Risk reporting	x		x		x		x		x				
						Risk monitoring	x		x		x		x		x				
						Risk review	x		x		x		x		x				
			Do	Leadership, Structure, Relationships, Helping Mechanisms, External environment	V. Implement the ERM program.	Implementing the framework for managing risk.	Define the appropriate timing and strategy for implementing the framework;	To establish a time line for risk management activities.	Risk management plan (calendar)	x		x		x		x		x	
									Critical path analysis for key dependencies	x		x		x		x		x	
							Apply the risk management policy and process to the organisational processes;	To embed risk management in all the organisation's practices and processes in a way that it is relevant, effective and efficient.	Common risk language	x		x		x		x		x	
									Risk owners matrix	x		x		x		x		x	
Strategic planning process	x								x		x		x		x				
Business planing process	x								x		x		x		x				
Financial planning process	x								x		x		x		x				
Change management process	x								x		x		x		x				
Quality assurance process	x								x		x		x		x				
Risk management process	x								x		x		x		x				
Risk & incident escalation process	x								x		x		x		x				
Performance management process	x								x		x		x		x				
Comply with legal and regulatory requirements;	To communicate risk related compliance requirements.	Legal, regulatory & best practice compliance register (pertaining to risk)					x		x		x		x		x				
Ensure that decision making, including the development and setting of objectives, is aligned with the outcomes of risk management processes;	To encourage a risk mind-set for decision making.	Risk appetite statements					x		x		x		x		x				
		Risk tolerance levels					x		x		x		x		x				
		Strategic plan					x		x		x		x		x				
Hold information and training sessions; and	To create a common risk language, improve risk awareness and encourage risk based decision making.	ERM framework & policy					x		x		x		x		x				
		Risk awareness gap analysis				x		x		x		x		x					
	To ensure that the risk management framework remains appropriate.	Risk maturity assessment				x		x		x		x		x					
		Risk awareness strategy & -plan				x		x		x		x		x					
		Risk facilitation sessions				x		x		x		x		x					
Implementing the risk management process.	Step 1: Communication and consultation with external and internal stakeholders should take place during all stages of the risk management process.	To identify the internal and external stakeholders for the organisation / division / department / project.				Stakeholder analysis	x		x		x		x		x				
						To identify the most appropriate communication tools and establish timelines.	Risk communication plan	x		x		x		x		x			
		To ensure that the right information reaches the right people at the right time.				Risk reports e.g. stress tests, risk & control self-assessments, incident reports, risk treatment plans, key risk indicator reports.	x		x		x		x		x				
	Step 2: Establish the context (Know your organisation / division / department / project / risk type)	To describe the UNIQUE context for the risk management project.																	
						Establish the external context	External environment mind map	x		x		x		x		x			
	External stakeholder register						x		x		x		x		x				
	External stakeholder map						x		x		x		x		x				
	Establish the internal context					Internal value chain mind map	x		x		x		x		x				
						Internal stakeholder register	x		x		x		x		x				
						Internal stakeholder map	x		x		x		x		x				
Establishing the context of the risk management process	Standardised risk management context (refer to building block III)					x		x		x		x		x					
	Standardised risk criteria (refer to building block III)					x		x		x		x		x					
Step 3: Risk identification	Process of finding, recognising and describing risks.	Key / Principle / Strategic risk register				x		x		x		x		x					
		Divisional / departmental / business unit risk register				x		x		x		x		x					
		Emerging risk register				x		x		x		x		x					
		Risk library				x		x		x		x		x					

Addendum J: Phase 2 - Round 2: Validate the adjusted ERM implementation model: theoretical frameworks, building blocks, best practice requirements and proposed deliverables

Theoretical frameworks		Building blocks	Best practice requirements		Proposed deliverables		IV1		IV2		IV4		IV6		IV7	
Deming cycle	Weisbord organisational design model				Purpose	Deliverables	Agree	Dis-agree	Agree	Dis-agree	Agree	Dis-agree	Agree	Dis-agree	Agree	Dis-agree
				Step 4: Risk analysis	Process to comprehend the nature of risk and to determine the level of risk (e.g. high, medium, low).											
						Key / Principle / Strategic risk register - risk ratings applied	x		x		x		x		x	
						Divisional / departmental / business unit risk register - risk ratings applied	x		x		x		x		x	
				Step 5: Risk evaluation	Process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable.	Root cause analysis	x		x		x		x		x	
						Key / Principle / Strategic risk profile - risk ratings + current controls applied & risk owners identified	x		x		x		x		x	
						Divisional / departmental / business unit risk register risk ratings + current controls applied & risk owners identified	x		x		x		x		x	
				Step 6: Risk response	To identify the most appropriate risk treatment for the most significant risks.	Controls library	x		x		x		x		x	
						Risk response plans / Action plans	x		x		x		x		x	
						Risk response options	x		x		x		x		x	
Check	Rewards	VI. Monitor and review the ERM program.	Monitoring activities by the Board	The board should ensure continual risk monitoring by management	To ensure proper risk oversight.	Risk governance framework	x		x		x		x		x	
				The board should ensure that effective and continual monitoring of risk management takes place.	To reduce role confusion and provide clear guidelines for risk monitoring.	Risk management plan (monitoring roles and responsibilities)	x		x		x		x		x	
				The responsibility for monitoring should be defined in the risk management plan.	To periodically measure progress against, and deviation from, the risk management plan.	Status report on risk management plan implementation	x		x		x		x		x	
			Review activities by the Board	The board should comment in the integrated report on the effectiveness of the system and process of risk management.	To periodically review whether the risk management framework, policy and plan are still appropriate, given the organisations' external and internal context;	Integrated report (risk and opportunities section)	x		x		x		x		x	
				The board should ensure that effective and continual monitoring of risk management takes place.	To periodically measure progress against, and deviation from, the risk management plan.	Annual board risk report	x		x		x		x		x	
				The board should review the implementation of the risk management plan at least once a year.	To periodically measure progress against, and deviation from, the risk management plan.	Risk management plan implementation status report	x		x		x		x		x	
				The performance of the committee should be evaluated once a year by the board.	To ensure effectiveness and efficiency with regards to committee activities.	Risk improvement report	x		x		x		x		x	
					To ensure compliance with the risk appetite framework.	Internal audit report	x		x		x		x		x	
			Monitor the risk management framework	The board should monitor that risks taken are within the tolerance and appetite levels.	To ensure effectiveness and efficiency with regards to committee activities.	Board risk committee performance evaluation	x		x		x		x		x	
				Measure risk management performance against indicators, which are periodically reviewed for appropriateness;	To ensure compliance with the risk tolerance levels.	Risk appetite status report	x		x		x		x		x	
				Periodically measure progress against, and deviation from, the risk management plan;	To measure risk management performance against indicators, which are periodically reviewed for appropriateness;	Risk tolerance status report	x		x		x		x		x	
				Report on risk, progress with the risk management plan and how well the risk management policy is being followed;	To periodically measure progress against, and deviation from, the risk management plan.	KRI performance report	x		x		x		x		x	
				Monitor the level of risk awareness	To report on risk, progress with the risk management plan and how well the risk management policy is being followed.	Risk management plan implementation status report	x		x		x		x		x	
					To track the improvement of risk awareness.	Risk management policy compliance report	x		x		x		x		x	
						Deviations from risk management policy report	x		x		x		x		x	
			Review the risk management framework	Periodically review whether the risk management framework, policy and plan are still appropriate, given the organizations' external and internal context;		Risk culture surveys	x		x		x		x		x	
						Risk improvement report	x		x		x		x		x	
						Internal audit report	x		x		x		x		x	
						Risk calendar	x		x		x		x		x	
						Risk improvement report	x		x		x		x		x	
				Communicate and consult with stakeholders to ensure that its risk management framework remains appropriate.	To periodically review whether the risk management framework, policy and plan are still appropriate, given the organisations' external and internal context.	Subject matter expert gap analysis	x		x		x		x		x	
						Internal audit reports	x		x		x		x		x	
						Risk calendar	x		x		x		x		x	
				Review the effectiveness of the risk management framework.		ISO 9000 reports	x		x		x		x		x	
						Internal audit reports, risk committee effectiveness, qualitative conversations, risk appetite and risk tolerance level breaches, signed letters of representation.	x		x		x		x		x	

Addendum J: Phase 2 - Round 2: Validate the adjusted ERM implementation model: theoretical frameworks, building blocks, best practice requirements and proposed deliverables

Theoretical frameworks		Building blocks	Best practice requirements		Proposed deliverables		IV1		IV2		IV4		IV6		IV7	
Deming cycle	Weisbord organisational design model		Level 1	Level 2	Purpose	Deliverables	Agree	Dis-agree	Agree	Dis-agree	Agree	Dis-agree	Agree	Dis-agree	Agree	Dis-agree
			Monitor the risk management process	Ensuring that controls are effective and efficient in both design and operation.	To ensure that controls are effective and efficient in both design and operation.	Subject matter expert gap analysis	x		x		x		x		x	
						Combined assurance reports	x		x		x		x		x	
						Risk profile status reports	x		x		x		x		x	
						Internal audit reports	x		x		x		x		x	
						External audit reports	x		x		x		x		x	
			Review the risk management process	Identifying emerging risks.	To identify emerging risks in the organisation's internal value chain and external environment.	Emerging risk register	x		x		x		x		x	
						Variance and trend analysis	x		x		x		x		x	
						Post mortem sessions	x		x		x		x		x	
						Environmental scanning	x		x		x		x		x	
						Risk reconciliation reports	x		x		x		x		x	
Adjust	Leadership, Purposes, Structure, Relationships, Rewards, Helpful mechanisms, External environment	VII. Continual improvement of the ERM program.	Management should provide assurance to the board that the risk management plan is integrated in the daily activities of the company.		To inform the relevant committees and risk stakeholders of the level of assurance provided by assurance providers.	Combined assurance report.	x		x		x		x		x	
						Risk reports to various committees	x		x		x		x		x	
						Risk maturity assessment	x		x		x		x		x	
						Benchmarking assessments (peer reviews & best practice)	x		x		x		x		x	
			Internal audit should: provide a written assessment of the effectiveness of the system of internal controls and risk management to the board.			Risk improvement report	x		x		x		x		x	
						Internal audit report	x		x		x		x		x	
			detect changes in the external and internal context, including changes to risk criteria and the risk itself which can require revision of risk treatments and priorities; and	Detecting changes in the external and internal context, including changes to risk criteria and the risk itself which can require revision of risk treatments and priorities; and	To periodically review whether the risk management framework, policy and plan are still appropriate, given the organisations' external and internal context;	Risk improvement report (List of internal, external, risk management process & risk criteria context changes)	x		x		x		x		x	
						Risk improvement report (risk assessment process & methodology)	x		x		x		x		x	
			obtaining further information to improve risk assessment.	Obtaining further information to improve risk assessment.												

Source: Researcher's own compilation

Addendum J: Phase 2 - Round 2: Validate the adjusted ERM implementation model: theoretical frameworks, building blocks, b proposed deliverables

Theoretical frameworks		Building blocks	Best practice requirements		Proposed c	IV8		IV9		IV13		IV17		IV18		IV19	
Deming cycle	Weisbord organisational design model		Level 1	Level 2	Purpose	Agree	Dis-agree	Agree	Dis-agree	Agree	Dis-agree	Agree	Dis-agree	Agree	Dis-agree	Agree	Dis-agree
Plan	Purpose, Leadership	I. Formalise the instruction and get permission.	Instruction / Trigger	Business trigger e.g. event, merger & acquisition due diligence requirement, peer pressure, etc.	To motivate the need for an ERM program.	x		x		x		x		x		x	
				Ensure legal and regulatory compliance.	To motivate the need for an ERM program.	x		x		x		x		x		x	
			Permission / Mandate	The board should delegate to management the responsibility to design, implement and monitor the risk management plan.	To ask for permission / mandate to design and implement the ERM program.	x		x		x		x		x		x	
					To record the permission / mandate received to design and implement an ERM program.	x		x		x		x		x		x	
			Oversight: the risk committee or audit committee should assist the board in carrying out its risk responsibilities	The board should appoint a committee responsible for risk.	To assist the board in carrying out its risk roles and responsibilities.												
				The risk committee should:													
				consider the risk management policy and plan and monitor the risk management process;													
				have as its members executive and non-executive directors, members of senior management and independent risk management experts to be invited, if necessary;		x		x		x		x		x		x	
				have a minimum of three members; and													
				convene at least twice per year.													
				The board's responsibility for risk governance should be expressed in the board charter.													
			Define and endorse the risk management policy	The board's responsibility for risk governance should manifest in a documented risk management policy and plan.	To document risk management scope, objectives and roles and responsibilities.	x		x		x		x		x		x	
				The board should approve the risk management policy and plan.													
				The risk management policy should be widely distributed throughout the company.													

Addendum J: Phase 2 - Round 2: Validate the adjusted ERM implementation model: theoretical frameworks, building blocks, b proposed deliverables

Theoretical frameworks		Building blocks	Best practice requirements		Proposed c	IV8		IV9		IV13		IV17		IV18		IV19			
Deming cycle	Weisbord organisational design model					Agree	Dis-agree	Agree	Dis-agree	Agree	Dis-agree	Agree	Dis-agree	Agree	Dis-agree	Agree	Dis-agree		
			Level 1	Level 2	Purpose	Agree	Dis-agree	Agree	Dis-agree	Agree	Dis-agree	Agree	Dis-agree	Agree	Dis-agree	Agree	Dis-agree		
Plan	Leadership, Relationships	II. Establish the tone of the organisation.	Establishing the tone of the organisation: The introduction of risk management and ensuring its ongoing effectiveness require strong and sustained commitment by management of the organisation, as well as strategic and rigorous planning to achieve commitment at all levels.		A senior level ERM program sponsor / Chief Risk Officer should have clear authority over and accountability for oversight of risk across the enterprise	x		x		x		x		x		x			
				(a) Ensure that the organisation's culture and risk management policy are aligned.	To create risk awareness at all levels of the organisations and to encourage risk based decision making.	x		x		x		x		x		x			
				(b) Determine risk management performance indicators that align with performance indicators of the organisation.	To measure risk management performance against indicators, which are periodically reviewed for appropriateness;	x		x		x		x		x		x			
				(c) Align risk management objectives with the objectives and strategies of the organisation.	To encourage a risk mind-set for decision making.	x		x		x		x		x		x			
				(d) Assign accountabilities and responsibilities at appropriate levels within the organisation.	To reduce role confusion by establishing clear roles and responsibilities for risk activities across businesses and risk types.	x		x		x		x		x		x			
				(e) Ensure that the necessary resources are allocated to risk management.	To ensure the effective and efficient implementation of the ERM program.	x		x		x		x		x		x			
				(f) Communicate the benefits of risk management to all stakeholders.	To raise risk awareness and create excitement for the project.	x		x		x		x		x		x			
			The induction and ongoing training programs of the board should incorporate risk governance. (Note: apply to all the levels in the organisation)		To create a common risk language, improve risk awareness and encourage risk based decision making.	x		x		x		x		x		x		x	
						x		x		x		x		x		x		x	
						x		x		x		x		x		x		x	
Plan	Purpose, Relationships, Structure, External environment	III. Design the rules of the game.	Design the risk management framework.	Task: Understanding the organisation and its context (Know your organisation)															
				Establish the external context:															
				(a) the social and cultural, political, legal, regulatory, financial, technological, economic, natural and competitive environment, whether international, national, regional or local;		To get an overall picture of the external environment based PESTLE and / or Porter's 5 forces.	x		x		x		x		x		x		
				(b) key drivers and trends having impact on the objectives of the organisation; and			x		x		x		x		x				
				(c) External stakeholder analysis			x		x		x		x		x				
				Establish the internal context:															
				(a) Governance, organisational structure, roles and accountabilities;		To describe the internal value chain of the organisation and to identify areas that would create risks and opportunities	x		x		x		x		x		x		
							x		x		x		x		x		x		
							x		x		x		x		x		x		
							x		x		x		x		x		x		
							x		x		x		x		x		x		
							x		x		x		x		x		x		
							x		x		x		x		x		x		
							x		x		x		x		x		x		
				(b) Policies, objectives, and the strategies that are in place to achieve them;			x		x		x		x		x		x		
							x		x		x		x		x		x		
							x		x		x		x		x		x		
							x		x		x		x		x		x		
				(c) Capabilities, understood in terms of resources and knowledge (e.g. capital, time, people, processes, systems and technologies);			x		x		x		x		x		x		
							x		x		x		x		x		x		
							x		x		x		x		x		x		
							x		x		x		x		x		x		

Addendum J: Phase 2 - Round 2: Validate the adjusted ERM implementation model: theoretical frameworks, building blocks, b proposed deliverables

Theoretical frameworks		Building blocks	Best practice requirements		Proposed c	IV8		IV9		IV13		IV17		IV18		IV19	
Deming cycle	Weisbord organisational design model		Level 1	Level 2		Agree	Dis-agree	Agree	Dis-agree	Agree	Dis-agree	Agree	Dis-agree	Agree	Dis-agree	Agree	Dis-agree
Plan	Purpose, Relationships, Structure, External environment	III. Design the rules of the game.		(d) Information systems, information flows and decision making processes (both formal and informal)	To describe the internal value chain of the organisation and to identify areas that would create risks and opportunities	x		x		x		x		x		x	
						x		x		x		x		x		x	
						x		x		x		x		x		x	
				Connected stakeholder analysis		x		x		x		x		x		x	
				(e) Internal stakeholder analysis		x		x		x		x		x		x	
				(f) Temperature checks on organisational culture		x		x		x		x		x		x	
				(g) Standards, guidelines and models adopted by the organisation; and		x		x		x		x		x		x	
				(h) the form and extent of contractual relationships.		x		x		x		x		x		x	
						x		x		x		x		x		x	
						x		x		x		x		x		x	
						x		x		x		x		x		x	
						x		x		x		x		x		x	
				Establish the context of the risk management process (The context of the risk management process will vary according to the needs of an organisation. It can involve, but is not limited to:	To create ONE set of risk management rules for the organisation.												
				(a) Defining the goals and objectives of the risk management activities;		x		x		x		x		x		x	
				(b) Defining responsibilities for and within the risk management process;		x		x		x		x		x		x	
				(c) Defining the scope, as well as the depth and breadth of the risk management activities to be carried out, including specific		x		x		x		x		x		x	
				(e) Defining the activity, process, function, project, product, service or asset in terms of time and location;													
				(f) Defining the relationships between a particular project, process or activity and other projects, processes or activities of the organisation;		x		x		x		x		x		x	
				(g) Defining the risk assessment methodologies;		x		x		x		x		x		x	
				(h) Defining the way performance and effectiveness is evaluated in the management of risk;		x		x		x		x		x		x	
				(i) Identifying and specifying the decisions that have to be made; and		x		x		x		x		x		x	
				(j) Identifying, scoping or framing studies needed, their extent and objectives, and the resources required for such studies.		x		x		x		x		x		x	
				Define the risk criteria (When defining risk criteria, factors to be considered should include the following:	To create standardised risk assessment criteria for the organisation as a whole. To give risk owners and other risk stakeholders insight into risk management in their terms.												
				(a) The nature and types of causes and consequences that can occur and how they will be measured;		x		x		x		x		x		x	
				(b) How likelihood will be defined;		x		x		x		x		x		x	
				(c) The timeframe(s) of the likelihood and/or consequence(s);		x		x		x		x		x		x	
				(d) How the level of risk is to be determined;		x		x		x		x		x		x	
				(e) The views of stakeholders;		x		x		x		x		x		x	
				(f) The level at which risk becomes acceptable or tolerable; and													
				(g) Whether combinations of multiple risks should be taken into account and, if so, how and which combinations should be considered.													
				Task: establishing the risk management policy	To document risk management scope, objectives and roles and responsibilities.	x	x	x	x	x	x	x	x	x	x	x	x
				(a) A policy and plan for a system and process of risk management should be developed.													

Addendum J: Phase 2 - Round 2: Validate the adjusted ERM implementation model: theoretical frameworks, building blocks, b proposed deliverables

Theoretical frameworks		Building blocks	Best practice requirements		Proposed c	IV8		IV9		IV13		IV17		IV18		IV19																																																																	
Deming cycle	Weisbord organisational design model					Agree	Dis-agree	Agree	Dis-agree	Agree	Dis-agree	Agree	Dis-agree	Agree	Dis-agree	Agree	Dis-agree																																																																
Plan	Purpose, Relationships, Structure, External environment	III. Design the rules of the game.	Level 1	Level 2	Purpose	Agree	Dis-agree	Agree	Dis-agree	Agree	Dis-agree	Agree	Dis-agree	Agree	Dis-agree	Agree	Dis-agree																																																																
																		(c) The board's responsibility for risk governance should manifest in a documented risk management policy and plan. (d) The board should approve the risk management policy and plan. The risk management policy should be widely distributed throughout the company.	To document risk management scope, objectives and roles and responsibilities.	Agree	Dis-agree	Agree	Dis-agree	Agree	Dis-agree	Agree	Dis-agree	Agree	Dis-agree	Agree	Dis-agree																																																		
																																Task: develop an accountability matrix / risk governance framework (a) Identifying risk owners that have the accountability and authority to manage risks; (b) Identifying who is accountable for the development, implementation and maintenance of the framework for managing risk; (c) Identifying other responsibilities of people at all levels in the organisation for the risk management process; (d) Establishing performance measurement and external and/or internal reporting and escalation processes; and (e) Ensuring appropriate levels of recognition. Task: integration into organisational processes Develop a common risk language	To establish clear roles and responsibilities for risk activities across businesses and risk types.	Agree	Dis-agree	Agree	Dis-agree	Agree	Dis-agree	Agree	Dis-agree	Agree	Dis-agree																																						
																																												Risk management should be embedded in all the organisation's practices and processes in a way that it is relevant, effective and efficient.	To embed risk management in all the organisation's practices and processes in a way that it is relevant, effective and efficient.	Agree	Dis-agree	Agree	Dis-agree	Agree	Dis-agree	Agree	Dis-agree	Agree	Dis-agree																										
																		Align risk management objectives with the objectives and strategies of the organisation.	To encourage a risk mind-set for decision making.																																					Agree	Dis-agree	Agree	Dis-agree	Agree	Dis-agree	Agree	Dis-agree																		
																																																																Determine risk management performance indicators that align with performance indicators of the organisation. Task: Establishing internal communication and reporting mechanisms (a) Key components of the risk management framework, and any subsequent modifications, are communicated appropriately; (b) there is adequate internal reporting on the framework, its effectiveness and the outcomes; (c) relevant information derived from the application of risk management is available at appropriate levels and times; and (d) there are processes for consultation with internal stakeholders.	To measure risk management performance against indicators, which are periodically reviewed for appropriateness;	Agree	Dis-agree	Agree	Dis-agree	Agree	Dis-agree	Agree	Dis-agree								
																																																																										To create one set of rules for risk communication and also to increase risk transparency.		Agree	Dis-agree	Agree	Dis-agree	Agree	Dis-agree

Addendum J: Phase 2 - Round 2: Validate the adjusted ERM implementation model: theoretical frameworks, building blocks, b proposed deliverables

Theoretical frameworks		Building blocks	Best practice requirements		Proposed c	IV8		IV9		IV13		IV17		IV18		IV19	
Deming cycle	Weisbord organisational design model		Level 1	Level 2	Purpose	Agree	Dis-agree	Agree	Dis-agree	Agree	Dis-agree	Agree	Dis-agree	Agree	Dis-agree	Agree	Dis-agree
Plan	Purpose, Relationships, Structure, External environment	III. Design the rules of the game.	Design the risk management framework.	Task: Establishing external communication and reporting mechanisms	To create one set of rules for risk communication and also to increase risk transparency.												
				(a) Engaging appropriate external stakeholders and ensuring an effective exchange of information;		x		x		x		x		x		x	
				(b) External reporting to comply with legal, regulatory, and governance requirements;		x		x		x		x		x		x	
				(c) Providing feedback and reporting on communication and consultation;													
			Design the risk management process.	Step 1: Communication and consultation	To develop a standardised risk management process for the organisation.	x		x		x		x		x		x	
				Step 2: Establish the context													
				Step 3: Risk identification													
				Step 4: Risk analysis													
				Step 5: Risk evaluation													
				Step 6: Risk treatment													
				Step 7: Monitor and review													
				Step 8: Continuous improvement													
			Task: Allocate appropriate resources for risk management														
			People (skills, experience, competence & training programs).	People: skills, experience, competence & training programs	To establish decision making structures, escalation protocol & identify risk stakeholders.	x		x		x		x		x		x	
						x		x		x		x		x		x	
					To identify competencies, skills levels and experience required by risk stakeholders.	x		x		x		x		x		x	
					To ensure proper training for risk stakeholders.	x		x		x		x		x		x	
			Committees: the board should delegate certain functions to well-structured committees but without abdicating its own responsibilities.	Board committees:	To formalise decision making structures, escalation protocol & identify risk stakeholders.												
				Formal terms of reference should be established and approved for each committee of the board.		x		x		x		x		x		x	
				The committees' terms of reference should be reviewed yearly.													
				The committees should be appropriately constituted and the composition and the terms of reference should be disclosed in the integrated report.		x		x		x		x		x		x	
				The risk committee should:													
				consider the risk management policy and plan and monitor the risk management process;		x		x		x		x		x		x	
				have as its members executive and non-executive directors, members of senior management and independent risk management experts to be invited, if necessary;		x		x		x		x		x		x	
				have a minimum of three members; and		x		x		x		x		x		x	
				convene at least twice per year.		x		x		x		x		x		x	
				The audit committee should:													
				oversee integrated reporting.		x	x	x	x	x	x	x	x	x	x	x	x
				have regard to all factors and risks that may impact on the integrity of the integrated report.													
				review and comment on the financial statements included in the integrated report.													
				review the disclosure of sustainability issues in the integrated report to ensure that it is reliable and does not conflict with the financial information.													
				recommend to the board to engage an external assurance provider on material sustainability issues.													
				consider the need to issue interim results.													

Addendum J: Phase 2 - Round 2: Validate the adjusted ERM implementation model: theoretical frameworks, building blocks, b proposed deliverables

Theoretical frameworks		Building blocks	Best practice requirements		Proposed c	IV8		IV9		IV13		IV17		IV18		IV19	
Deming cycle	Weisbord organisational design model		Level 1	Level 2	Purpose	Agree	Dis-agree	Agree	Dis-agree	Agree	Dis-agree	Agree	Dis-agree	Agree	Dis-agree	Agree	Dis-agree
Plan	Helping mechanisms, Relationships, Rewards	IV. Develop the risk infrastructure.	Committees: the board should delegate certain functions to well-structured committees but without abdicating its own responsibilities.	review the content of the summarised information.	To formalise decision making structures, escalation protocol & identify risk stakeholders.												
				engage the external auditors to provide assurance on the summarised financial information.													
				ensure that a combined assurance model is applied to provide a coordinated approach to all assurance activities.													
				ensure that the combined assurance is received is appropriate to address all the significant risks facing the company.													
				monitor the relationship between the external assurance providers and the company.													
				The audit committee should be an integral component of the risk management process.													
				The charter of the audit committee should set out its responsibilities regarding risk management.													
				The audit committee should specifically have oversight of:													
				financial reporting risks;													
				internal financial controls;													
				fraud risks as it relates to financial reporting; and													
				IT risks as it relates to financial reporting.													
				The audit committee should also:													
				ensure that a combined assurance model is applied to provide a coordinated approach to all assurance activities		x		x		x		x		x		x	
				ensure that the combined assurance is received is appropriate to address all the significant risks facing the company.													
						x		x		x		x		x		x	
			Models & tools: the organisation's processes, methods and tools to be used for managing risk		To assess and decide on standardised tools that should be used across the organisation.	x		x		x		x		x		x	
						x		x		x		x		x		x	
						x		x		x		x		x		x	
						x		x		x		x		x		x	
						x		x		x		x		x		x	
						x		x		x		x		x		x	
			Templates: standardised recording, reporting and assessment templates		To standardise policy, framework, recording, reporting and assessment templates.												
						x		x		x		x		x		x	
						x		x		x		x		x		x	
						x		x		x		x		x		x	
						x		x		x		x		x		x	
						x		x		x		x		x		x	
						x		x		x		x		x		x	
						x		x		x		x		x		x	
						x		x		x		x		x		x	
						x		x		x		x		x		x	
						x		x		x		x		x		x	
						x		x		x		x		x		x	
						x		x		x		x		x		x	
						x		x		x		x		x		x	
						x		x		x		x		x		x	

Addendum J: Phase 2 - Round 2: Validate the adjusted ERM implementation model: theoretical frameworks, building blocks, b proposed deliverables

Theoretical frameworks		Building blocks	Best practice requirements		Proposed content	IV8		IV9		IV13		IV17		IV18		IV19																						
Deming cycle	Weisbord organisational design model					Agree	Dis-agree	Agree	Dis-agree	Agree	Dis-agree	Agree	Dis-agree	Agree	Dis-agree	Agree	Dis-agree																					
			Level 1	Level 2	Purpose																																	
			Processes: documented processes and procedures.		To embed risk management in all the organisation's practices and processes in a way that it is relevant, effective and efficient.	X		X		X		X		X		X																						
						X		X		X		X		X		X																						
						X		X		X		X		X		X																						
						X		X		X		X		X		X																						
						X		X		X		X		X		X																						
						X		X		X		X		X		X																						
						X		X		X		X		X		X																						
						X		X		X		X		X		X																						
						X		X		X		X		X		X																						
			Systems: information and knowledge management systems		To select the most appropriate risk management systems.	X		X		X		X		X		X		X																				
						X		X		X		X		X		X		X																				
						X		X		X		X		X		X		X																				
						X		X		X		X		X		X		X																				
						X		X		X		X		X		X		X																				
						X		X		X		X		X		X		X																				
						X		X		X		X		X		X		X																				
	Leadership, Structure, Relationships, Helping Mechanisms, External environment	V. Implement the ERM program.	Implementing the framework for managing risk.	Define the appropriate timing and strategy for implementing the framework;	To establish a time line for risk management activities.	X		X		X		X		X		X																						
				Apply the risk management policy and process to the organisational processes;	To embed risk management in all the organisation's practices and processes in a way that it is relevant, effective and efficient.	X		X		X		X		X		X		X																				
						X		X		X		X		X		X		X																				
						X		X		X		X		X		X		X																				
						X		X		X		X		X		X		X																				
						X		X		X		X		X		X		X																				
						X		X		X		X		X		X		X																				
						X		X		X		X		X		X		X																				
						X		X		X		X		X		X		X																				
						X		X		X		X		X		X		X																				
				Comply with legal and regulatory requirements;	To communicate risk related compliance requirements.	X		X		X		X		X		X		X		X																		
						Ensure that decision making, including the development and setting of objectives, is aligned with the outcomes of risk management processes;	To encourage a risk mind-set for decision making.	X		X		X		X		X		X		X																		
								X		X		X		X		X		X		X																		
								X		X		X		X		X		X		X																		
				Hold information and training sessions; and	To create a common risk language, improve risk awareness and encourage risk based decision making.	X		X		X		X		X		X		X		X																		
						X		X		X		X		X		X		X		X																		
			X				X		X		X		X		X		X		X																			
					To ensure that the risk management framework remains appropriate.	X		X		X		X		X		X		X																				
			Implementing the risk management process.	Step 1: Communication and consultation with external and internal stakeholders should take place during all stages of the risk management process.	To identify the internal and external stakeholders for the organisation / division / department / project.	X		X		X		X		X		X		X		X																		
						To identify the most appropriate communication tools and establish timelines.	X		X		X		X		X		X		X		X																	
					To ensure that the right information reaches the right people at the right time.	X		X		X		X		X		X		X		X																		
				Step 2: Establish the context (Know your organisation / division / department / project / risk type)																																		
																						Establish the external context	X		X		X		X		X		X		X		X	
																							X		X		X		X		X		X		X		X	
																							Establish the internal context	X		X		X		X		X		X		X		X
				X		X		X		X		X		X		X		X																				
				X		X		X		X		X		X		X		X		X																		
				Establishing the context of the risk management process																																		
																						Apply the risk criteria	X		X		X		X		X		X		X		X	
																							X		X		X		X		X		X		X		X	
				Step 3: Risk identification																																		
																							X		X		X		X		X		X		X		X	
X		X																						X		X		X		X		X		X				
X		X																						X		X		X		X		X		X				

Addendum J: Phase 2 - Round 2: Validate the adjusted ERM implementation model: theoretical frameworks, building blocks, b proposed deliverables

Theoretical frameworks		Building blocks	Best practice requirements		Proposed c	IV8		IV9		IV13		IV17		IV18		IV19	
Deming cycle	Weisbord organisational design model		Level 1	Level 2	Purpose	Agree	Dis-agree	Agree	Dis-agree	Agree	Dis-agree	Agree	Dis-agree	Agree	Dis-agree	Agree	Dis-agree
				Step 4: Risk analysis	Process to comprehend the nature of risk and to determine the level of risk (e.g. high, medium, low).												
						x		x		x		x		x		x	
						x		x		x		x		x		x	
				Step 5: Risk evaluation	Process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable.	x		x		x		x		x		x	
						x		x		x		x		x		x	
						x		x		x		x		x		x	
				Step 6: Risk response	To identify the most appropriate risk treatment for the most significant risks.	x		x		x		x		x		x	
						x		x		x		x		x		x	
						x		x		x		x		x		x	
Check	Rewards	VI. Monitor and review the ERM program.	Monitoring activities by the Board	The board should ensure continual risk monitoring by management	To ensure proper risk oversight.	x		x		x		x		x		x	
				The board should ensure that effective and continual monitoring of risk management takes place.	To reduce role confusion and provide clear guidelines for risk monitoring.	x		x		x		x		x		x	
				The responsibility for monitoring should be defined in the risk management plan.	To periodically measure progress against, and deviation from, the risk management plan.	x		x		x		x		x		x	
			Review activities by the Board	The board should comment in the integrated report on the effectiveness of the system and process of risk management.	To periodically review whether the risk management framework, policy and plan are still appropriate, given the organisations' external and internal context;	x		x		x		x		x		x	
						x		x		x		x		x		x	
				The board should ensure that effective and continual monitoring of risk management takes place.	To periodically measure progress against, and deviation from, the risk management plan.	x		x		x		x		x		x	
				The board should review the implementation of the risk management plan at least once a year.	To periodically review whether the risk management framework, policy and plan are still appropriate, given the organisations' external and internal context;	x		x		x		x		x		x	
						x		x		x		x		x		x	
				The performance of the committee should be evaluated once a year by the board.	To ensure effectiveness and efficiency with regards to committee activities.	x		x		x		x		x		x	
			Monitor the risk management framework	The board should monitor that risks taken are within the tolerance and appetite levels.	To ensure compliance with the risk appetite framework.	x		x		x		x		x		x	
						x		x		x		x		x		x	
				Measure risk management performance against indicators, which are periodically reviewed for appropriateness;	To measure risk management performance against indicators, which are periodically reviewed for appropriateness;	x		x		x		x		x		x	
				Periodically measure progress against, and deviation from, the risk management plan;	To periodically measure progress against, and deviation from, the risk management plan.	x		x		x		x		x		x	
				Report on risk, progress with the risk management plan and how well the risk management policy is being followed;	To report on risk, progress with the risk management plan and how well the risk management policy is being followed.	x		x		x		x		x		x	
						x		x		x		x		x		x	
				Monitor the level of risk awareness	To track the improvement of risk awareness.	x		x		x		x		x		x	
			Review the risk management framework	Periodically review whether the risk management framework, policy and plan are still appropriate, given the organizations' external and internal context;	To periodically review whether the risk management framework, policy and plan are still appropriate, given the organisations' external and internal context.	x		x		x		x		x		x	
						x		x		x		x		x		x	
						x		x		x		x		x		x	
						x		x		x		x		x		x	
						x		x		x		x		x		x	
						x		x		x		x		x		x	
						x		x		x		x		x		x	
				Review the effectiveness of the risk management framework.		x		x		x		x		x		x	

Addendum J: Phase 2 - Round 2: Validate the adjusted ERM implementation model: theoretical frameworks, building blocks, b proposed deliverables

Theoretical frameworks		Building blocks	Best practice requirements		Proposed c	IV8		IV9		IV13		IV17		IV18		IV19	
Deming cycle	Weisbord organisational design model		Level 1	Level 2	Purpose	Agree	Dis-agree	Agree	Dis-agree	Agree	Dis-agree	Agree	Dis-agree	Agree	Dis-agree	Agree	Dis-agree
			Monitor the risk management process	Ensuring that controls are effective and efficient in both design and operation.	To ensure that controls are effective and efficient in both design and operation.	x		x		x		x		x		x	
						x		x		x		x		x		x	
						x		x		x		x		x		x	
						x		x		x		x		x		x	
						x		x		x		x		x		x	
			Identifying emerging risks.	To identify emerging risks in the organisation's internal value chain and external environment.		x		x		x		x		x		x	
						x		x		x		x		x		x	
						x		x		x		x		x		x	
						x		x		x		x		x		x	
						x		x		x		x		x		x	
Adjust	Leadership, Purposes, Structure, Relationships, Rewards, Helpful mechanisms, External environment	VII. Continual improvement of the ERM program.	Management should provide assurance to the board that the risk management plan is integrated in the daily activities of the company.		To inform the relevant committees and risk stakeholders of the level of assurance provided by assurance providers.	x		x		x		x		x		x	
						x		x		x		x		x		x	
						x		x		x		x		x		x	
						x		x		x		x		x		x	
			Internal audit should: provide a written assessment of the effectiveness of the system of internal controls and risk management to the board.														
						x		x		x		x		x		x	
			detect changes in the external and internal context, including changes to risk criteria and the risk itself which can require revision of risk treatments and priorities; and	Detecting changes in the external and internal context, including changes to risk criteria and the risk itself which can require revision of risk treatments and priorities; and	To periodically review whether the risk management framework, policy and plan are still appropriate, given the organisations' external and internal context;	x		x		x		x		x		x	
						x		x		x		x		x		x	
			obtaining further information to improve risk assessment.	Obtaining further information to improve risk assessment.		x		x		x		x		x		x	
						x		x		x		x		x		x	

Source: Researcher's own compilation

Addendum K: Validated ERM implementation model: theoretical frameworks, building blocks, best practice requirements and proposed deliverables

Theoretical frameworks		Building blocks	Best practice requirements		Proposed deliverables	
Deming cycle	Weisbord organisational design model		Level 1	Level 2	Purpose	Deliverables
Plan	Purpose, Leadership	I. Formalise the instruction and get permission.	Instruction / Trigger	Business trigger e.g. event, merger & acquisition due diligence requirement, peer pressure, etc.	To motivate the need for an ERM program.	Business case document
				Ensure legal and regulatory compliance.	To motivate the need for an ERM program.	Compliance register (legal + regulatory + best practise frameworks)
			Permission / Mandate	The board should delegate to management the responsibility to design, implement and monitor the risk management plan.	To ask for permission / mandate to design and implement the ERM program.	Agenda item for the decision making forum e.g. Board meeting, Executive committee meeting.
					To record the permission / mandate received to design and implement an ERM program.	Minutes of the decision making forum e.g. Board meeting, Executive committee meeting.
			Oversight: the risk committee or audit committee should assist the board in carrying out its risk responsibilities	The board should appoint a committee responsible for risk.	To assist the board in carrying out its risk roles and responsibilities.	Board risk committee (BRC) terms of reference / Audit committee charter / Audit and risk committee charter
				The risk committee should:		
				consider the risk management policy and plan and monitor the risk management process;		
				have as its members executive and non-executive directors, members of senior management and independent risk management experts to be invited, if necessary;		
				have a minimum of three members; and		
				convene at least twice per year.		
				The board's responsibility for risk governance should be expressed in the board charter.		
			Define and endorse the risk management policy	The board's responsibility for risk governance should manifest in a documented risk management policy and plan.	To document risk management scope, objectives and roles and responsibilities.	Risk management policy
				The board should approve the risk management policy and plan.		
				The risk management policy should be widely distributed throughout the company.		
Plan	Leadership, Relationships	II. Establish the tone of the organisation.	Establishing the tone of the organisation: The introduction of risk management and ensuring its ongoing effectiveness require strong and sustained commitment by management of the organisation, as well as strategic and rigorous planning to achieve commitment at all levels.	The CRO should be a suitably experienced person who should have access and interact regularly on strategic matters with the board and/or appropriate board committee and executive management.	A senior level ERM program sponsor / Chief Risk Officer should have clear authority over and accountability for oversight of risk across the enterprise	CRO / Senior level project sponsor
				(a) Ensure that the organisation's culture and risk management policy are aligned.	To create risk awareness at all levels of the organisations and to encourage risk based decision making.	Risk management policy / Risk requirements evident in business, project and HR requirements and standards / Strategic intent document / Risk communication strategy / Internal audit reports / External audit report / Insurance claims
				(b) Determine risk management performance indicators that align with performance indicators of the organisation.	To measure risk management performance against indicators, which are periodically reviewed for appropriateness;	Performance indicators (Key risk indicators)
				(c) Align risk management objectives with the objectives and strategies of the organisation.	To encourage a risk mind-set for decision making.	Strategic plan / Business plan / Risk plan / Risk management objectives / Risk appetite statement / Risk tolerance levels

Addendum K: Validated ERM implementation model: theoretical frameworks, building blocks, best practice requirements and proposed deliverables

Theoretical frameworks		Building blocks	Best practice requirements		Proposed deliverables	
Deming cycle	Weisbord organisational design model		Level 1	Level 2	Purpose	Deliverables
Plan	Leadership, Relationships	II. Establish the tone of the organisation.	The organisation: introduction of risk management and ensuring its ongoing effectiveness require strong and sustained commitment by management of the organisation, as well as strategic and rigorous planning to achieve commitment at all levels. The induction and ongoing training programs of the board should incorporate risk governance. (Note:	(d) Assign accountabilities and responsibilities at appropriate levels within the organisation.	To reduce role confusion by establishing clear roles and responsibilities for risk activities across businesses and risk types.	Risk governance model: (incl. risk owners' matrix, roles & responsibilities, reporting & escalation process & incentives guidelines & individual performance scorecard.)
				(e) Ensure that the necessary resources are allocated to risk management.	To ensure the effective and efficient implementation of the ERM program.	Risk management plan (People, Processes and Budget) / Annual performance plan / Operational budget
				(f) Communicate the benefits of risk management to all stakeholders.	To raise risk awareness and create excitement for the project.	Risk training material / Business case / Risk management policy / Embedded in risk reports / Board risk report
					To create a common risk language, improve risk awareness and encourage risk based decision making.	Risk awareness gap analysis Risk maturity assessment Risk awareness strategy & plan
Plan	Purpose, Relationships, Structure, External environment	III. Design the rules of the game.	Design the risk management framework.	Task: Understanding the organisation and its context (Know your organisation) Establish the external context:		
				(a) the social and cultural, political, legal, regulatory, financial, technological, economic, natural and competitive environment, whether international, national, regional or local;	To get an overall picture of the external environment based PESTLE and / or Porter's 5 forces.	Environmental scanning report
				(b) key drivers and trends having impact on the objectives of the organisation; and		Key business drivers report
				(c) External stakeholder analysis		Stakeholder analysis
				Establish the internal context:	To describe the internal value chain of the organisation and to identify areas that would create risks and opportunities	Environmental scanning of the INTERNAL value chain SWOT analysis Organisational organigram Divisional organigram Departmental organigram Delegation of authority Committee structure Committee charters List of policies Copy of policies Action plans (strategies) Risk competency model Job profiles / specification Technical job specs List of systems Process maps Escalation policy Escalation process Connected stakeholder analysis Internal stakeholder analysis Organisational culture survey results List of standards, guidelines and models Contracts register
				(a) Governance, organisational structure, roles and accountabilities;		
				(b) Policies, objectives, and the strategies that are in place to achieve them;		
				(c) Capabilities, understood in terms of resources and knowledge (e.g. capital, time, people, processes, systems and		
				(d) Information systems, information flows and decision making processes (both formal and informal)		
				Connected stakeholder analysis		
				(e) Internal stakeholder analysis		
				(f) Temperature checks on organisational culture		
				(g) Standards, guidelines and models adopted by the organisation; and		
				(h) the form and extent of contractual relationships.		

Addendum K: Validated ERM implementation model: theoretical frameworks, building blocks, best practice requirements and proposed deliverables

Theoretical frameworks		Building blocks	Best practice requirements		Proposed deliverables	
Deming cycle	Weisbord organisational design model		Level 1	Level 2	Purpose	Deliverables
Plan	Purpose, Relationships, Structure, External environment	III. Design the rules of the game.	Design the risk management framework.		To describe the internal value chain of the organisation and to identify areas that would create risks and opportunities	Internal audit reports
						External audit reports
						Strategic plan
						Business plans
				Establish the context of the risk management process (The context of the risk management process will vary according to the needs of an organisation. It can involve, but is not limited to:	To create ONE set of risk management rules for the organisation.	Risk management file / manual that includes:
				(a) Defining the goals and objectives of the risk management activities;		Risk management goals & -objectives
				(b) Defining responsibilities for and within the risk management process;		Risk governance model
				(c) Defining the scope, as well as the depth and breadth of the risk management activities to be carried out, including specific inclusions and exclusions;		Top-down & Bottom-up risk management activities
				(e) Defining the activity, process, function, project, product, service or asset in terms of time and location;		
				(f) Defining the relationships between a particular project, process or activity and other projects, processes or activities of the organisation;		
				(g) Defining the risk assessment methodologies;		Interconnectedness maps
				(h) Defining the way performance and effectiveness is evaluated in the management of risk;		Risk assessment methodologies
				(i) Identifying and specifying the decisions that have to be made; and		Key risk indicators
				(j) Identifying, scoping or framing studies needed, their extent and objectives, and the resources required for such studies.		Decision matrix
				Define the risk criteria (When defining risk criteria, factors to be considered should include the following:	To create standardised risk assessment criteria for the organisation as a whole. To give risk owners and other risk stakeholders insight into risk management in their terms.	Risk management file / manual that includes:
				(a) The nature and types of causes and consequences that can occur and how they will be measured;		Examples of causes and consequences
				(b) How likelihood will be defined;		Risk assessment tools and techniques
				(c) The timeframe(s) of the likelihood and/or consequence(s);		Risk management plan
				(d) How the level of risk is to be determined;		Risk appetite guidelines
				(e) The views of stakeholders;		Risk tolerance levels guidelines
				(f) The level at which risk becomes acceptable or tolerable; and		
				(g) Whether combinations of multiple risks should be taken into account and, if so, how and which combinations should be considered.		

Addendum K: Validated ERM implementation model: theoretical frameworks, building blocks, best practice requirements and proposed deliverables

Theoretical frameworks		Building blocks	Best practice requirements		Proposed deliverables	
Deming cycle	Weisbord organisational design model		Level 1	Level 2	Purpose	Deliverables
Plan	Purpose, Relationships, Structure, External environment	III. Design the rules of the game.	Design the risk management framework.	Task: establishing the risk management policy	To document risk management scope, objectives and roles and responsibilities.	Risk management policy
				(a) A policy and plan for a system and process of risk management should be developed.		
				(c) The board's responsibility for risk governance should manifest in a documented risk management policy and plan.		
				(d) The board should approve the risk management policy and plan.		
				The risk management policy should be widely distributed throughout the company.		
				Task: develop an accountability matrix / risk governance framework	To establish clear roles and responsibilities for risk activities across businesses and risk types.	Risk governance framework: (incl. risk owners' matrix, roles & responsibilities, reporting & escalation process & incentives guidelines & individual performance scorecards)
				(a) Identifying risk owners that have the accountability and authority to manage risks;		
				(b) Identifying who is accountable for the development, implementation and maintenance of the framework for managing risk;		
				(c) Identifying other responsibilities of people at all levels in the organisation for the risk management process;		
				(d) Establishing performance measurement and external and/or internal reporting and escalation processes; and		
				(e) Ensuring appropriate levels of recognition.		
				Task: integration into organisational processes	To embed risk management in all the organisation's practices and processes in a way that it is relevant, effective and efficient.	
				Develop a common risk language		Common risk language
				Risk management should be embedded in all the organisation's practices and processes in a way that it is relevant, effective and efficient.		Risk owners
						Strategic plan
						Business plan
						Financial plan
						Risk & incident escalation process
						New products development
						Operational processes
						Investment decisions
						Combined assurance
						Performance management process
						Change management process
						Quality assurance process
				Align risk management objectives with the objectives and strategies of the organisation.	To encourage a risk mind-set for decision making.	Risk appetite guidelines Risk tolerance levels guidelines Strategic plans Business plans
				Determine risk management performance indicators that align with performance indicators of the organisation.	To measure risk management performance against indicators, which are periodically reviewed for appropriateness;	Performance reporting metrics, i.e. key risk indicators

Addendum K: Validated ERM implementation model: theoretical frameworks, building blocks, best practice requirements and proposed deliverables

Theoretical frameworks		Building blocks	Best practice requirements		Proposed deliverables	
Deming cycle	Weisbord organisational design model		Level 1	Level 2	Purpose	Deliverables
Plan	Purpose, Relationships, Structure, External environment	III. Design the rules of the game.	Design the risk management framework.	Task: Establishing internal communication and reporting mechanisms	To create one set of rules for risk communication and also to increase risk transparency.	Internal reporting guidelines
				(a) Key components of the risk management framework, and any subsequent modifications, are communicated appropriately;		Communication guidelines
				(b) there is adequate internal reporting on the framework, its effectiveness and the outcomes;		
				(c) relevant information derived from the application of risk management is available at appropriate levels and times; and		
				(d) there are processes for consultation with internal stakeholders.		
				Task: Establishing external communication and reporting mechanisms	To create one set of rules for risk communication and also to increase risk transparency.	
				(a) Engaging appropriate external stakeholders and ensuring an effective exchange of information;		External reporting guidelines
				(b) External reporting to comply with legal, regulatory, and governance requirements;		Communication guidelines
				(c) Providing feedback and reporting on communication and consultation;		
			Design the risk management process.	Step 1: Communication and consultation	To develop a standardised risk management process for the organisation.	Risk management process guidelines
				Step 2: Establish the context		
				Step 3: Risk identification		
				Step 4: Risk analysis		
				Step 5: Risk evaluation		
				Step 6: Risk treatment		
				Step 7: Monitor and review		
				Step 8: Continuous improvement		
Plan	Helping mechanisms, Relationships, Rewards	IV. Develop the risk infrastructure.	Task: Allocate appropriate resources for risk management			
			People (skills, experience, competence & training programs).	People: skills, experience, competence & training programs	To establish decision making structures, escalation protocol & identify risk	Risk governance models
					To identify competencies, skills levels and experience required by risk stakeholders.	Performance management scorecards
					To ensure proper training for risk stakeholders.	Job profiles
			Committees: the board should delegate certain functions to well-structured committees but without abdicating its own responsibilities.	Board committees: Formal terms of reference should be established and approved for each committee of the board. The committees' terms of reference should be reviewed yearly.	To formalise decision making structures, escalation protocol & identify risk stakeholders.	Risk training: induction sessions and risk awareness sessions
						Board committees charter / terms of reference

Addendum K: Validated ERM implementation model: theoretical frameworks, building blocks, best practice requirements and proposed deliverables

Theoretical frameworks		Building blocks	Best practice requirements		Proposed deliverables	
Deming cycle	Weisbord organisational design model		Level 1	Level 2	Purpose	Deliverables
Plan	Helping mechanisms, Relationships, Rewards	IV. Develop the risk infrastructure.	Committees: the board should delegate certain functions to well-structured committees but without abdicating its own responsibilities.	The committees should be appropriately constituted and the composition and the terms of reference should be disclosed in the integrated report.	To formalise decision making structures, escalation protocol & identify risk stakeholders.	Integrated report
				The risk committee should:		Risk committees:
				consider the risk management policy and plan and monitor the risk management process;		Board risk committee terms of reference
				have as its members executive and non-executive directors, members of senior management and independent risk management experts to be invited, if necessary;		Executive risk committee terms of reference
				have a minimum of three members; and		Departmental risk committee terms of reference
				convene at least twice per year.		Audit and risk committee
				The audit committee should:		Audit committee charter
				oversee integrated reporting.		
				have regard to all factors and risks that may impact on the integrity of the integrated report.		
				review and comment on the financial statements included in the integrated report.		
				review the disclosure of sustainability issues in the integrated report to ensure that it is reliable and does not conflict with the financial information.		
				recommend to the board to engage an external assurance provider on material sustainability issues.		
				consider the need to issue interim results.		
				review the content of the summarised information.		
				engage the external auditors to provide assurance on the summarised financial information.		
				ensure that a combined assurance model is applied to provide a coordinated approach to all assurance activities.		
				ensure that the combined assurance is received is appropriate to address all the significant risks facing the company.		
				monitor the relationship between the external assurance providers and the company.		
				The audit committee should be an integral component of the risk management process.		
				The charter of the audit committee should set out its responsibilities regarding risk management.		
				The audit committee should specifically have oversight of:		
				financial reporting risks;		
				internal financial controls;		

Addendum K: Validated ERM implementation model: theoretical frameworks, building blocks, best practice requirements and proposed deliverables

Theoretical frameworks		Building blocks	Best practice requirements		Proposed deliverables	
Deming cycle	Weisbord organisational design model		Level 1	Level 2	Purpose	Deliverables
Plan	Helping mechanisms, Relationships, Rewards	IV. Develop the risk infrastructure.	Committees: the board should delegate certain functions to well-structured committees but without abdicating its own responsibilities.	fraud risks as it relates to financial reporting; and	To formalise decision making structures, escalation protocol & identify risk stakeholders.	Audit committee charter
				IT risks as it relates to financial reporting.		Combined assurance committee terms of reference
				The audit committee should also:		
				ensure that a combined assurance model is applied to provide a coordinated approach to all assurance activities		
				ensure that the combined assurance is received is appropriate to address all the significant risks facing the company.		Risk specific committee terms of reference e.g. Fraud risk committee
			Models & tools: the organisation's processes, methods and tools to be used for managing risk		To assess and decide on standardised tools that should be used across the organisation.	Risk identification tools
						Risk analysis tools
						Risk evaluation tools
						Risk response tools
						Risk monitoring tools
						Risk reporting tools
						Risk quantification models
			Templates: standardised recording, reporting and assessment templates		To standardise policy, framework, recording, reporting and assessment templates.	Examples:
						Risk management plan
						Risk communication plan
						Stakeholder maps
						Stakeholder register
						Risk register
						Risk improvement report
						Integrated assurance dashboard
						Integrated report
						Risk self-assessments
						Stewardship report
						Recording process
						Risk acceptance form
						Risk retirement form
						Reporting dashboards
						Reporting scorecards
						Risk policy
						Risk management framework
						Risk committee terms of reference
			Processes: documented processes and procedures.		To embed risk management in all the organisation's practices and processes in a way that it is relevant, effective and efficient.	Common risk language
						Risk owners matrix
						Strategic planning process
						Business planing process
						Financial planning process
			Systems: information and knowledge management systems		To select the most appropriate risk management systems.	Change management process
						Quality assurance process
						Risk management process
						Risk & incident escalation process
						External audit process
						Performance management process
						Risk recording
						Risk reporting
						Risk monitoring
						Risk review

Addendum K: Validated ERM implementation model: theoretical frameworks, building blocks, best practice requirements and proposed deliverables

Theoretical frameworks		Building blocks	Best practice requirements		Proposed deliverables	
Deming cycle	Weisbord organisational design model		Level 1	Level 2	Purpose	Deliverables
Do	Leadership, Structure, Relationships, Helping Mechanisms, External environment	V. Implement the ERM program.	Implementing the framework for managing risk.	Define the appropriate timing and strategy for implementing the framework;	To establish a time line for risk management activities.	Risk management plan (calendar) Critical path analysis for key dependencies
				Apply the risk management policy and process to the organisational processes;	To embed risk management in all the organisation's practices and processes in a way that it is relevant, effective and efficient.	Common risk language
						Risk owners matrix
						Strategic planning process
						Business planning process
						Financial planning process
						Change management process
						Quality assurance process
						Risk management process
				Risk & incident escalation process		
			Performance management process			
			Comply with legal and regulatory requirements;	To communicate risk related compliance requirements.	Legal, regulatory & best practice compliance register (pertaining to risk)	
			Ensure that decision making, including the development and setting of objectives, is aligned with the outcomes of risk management processes;	To encourage a risk mind-set for decision making.	Risk appetite statements Risk tolerance levels Strategic plan ERM framework & policy	
			Hold information and training sessions; and	To create a common risk language, improve risk awareness and encourage risk based decision making.	Risk awareness gap analysis Risk maturity assessment Risk awareness strategy & -plan	
				To ensure that the risk management framework remains appropriate.	Risk facilitation sessions	
			Implementing the risk management process.	Step 1: Communication and consultation with external and internal stakeholders should take place during all stages of the risk management process.	To identify the internal and external stakeholders for the organisation / division / department / project.	Stakeholder analysis
					To identify the most appropriate communication tools and establish timelines.	Risk communication plan
					To ensure that the right information reaches the right people at the right time.	Risk reports e.g. stress tests, risk & control self-assessments, incident reports, risk treatment plans, key risk indicator reports.
				Step 2: Establish the context (Know your organisation / division / department / project / risk type)	To describe the UNIQUE context for the risk management project.	
				Establish the external context		External environment mind map External stakeholder register External stakeholder map
				Establish the internal context		Internal value chain mind map Internal stakeholder register Internal stakeholder map
				Establishing the context of the risk management process		Standardised risk management context (refer to building block III)
				Apply the risk criteria		Standardised risk criteria (refer to building block III)
				Step 3: Risk identification	Process of finding, recognising and describing risks.	Key / Principle / Strategic risk register Divisional / departmental / business unit risk register Emerging risk register Risk library

Addendum K: Validated ERM implementation model: theoretical frameworks, building blocks, best practice requirements and proposed deliverables

Theoretical frameworks		Building blocks	Best practice requirements		Proposed deliverables	
Deming cycle	Weisbord organisational design model		Level 1	Level 2	Purpose	Deliverables
			Implementing the risk management process.	Step 4: Risk analysis	Process to comprehend the nature of risk and to determine the level of risk (e.g. high, medium, low).	Key / Principle / Strategic risk register - risk ratings applied
				Step 5: Risk evaluation	Process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable.	Divisional / departmental / business unit risk register - risk ratings applied
						Root cause analysis
				Step 6: Risk response	To identify the most appropriate risk treatment for the most significant risks.	Key / Principle / Strategic risk profile - risk ratings + current controls applied & risk owners identified
						Divisional / departmental / business unit risk register risk ratings + current controls applied & risk owners identified
						Controls library
Check	Rewards	VI. Monitor and review the ERM program.	Monitoring activities by the Board	The board should ensure continual risk monitoring by management	To ensure proper risk oversight.	Risk governance framework
				The board should ensure that effective and continual monitoring of risk management takes place.	To reduce role confusion and provide clear guidelines for risk monitoring.	Risk management plan (monitoring roles and responsibilities)
				The responsibility for monitoring should be defined in the risk management plan.	To periodically measure progress against, and deviation from, the risk management plan.	Status report on risk management plan implementation
			Review activities by the Board	The board should comment in the integrated report on the effectiveness of the system and process of risk management.	To periodically review whether the risk management framework, policy and plan are still appropriate, given the	Integrated report (risk and opportunities section)
				The board should ensure that effective and continual monitoring of risk management takes place.	To periodically measure progress against, and deviation from, the risk management plan.	Annual board risk report
				The board should review the implementation of the risk management plan at least once a year.	To periodically review whether the risk management framework, policy and plan	Risk management plan implementation status report
				The performance of the committee should be evaluated once a year by the board.	To periodically review whether the risk management framework, policy and plan	Risk improvement report
			Monitor the risk management framework	The board should monitor that risks taken are within the tolerance and appetite levels.	To ensure effectiveness and efficiency with regards to committee activities.	Internal audit report
				Measure risk management performance against indicators, which are periodically reviewed for appropriateness;	To ensure compliance with the risk appetite framework.	Board risk committee performance evaluation
					To ensure compliance with the risk tolerance levels.	Risk appetite status report
				Periodically measure progress against, and deviation from, the risk management plan;	To measure risk management performance against indicators, which are periodically reviewed for appropriateness;	Risk tolerance status report
				Report on risk, progress with the risk management plan and how well the risk management policy is being followed;	To periodically measure progress against, and deviation from, the risk management plan.	KRI performance report
				Monitor the level of risk awareness	To periodically measure progress against, and deviation from, the risk management plan.	Risk management plan implementation status report
					To report on risk, progress with the risk management plan and how well the risk management policy is being followed.	Risk management policy compliance report
			Review the risk management framework	Periodically review whether the risk management framework, policy and plan are still appropriate, given the organizations' external and internal context;	To track the improvement of risk awareness.	Deviations from risk management policy report
						Risk culture surveys
						Risk improvement report
						Internal audit report
						Risk calendar

Addendum K: Validated ERM implementation model: theoretical frameworks, building blocks, best practice requirements and proposed deliverables

Theoretical frameworks		Building blocks	Best practice requirements		Proposed deliverables			
Deming cycle	Weisbord organisational design model		Level 1	Level 2	Purpose	Deliverables		
Check	Rewards	VI. Monitor and review the ERM program.	Review the risk management framework	Communicate and consult with stakeholders to ensure that its risk management framework remains appropriate.	To periodically review whether the risk management framework, policy and plan are still appropriate, given the organisations' external and internal context.	Risk improvement report		
				Review the effectiveness of the risk management framework.		Subject matter expert gap analysis		
			Monitor the risk management process	Ensuring that controls are effective and efficient in both design and operation.		Internal audit reports		
						Risk calendar		
				Identifying emerging risks.		To identify emerging risks in the organisation's internal value chain and external environment.	ISO 9000 reports	
			Review the risk management process	Analysing and learning lessons from events (including near-misses), changes, trends, successes and failures;	To ensure that controls are effective and efficient in both design and operation.	Internal audit reports, risk committee effectiveness, qualitative conversations, risk appetite and risk tolerance level breaches, signed letters of representation.		
						To ensure that controls are effective and efficient in both design and operation.		Subject matter expert gap analysis
								Combined assurance reports
			To identify emerging risks in the organisation's internal value chain and external environment.		Risk profile status reports			
					Internal audit reports			
To analyse and learn lessons from events (including near-misses), changes, trends, successes and failures.		External audit reports						
		Emerging risk register						
Adjust	Leadership, Purposes, Structure, Relationships, Rewards, Helpful mechanisms, External environment	VII. Continual improvement of the ERM program.	The board should receive assurance regarding the effectiveness of the risk management process	Management should provide assurance to the board that the risk management plan is integrated in the daily activities of the company.	To inform the relevant committees and risk stakeholders of the level of assurance provided by assurance providers.	Variance and trend analysis		
				Internal audit should:		Post mortem sessions		
				provide a written assessment of the effectiveness of the system of internal controls and risk management to the board.		Environmental scanning		
				detect changes in the external and internal context, including changes to risk criteria and the risk itself which can require revision of risk treatments and priorities; and		Risk reconciliation reports		
			obtaining further information to improve risk assessment.		To periodically review whether the risk management framework, policy and plan are still appropriate, given the organisations' external and internal context;	Post loss analysis		
						To periodically review whether the risk management framework, policy and plan are still appropriate, given the organisations' external and internal context;		Combined assurance report.
								Risk reports to various committees
								Risk maturity assessment
						Benchmarking assessments (peer reviews & best practice)		
								Risk improvement report
								Internal audit report
						Risk improvement report (List of internal, external, risk management process & risk criteria context changes)		
						Risk improvement report (risk assessment process & methodology)		

Source: Researcher's own compilation

Addendum L: Phase 2 - Round 3: Confirm the conceptual ERM implementation and degree of formality assessment tools

				IV1			IV2			IV4			IV6		
Process		Responsibility	Deliverable	Agree	Dis-agree	Comments	Agree	Dis-agree	Comments	Agree	Dis-agree	Comments	Agree	Dis-agree	Comments
1	Assign the responsible risk stakeholder per deliverable.	Risk owner	ERM implementation plan	x			x			x			x		
2	Get implementation status (Who? Risk facilitator)	Risk facilitator	Status on ERM implementation	x			x			x			x		
3	Prepare the ERM implementation status reporting dashboard (Who? Risk facilitator)	Risk facilitator	ERM implementation reporting dashboard	x			x		Maybe it is not level but it is about whether the implementation program is 'done or not done'.	x			x		
4	For YES deliverables, assess the degree of formality (Who? Independent assurance provider	Independent risk assurance provider	Degree of formality report	x			x		"No. 3", What will happen if the answer to implementation status checklist is 'NO'. I would suggest you cover that, unless it is mentioned somewhere in the document.	x			x		
5	Prepare the ERM implemented deliverables: degree of formality reporting dashboard (Who? Independent assurance provider)	Independent risk assurance provider	Degree of formality reporting dashboard	x			x		The degree makes it sounds as if we are assessing the magnitude/level of implementation. Yet to me it appears as if we are checking if it exists.	x			x		
6	Report to relevant risk committees.	Independent risk assurance provider	Degree of formality reporting dashboard	x		Note: the risk committee acts on behalf of the Board	x			x			x		
7	Feedback loops from risk committees to risk facilitators and independent assurance providers			x			x			x			x		

Addendum L: Phase 2 - Round 3: Confirm the conceptual ERM implementation and degree of formality assessment tools

Process	Responsibility	Deliverable	IV1			IV2			IV4			IV6		
			Agree	Dis-agree	Comments	Agree	Dis-agree	Comments	Agree	Dis-agree	Comments	Agree	Dis-agree	Comments
General comments											I support the two-prong approach with the two tools, one being a precursor or input to the other. However, I think that status on implementation should include "In process and on schedule" and "In process but behind schedule" – the Steering Committee could derive greater value from the expanded status report. Just out of interest, remember in linguistics, a yes–no question, is formally known as a polar question (a			

Source: Researcher's own compilation

Addendum L: Phase 2 - Round 3: Confirm the conceptual ERM implementation and degree

				IV7			IV8			IV13			IV19			Frequency	
Process		Responsibility	Deliverable	Agree	Dis-agree	Comments	Agree	Dis-agree	Comments	Agree	Dis-agree	Comments	Agree	Dis-agree	Comments	Agree	Dis-agree
1	Assign the responsible risk stakeholder per deliverable.	Risk owner	ERM implementation plan	x			x			x						11	
2	Get implementation status (Who? Risk facilitator)	Risk facilitator	Status on ERM implementation	x			x			x					1) Do not understand this "assessment" done at this stage, as your first checklist that flow from your model is to determine what will be implemented from he model and what not. Should this not then be "determine ERM implemenation status"? Also see comment on yes and no 0 at no 3. 2) Not sure what you see as a risk facilitator, but implementation status (See comment on that it I feel this should not be done here) is determined by the ERM division/practitioner and then reviewed/assessed by Internal Audit	11	
3	Prepare the ERM implementation status reporting dashboard (Who? Risk facilitator)	Risk facilitator	ERM implementation reporting dashboard	x			x			x					Where does approval from management on what should be implemented and what not come in? What does yes and no means? Does yes mean that this will be implemented and no means that this will not be implemented? If not, then the checklist at 5 "Not started" does not fit.	11	
4	For YES deliverables, assess the degree of formality (Who? Independent assurance provider	Independent risk assurance provider	Degree of formality report	x			x			x					1) My English is letting me down but I do not understand what is meant with Degree of Formality? 2) Again, first it should be assessed by the ERM Division/practitioner and then yearly reviewed by Internal Audit	11	
5	Prepare the ERM implemented deliverables: degree of formality reporting dashboard (Who? Independent assurance provider)	Independent risk assurance provider	Degree of formality reporting dashboard	x			x			x						11	
6	Report to relevant risk committees.	Independent risk assurance provider	Degree of formality reporting dashboard	x			x			x					1) I am missing reporting to management. This should be done before reporting to the risk committees. 2) Providing assurance of the implementation status to be done by IA should be added	11	
7	Feedback loops from risk committees to risk facilitators and independent assurance providers			x			x			x					The flow should only go from RC to ERM implementation model as the process ensure reporting at the end and not required at this stage.	11	

Addendum L: Phase 2 - Round 3: Confirm the conceptual ERM implementation and degree

Process	Responsibility	Deliverable	IV7			IV8			IV13			IV19			Frequency	
			Agree	Dis-agree	Comments	Agree	Dis-agree	Comments	Agree	Dis-agree	Comments	Agree	Dis-agree	Comments	Agree	Dis-agree
General comments														Here is the flow I suggest: 1 - ERM Model 2 - Determine what will be implemented 2.1 Approval from management on ERM model to be implemented 2.2 Checklist on what is in and what not. 3. Determine status of implementation 3.1 Checklist on implementation status 4. Review by IA of implementation status. 5. Reporting to Management 5.1 Feedback to ERM Model 6. Reporting to RC 6.1 Feedback to ERM Model		

Source: Researcher's own compilation

Addendum M: ERM implementation assessment tool - risk assurance checklist

Theoretical frameworks		Building blocks	Best practice requirements		Proposed deliverables		Building Block	Responsi- bility	Risk Assurance				Corrective Actions		
Deming cycle	Weisbord organisational design model		Level 1	Level 2	Purpose	Deliverables			YES	Not started	In process	Done	Activities	Responsibility	Target Date
Plan	Purpose, Leadership	I. Formalise the instruction and get permission.	Instruction / Trigger	Business trigger e.g. event, merger & acquisition due diligence requirement, peer pressure, etc.	To motivate the need for an ERM program.	Business case document	I		1						
				Ensure legal and regulatory compliance.	To motivate the need for an ERM program.	Compliance register (legal + regulatory + best practise frameworks)	I		1						
			Permission / Mandate	The board should delegate to management the responsibility to design, implement and monitor the risk management plan.	To ask for permission / mandate to design and implement the ERM program.	Agenda item for the decision making forum e.g. Board meeting, Executive committee meeting.	I		1						
					To record the permission / mandate received to design and implement an ERM program.	Minutes of the decision making forum e.g. Board meeting, Executive committee meeting.	I		1						
			Oversight: the risk committee or audit committee should assist the board in carrying out its risk responsibilities	The board should appoint a committee responsible for risk.	To assist the board in carrying out its risk roles and responsibilities.	Board risk committee (BRC) terms of reference / Audit committee charter / Audit and risk committee charter	I	CRO							
				The risk committee should:											
				consider the risk management policy and plan and monitor the risk management process;											
				have as its members executive and non-executive directors, members of senior management and independent risk management experts to be invited, if necessary;											
				have a minimum of three members; and convene at least twice per year.											
				The board's responsibility for risk governance should be expressed in the board charter.											
			Define and endorse the risk management policy	The board's responsibility for risk governance should manifest in a documented risk management policy and plan.	To document risk management scope, objectives and roles and responsibilities.	Risk management policy	I	CRO							
				The board should approve the risk management policy and plan.											
				The risk management policy should be widely distributed throughout the company.											
Plan	Leadership, Relationships	II. Establish the tone of the organisation.	Establishing the tone of the organisation: The introduction of risk management and ensuring its ongoing effectiveness require strong and sustained commitment by management of the organisation, as well as strategic and rigorous planning to achieve commitment at all levels.	The CRO should be a suitably experienced person who should have access and interact regularly on strategic matters with the board and/or appropriate board committee and executive management.	A senior level ERM program sponsor / Chief Risk Officer should have clear authority over and accountability for oversight of risk across the enterprise	CRO / Senior level project sponsor	II		1						
				(a) Ensure that the organisation's culture and risk management policy are aligned.	To create risk awareness at all levels of the organisations and to encourage risk based decision making.	Risk management policy / Risk requirements evident in business, project and HR requirements and standards / Strategic intent document / Risk communication strategy / Internal audit reports / External audit report / Insurance claims	II	CRO							

Addendum M: ERM implementation assessment tool - risk assurance checklist

Theoretical frameworks		Building blocks	Best practice requirements		Proposed deliverables		Building Block	Responsi- bility	Risk Assurance				Corrective Actions			
Deming cycle	Weisbord organisational design model		Level 1	Level 2	Purpose	Deliverables			YES	Not started	In process	Done	Activities	Responsibility	Target Date	
Plan	Leadership, Relationships	II. Establish the tone of the organisation.	Establishing the tone of the organisation: The introduction of risk management and ensuring its ongoing effectiveness require strong and sustained commitment by management of the organisation, as well as strategic and rigorous planning to achieve commitment at all levels.	(b) Determine risk management performance indicators that align with performance indicators of the organisation.	To measure risk management performance against indicators, which are periodically reviewed for appropriateness;	Performance indicators (Key risk indicators)	II	CRO								
				(c) Align risk management objectives with the objectives and strategies of the organisation.	To encourage a risk mind-set for decision making.	Strategic plan / Business plan / Risk plan / Risk management objectives / Risk appetite statement / Risk tolerance levels	II	CRO								
				(d) Assign accountabilities and responsibilities at appropriate levels within the organisation.	To reduce role confusion by establishing clear roles and responsibilities for risk activities across businesses and risk types.	Risk governance model: (incl. risk owners' matrix, roles & responsibilities, reporting & escalation process & incentives guidelines & individual performance scorecard.)	II		1							
				(e) Ensure that the necessary resources are allocated to risk management.	To ensure the effective and efficient implementation of the ERM program.	Risk management plan (People, Processes and Budget) / Annual performance plan / Operational budget	II		1							
				(f) Communicate the benefits of risk management to all stakeholders.	To raise risk awareness and create excitement for the project.	Risk training material / Business case / Risk management policy / Embedded in risk reports / Board risk report	II		1							
			The induction and ongoing training programmes of the board should incorporate risk governance. (Note:		To create a common risk language, improve risk awareness and encourage risk based decision making.	Risk awareness gap analysis	II	CRO								
Plan	Purpose, Relationships, Structure, External environment	III. Design the rules of the game.	Design the risk management framework.	Task: Understanding the organisation and its context (Know your organisation)												
				Establish the external context:	To get an overall picture of the external environment based PESTLE and / or Porter's 5 forces.	Environmental scanning report	III	CRO								
				(a) the social and cultural, political, legal, regulatory, financial, technological, economic, natural and competitive environment, whether international, national, regional or local;												
				(b) key drivers and trends having impact on the objectives of the organisation; and												
				(c) External stakeholder analysis												
				Establish the internal context:	To describe the internal value chain of the organisation and to identify areas that would create risks and opportunities	Environmental scanning of the INTERNAL value chain	III	CRO (get from CSO)								
				(a) Governance, organisational structure, roles and accountabilities;		SWOT analysis	III		1							
						Organisational organigram	III		1							
						Divisional organigram	III		1							
						Departmental organigram	III		1							
						Delegation of authority	III		1							
						Committee structure	III		1							
						Committee charters	III		1							
						(b) Policies, objectives, and the strategies that are in place to achieve them;	List of policies	III	CRO (get from Company Secretary)							
				Copy of policies			III	CRO (get from Company Secretary)								
				Action plans (strategies)			III	CRO (get from Company Secretary)								
				(c) Capabilities, understood in terms of resources and knowledge (e.g. capital, time, people, processes, systems and		Risk competency model	III		1							
						Job profiles / specification	III		1							
					Technical job specs	III		1								
				(d) Information systems, information flows and decision making processes (both formal and informal)	List of systems	III	CRO (get from CTO)									
					Process maps	III		1								
					Escalation policy	III		1								
					Escalation process	III		1								
				Connected stakeholder analysis	Connected stakeholder analysis	III	CRO (get from CSO)									
				(e) Internal stakeholder analysis	Internal stakeholder analysis	III		1								
				(f) Temperature checks on organisational culture	Organisational culture survey results	III		1								
				(g) Standards, guidelines and models adopted by the organisation; and	List of standards, guidelines and models	III		1								
(h) the form and extent of contractual relationships.	Contracts register	III	CRO (get from CPO)													

Addendum M: ERM implementation assessment tool - risk assurance checklist

Theoretical frameworks		Building blocks	Best practice requirements		Proposed deliverables		Building Block	Responsi- bility	Risk Assurance				Corrective Actions		
Deming cycle	Weisbord organisational design model		Level 1	Level 2	Purpose	Deliverables			YES	Not started	In process	Done	Activities	Responsibility	Target Date
Plan	Purpose, Relationships, Structure, External environment	III. Design the rules of the game.	Design the risk management framework.		To describe the internal value chain of the organisation and to identify areas that would create risks and opportunities	Internal audit reports	III		1						
					External audit reports	III		1							
					Strategic plan	III		1							
					Business plans	III	CRO (get from C-LEVELS)								
					Establish the context of the risk management process (The context of the risk management process will vary according to the needs of an organisation. It can involve, but is not limited to:		Risk management file / manual that includes:								
				(a) Defining the goals and objectives of the risk management activities;		Risk management goals & -objectives	III		1						
				(b) Defining responsibilities for and within the risk management process;		Risk governance model	III		1						
				(c) Defining the scope, as well as the depth and breadth of the risk management activities to be carried out, including specific inclusions and exclusions;		Top-down & Bottom-up risk management activities	III		1						
				(e) Defining the activity, process, function, project, product, service or asset in terms of time and location;	To create ONE set of risk management rules for the organisation.	Interconnectedness maps	III		1						
				(f) Defining the relationships between a particular project, process or activity and other projects, processes or activities of the organisation;		Risk assessment methodologies	III		1						
				(g) Defining the risk assessment methodologies;		Key risk indicators	III	CRO							
				(h) Defining the way performance and effectiveness is evaluated in the management of risk;		Decision matrix	III	CRO							
				(i) Identifying and specifying the decisions that have to be made; and		Research to clarify context	III	CRO							
				(j) Identifying, scoping or framing studies needed, their extent and objectives, and the resources required for such studies.											
				Define the risk criteria (When defining risk criteria, factors to be considered should include the following:		Risk management file / manual that includes:									
				(a) The nature and types of causes and consequences that can occur and how they will be measured;		Examples of causes and consequences	III		1						
				(b) How likelihood will be defined;		Risk assessment tools and techniques	III		1						
				(c) The timeframe(s) of the likelihood and/or consequence(s);	To create standardised risk assessment criteria for the organisation as a whole. To give risk owners and other risk stakeholders insight into risk management in their terms.	Risk management plan	III	CRO							
				(d) How the level of risk is to be determined;		Risk appetite guidelines	III	CRO							
				(e) The views of stakeholders;		Risk tolerance levels guidelines	III	CRO							
				(f) The level at which risk becomes acceptable or tolerable; and											
				(g) Whether combinations of multiple risks should be taken into account and, if so, how and which combinations should be considered.											
				Task: establishing the risk management policy											
				(a) A policy and plan for a system and process of risk management should be developed.											
				(c) The board's responsibility for risk governance should manifest in a documented risk management policy and plan.	To document risk management scope, objectives and roles and responsibilities.	Risk management policy	III	CRO							
				(d) The board should approve the risk management policy and plan.											
				The risk management policy should be widely distributed throughout the company.											
				Task: develop an accountability matrix / risk governance framework											
				(a) Identifying risk owners that have the accountability and authority to manage risks;	To establish clear roles and responsibilities for risk activities across businesses and risk types.	Risk governance framework: (incl. risk owners' matrix, roles & responsibilities, reporting & escalation process & incentives guidelines & individual performance scorecards)	III		1						
				(b) Identifying who is accountable for the development, implementation and maintenance of the framework for managing risk;											

Addendum M: ERM implementation assessment tool - risk assurance checklist

Theoretical frameworks		Building blocks	Best practice requirements		Proposed deliverables		Building Block	Responsi- bility	Risk Assurance				Corrective Actions		
Deming cycle	Weisbord organisational design model		Level 1	Level 2	Purpose	Deliverables			YES	Not started	In process	Done	Activities	Responsibility	Target Date
Plan	Purpose, Relationships, Structure, External environment	III. Design the rules of the game.	Design the risk management framework.	(c) Identifying other responsibilities of people at all levels in the organisation for the risk management process;	To establish clear roles and responsibilities for risk activities across businesses and risk types.	Risk governance framework: (incl. risk owners' matrix, roles & responsibilities, reporting & escalation process & incentives guidelines & individual performance scorecards)	III								
				(d) Establishing performance measurement and external and/or internal reporting and escalation processes; and											
				(e) Ensuring appropriate levels of recognition.											
				Task: integration into organisational processes	To embed risk management in all the organisation's practices and processes in a way that it is relevant, effective and efficient.										
				Develop a common risk language		Common risk language	III		1						
				Risk management should be embedded in all the organisation's practices and processes in a way that it is relevant, effective and efficient.		Risk owners	III	CRO							
						Strategic plan	III	CSO							
						Business plan	III	C-LEVELS							
						Financial plan	III	CFO							
						Risk & incident escalation process	III		1						
						New products development	III	CRO							
						Operational processes	III	CRO							
						Investment decisions	III	CRO							
						Combined assurance	III	CRO							
						Performance management process	III	CRO							
						Change management process	III	CHRO							
						Quality assurance process	III	CPO							
						Risk appetite guidelines	III	CRO							
						Risk tolerance levels guidelines	III	CRO							
						Strategic plans	III	CSO							
						Business plans	III	C-LEVELS							
				Determine risk management performance indicators that align with performance indicators of the organisation.	To measure risk management performance against indicators, which are periodically reviewed for appropriateness;	Performance reporting metrics, i.e. key risk indicators	III	CRO							
				Task: Establishing internal communication and reporting mechanisms	To create one set of rules for risk communication and also to increase risk transparency.	Internal reporting guidelines	III		1						
				(a) Key components of the risk management framework, and any subsequent modifications, are communicated appropriately;		Communication guidelines	III		1						
				(b) there is adequate internal reporting on the framework, its effectiveness and the outcomes;											
				(c) relevant information derived from the application of risk management is available at appropriate levels and times; and											
				(d) there are processes for consultation with internal stakeholders.											
				Task: Establishing external communication and reporting mechanisms	To create one set of rules for risk communication and also to increase risk transparency.	External reporting guidelines	III		1						
				(a) Engaging appropriate external stakeholders and ensuring an effective exchange of information;		Communication guidelines	III		1						
				(b) External reporting to comply with legal, regulatory, and governance requirements;											
				(c) Providing feedback and reporting on communication and consultation;											
			Design the risk management process.	Step 1: Communication and consultation	To develop a standardised risk management process for the organisation.	Risk management process guidelines	III		1						
				Step 2: Establish the context											
				Step 3: Risk identification											
				Step 4: Risk analysis											
				Step 5: Risk evaluation											
				Step 6: Risk treatment											
				Step 7: Monitor and review											
				Step 8: Continuous improvement											

Addendum M: ERM implementation assessment tool - risk assurance checklist

Theoretical frameworks		Building blocks	Best practice requirements		Proposed deliverables		Building Block	Responsi- bility	Risk Assurance				Corrective Actions		
Deming cycle	Weisbord organisational design model		Level 1	Level 2	Purpose	Deliverables			YES	Not started	In process	Done	Activities	Responsibility	Target Date
Plan	Helping mechanisms, Relationships, Rewards	IV. Develop the risk infrastructure.	Task: Allocate appropriate resources for risk management												
			People (skills, experience, competence & training programs).	People: skills, experience, competence & training programs	To establish decision making structures, escalation protocol & identify risk	Risk governance models	IV	CRO							
					To identify competencies, skills levels and experience required by risk stakeholders.	Performance management scorecards	IV	CRO							
					To ensure proper training for risk stakeholders.	Job profiles	IV		1						
			Committees: the board should delegate certain functions to well-structured committees but without abdicating its own responsibilities.	Board committees:		Risk training: induction sessions and risk awareness sessions	IV	CRO							
				Formal terms of reference should be established and approved for each committee of the board.	To formalise decision making structures, escalation protocol & identify risk stakeholders.	Board committees charter / terms of reference	IV	CRO							
				The committees' terms of reference should be reviewed yearly.		Integrated report	IV	CRO							
				The committees should be appropriately constituted and the composition and the terms of reference should be disclosed in the integrated report.		Risk committees:									
				The risk committee should:		Board risk committee terms of reference	IV	CRO							
				consider the risk management policy and plan and monitor the risk management process;		Executive risk committee terms of reference	IV	CRO							
				have as its members executive and non-executive directors, members of senior management and independent risk management experts to be invited, if necessary;		Departmental risk committee terms of reference	IV	CRO							
				have a minimum of three members; and		Audit and risk committee	IV	CRO							
				convene at least twice per year.		Audit committee charter	IV	CAE							
				The audit committee should:											
				oversee integrated reporting.											
				have regard to all factors and risks that may impact on the integrity of the integrated report.											
				review and comment on the financial statements included in the integrated report.											
				review the disclosure of sustainability issues in the integrated report to ensure that it is reliable and does not conflict with the financial information.											
				recommend to the board to engage an external assurance provider on material sustainability issues.											
				consider the need to issue interim results.											
				review the content of the summarised information.											
				engage the external auditors to provide assurance on the summarised financial information.											
				ensure that a combined assurance model is applied to provide a coordinated approach to all assurance activities.											
				ensure that the combined assurance is received is appropriate to address all the significant risks facing the company.											
				monitor the relationship between the external assurance providers and the company.											
				The audit committee should be an integral component of the risk management process.											
				The charter of the audit committee should set out its responsibilities regarding risk management.											
				The audit committee should specifically have oversight of:											
				financial reporting risks;											

Addendum M: ERM implementation assessment tool - risk assurance checklist

Theoretical frameworks		Building blocks	Best practice requirements		Proposed deliverables		Building Block	Responsi- bility	Risk Assurance				Corrective Actions		
Deming cycle	Weisbord organisational design model		Level 1	Level 2	Purpose	Deliverables			YES	Not started	In process	Done	Activities	Responsibility	Target Date
Plan	Helping mechanisms, Relationships, Rewards	IV. Develop the risk infrastructure.	Committees: the board should delegate certain functions to well-structured committees but without abdication its own responsibilities.	internal financial controls;	To formalise decision making structures, escalation protocol & identify risk stakeholders.	Audit committee charter	IV	CAE							
				fraud risks as it relates to financial reporting; and											
				IT risks as it relates to financial reporting.											
				The audit committee should also:		Combined assurance committee terms of reference	IV	CAE							
				ensure that a combined assurance model is applied to provide a coordinated approach to all assurance activities											
				ensure that the combined assurance is received is appropriate to address all the significant risks facing the company.											
			Models & tools: the organisation's processes, methods and tools to be used for managing risk			Risk specific committee terms of reference e.g. Fraud risk committee	IV	CRO							
					To assess and decide on standardised tools that should be used across the organisation.	Risk identification tools	IV		1						
						Risk analysis tools	IV		1						
						Risk evaluation tools	IV		1						
						Risk response tools	IV		1						
						Risk monitoring tools	IV		1						
						Risk reporting tools	IV		1						
						Risk quantification models	IV		1						
			Templates: standardised recording, reporting and assessment templates		To standardise policy, framework, recording, reporting and assessment templates.	Examples:									
						Risk management plan	IV		1						
						Risk communication plan	IV		1						
						Stakeholder maps	IV		1						
						Stakeholder register	IV		1						
						Risk register	IV		1						
						Risk improvement report	IV		1						
						Integrated assurance dashboard	IV		1						
						Integrated report	IV		1						
						Risk self-assessments	IV		1						
						Stewardship report	IV		1						
						Recording process	IV		1						
						Risk acceptance form	IV		1						
						Risk retirement form	IV		1						
						Reporting dashboards	IV		1						
						Reporting scorecards	IV		1						
			Processes: documented processes and procedures.		To embed risk management in all the organisation's practices and processes in a way that it is relevant, effective and efficient.	Common risk language	IV		1						
						Risk owners matrix	IV	CRO							
						Strategic planning process	IV		1						
						Business planning process	IV		1						
						Financial planning process	IV		1						
						Change management process	IV		1						
						Quality assurance process	IV		1						
						Risk management process	IV		1						
			Systems: information and knowledge management systems		To select the most appropriate risk management systems.	Risk & incident escalation process	IV		1						
						External audit process	IV	CAE							
						Performance management process	IV	CHRO							
						Risk recording	IV		1						
						Risk reporting	IV		1						
						Risk monitoring	IV		1						
						Risk review	IV		1						

Addendum M: ERM implementation assessment tool - risk assurance checklist

Theoretical frameworks		Building blocks	Best practice requirements		Proposed deliverables		Building Block	Responsi- bility	Risk Assurance				Corrective Actions		
Deming cycle	Weisbord organisational design model		Level 1	Level 2	Purpose	Deliverables			YES	Not started	In process	Done	Activities	Responsibility	Target Date
Do	Leadership, Structure, Relationships, Helping Mechanisms, External environment	V. Implement the ERM program.	Implementing the framework for managing risk.	Define the appropriate timing and strategy for implementing the framework;	To establish a time line for risk management activities.	Risk management plan (calendar)	V		1						
						Critical path analysis for key dependencies	V	CRO							
				Apply the risk management policy and process to the organisational processes;	To embed risk management in all the organisation's practices and processes in a way that it is relevant, effective and efficient.	Common risk language	V		1						
						Risk owners matrix	V	CRO							
						Strategic planning process	V		1						
						Business planing process	V		1						
						Financial planning process	V		1						
						Change management process	V		1						
						Quality assurance process	V		1						
						Risk management process	V		1						
						Risk & incident escalation process	V		1						
						Performance management process	V	CHRO							
				Comply with legal and regulatory requirements;	To communicate risk related compliance requirements.	Legal, regulatory & best practice compliance register (pertaining to risk)	V		1						
				Ensure that decision making, including the development and setting of objectives, is aligned with the outcomes of risk management processes;	To encourage a risk mind-set for decision making.	Risk appetite statements	V	CRO							
						Risk tolerance levels	V	CRO							
						Strategic plan	V		1						
				Hold information and training sessions; and	To create a common risk language, improve risk awareness and encourage risk based decision making.	ERM framework & policy	V		1						
						Risk awareness gap analysis	V	CRO							
						Risk maturity assessment	V	CRO							
						Risk awareness strategy & -plan	V	CRO							
					To ensure that the risk management framework remains appropriate.	Risk facilitation sessions	V		1						
			Implementing the risk management process.	Step 1: Communication and consultation with external and internal stakeholders should take place during all stages of the risk management process.	To identify the internal and external stakeholders for the organisation / division / department / project.	Stakeholder analysis	V		1						
					To identify the most appropriate communication tools and establish timelines.	Risk communication plan	V	CRO							
					To ensure that the right information reaches the right people at the right time.	Risk reports e.g. stress tests, risk & control self-assessments, incident reports, risk treatment plans, key risk indicator reports.	V	CRO							
				Step 2: Establish the context (Know your organisation / division / department / project / risk type)	To describe the UNIQUE context for the risk management project.										
						External environment mind map	V	Risk Owners							
						External stakeholder register	V		1						
						External stakeholder map	V		1						
						Internal value chain mind map	V	Risk Owners							
						Internal stakeholder register	V		1						
						Internal stakeholder map	V		1						
						Standardised risk management context (refer to building block III)	V		1						
						Standardised risk criteria (refer to building block III)	V		1						
				Step 3: Risk identification	Process of finding, recognising and describing risks.	Key / Principle / Strategic risk register	V	Risk Owners							
						Divisional / departmental / business unit risk register	V	Risk Owners							
						Emerging risk register	V	CRO							
						Risk library	V	CRO							
				Step 4: Risk analysis	Process to comprehend the nature of risk and to determine the level of risk (e.g. high, medium, low).	Key / Principle / Strategic risk register - risk ratings applied	V	Risk Owners							
						Divisional / departmental / business unit risk register - risk ratings applied	V	Risk Owners							
						Root cause analysis	V	Risk Owners							
				Step 5: Risk evaluation	Process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable.	Key / Principle / Strategic risk profile - risk ratings + current controls applied & risk owners identified	V	Risk Owners							
						Divisional / departmental / business unit risk register risk ratings + current controls applied & risk owners identified	V	Risk Owners							
				Step 6: Risk response	To identify the most appropriate risk treatment for the most significant risks.	Controls library	V	CRO							
						Risk response plans / Action plans	V	Risk Owners							
						Risk response options	V	Risk Owners							

Addendum M: ERM implementation assessment tool - risk assurance checklist

Theoretical frameworks		Building blocks	Best practice requirements		Proposed deliverables		Building Block	Responsi- bility	Risk Assurance				Corrective Actions			
Deming cycle	Weisbord organisational design model		Level 1	Level 2	Purpose	Deliverables			YES	Not started	In process	Done	Activities	Responsibility	Target Date	
Check	Rewards	VI. Monitor and review the ERM program.	Monitoring activities by the Board	The board should ensure continual risk monitoring by management	To ensure proper risk oversight.	Risk governance framework	VI		1							
				The board should ensure that effective and continual monitoring of risk management takes place.	To reduce role confusion and provide clear guidelines for risk monitoring.	Risk management plan (monitoring roles and responsibilities)	VI		1							
				The responsibility for monitoring should be defined in the risk management plan.	To periodically measure progress against, and deviation from, the risk management plan.	Status report on risk management plan implementation	VI	CRO								
			Review activities by the Board	The board should comment in the integrated report on the effectiveness of the system and process of risk management.	To periodically review whether the risk management framework, policy and plan are still appropriate, given the	Integrated report (risk and opportunities section)	VI	CRO								
				The board should ensure that effective and continual monitoring of risk management takes place.	To periodically measure progress against, and deviation from, the risk management plan.	Risk management plan implementation status report	VI	CRO								
				The board should review the implementation of the risk management plan at least once a year.	To periodically review whether the risk management framework, policy and plan	Risk improvement report	VI	CAE								
						Internal audit report	VI	CAE								
				The performance of the committee should be evaluated once a year by the board.	To ensure effectiveness and efficiency with regards to committee activities.	Board risk committee performance evaluation	VI	Company Secretary								
				Monitor the risk management framework	The board should monitor that risks taken are within the tolerance and appetite levels.	To ensure compliance with the risk appetite framework.	Risk appetite status report	VI	CRO							
			To ensure compliance with the risk tolerance levels.			Risk tolerance status report	VI	CRO								
			Measure risk management performance against indicators, which are periodically reviewed for appropriateness;		To measure risk management performance against indicators, which are periodically reviewed for appropriateness;	KRI performance report	VI	CRO								
			Periodically measure progress against, and deviation from, the risk management plan;		To periodically measure progress against, and deviation from, the risk management plan.	Risk management plan implementation status report	VI	CRO								
			Report on risk, progress with the risk management plan and how well the risk management policy is being followed;		To report on risk, progress with the risk management plan and how well the risk management policy is being followed.	Risk management policy compliance report	VI	CCO								
						Deviations from risk management policy report	VI	CCO								
			Monitor the level of risk awareness		To track the improvement of risk awareness.	Risk culture surveys	VI	CRO								
			Review the risk management framework	Periodically review whether the risk management framework, policy and plan are still appropriate, given the organizations' external and internal	To periodically review whether the risk management framework, policy and plan are still appropriate, given the organisations' external and internal context.	Risk improvement report	VI	CAE								
						Internal audit report	VI	CAE								
						Risk calendar	VI		1							
						Risk improvement report	VI	CAE								
				Communicate and consult with stakeholders to ensure that its risk management framework remains appropriate.		Subject matter expert gap analysis	VI		1							
						Internal audit reports	VI	CAE								
						Risk calendar	VI		1							
						ISO 9000 reports	VI	CPO								
				Review the effectiveness of the risk management framework.		Internal audit reports, risk committee effectiveness, qualitative conversations, risk appetite and risk tolerance level breaches, signed letters of representation.	VI	CAE								
			Monitor the risk management process	Ensuring that controls are effective and efficient in both design and operation.	To ensure that controls are effective and efficient in both design and operation.	Subject matter expert gap analysis	VI		1							
						Combined assurance reports	VI	CAE								
				Risk profile status reports		VI		1								
				Internal audit reports		VI	CAE									
				External audit reports		VI	CAE									
			Identifying emerging risks.	To identify emerging risks in the organisation's internal value chain and external environment.	Emerging risk register	VI	CRO									
			Review the risk management process	Analysing and learning lessons from events (including near-misses), changes, trends, successes and failures;	To analyse and learn lessons from events (including near-misses), changes, trends, successes and failures.	Variance and trend analysis	VI	CRO								
						Post mortem sessions	VI	CRO								
						Environmental scanning	VI	CRO								
						Risk reconciliation reports	VI	CRO								
						Post loss analysis	VI	CRO								

Addendum M: ERM implementation assessment tool - risk assurance checklist

Theoretical frameworks		Building blocks	Best practice requirements		Proposed deliverables		Building Block	Responsi- bility	Risk Assurance				Corrective Actions		
Deming cycle	Weisbord organisational design model		Level 1	Level 2	Purpose	Deliverables			YES	Not started	In process	Done	Activities	Responsibility	Target Date
Adjust	Leadership, Purposes, Structure, Relationships, Rewards, Helpful mechanisms, External environment	VII: Continual improvement of the ERM program.	The board should receive assurance regarding the effectiveness of the risk management process	Management should provide assurance to the board that the risk management plan is integrated in the daily activities of the company.	To inform the relevant committees and risk stakeholders of the level of assurance provided by assurance providers.	Combined assurance report.	VII	CAE							
						Risk reports to various committees	VII		1						
						Risk maturity assessment	VII		1						
						Benchmarking assessments (peer reviews & best practice)	VII		1						
				Internal audit should:	To periodically review whether the risk management framework, policy and plan are still appropriate, given the organisations' external and internal context;										
				provide a written assessment of the effectiveness of the system of internal controls and risk management to the board.		Risk improvement report	VII	CAE							
				detect changes in the external and internal context, including changes to risk criteria and the risk itself which can require revision of risk treatments and priorities; and		Internal audit report	VII	CAE							
				obtaining further information to improve risk assessment.		Risk improvement report (List of internal, external, risk management process & risk criteria context changes)	VII	CAE							
						Risk improvement report (risk assessment process & methodology)	VII	CAE							

Source: Researcher's own compilation