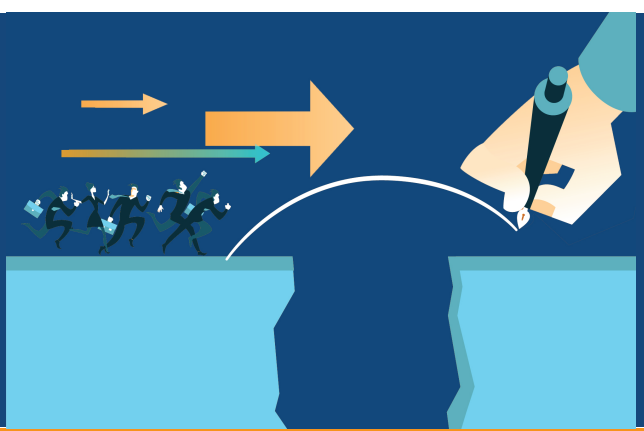
ISO 31000 RISK
Certified System

COMPASS
-ASSURANCE SERVICES-

ISO 31000:2009 RISK MANAGEMENT PRINCIPLES AND GUIDELINES CHECKLIST



COMPASS ASSURANCE SERVICES PTY LTD

NOTE: THIS IS A SIMPLIFIED SUMMARY OF THE REQUIREMENTS OF ISO 31000:2009 RISK MANAGEMENT PRINCPLES AND GUIDELINES – REQUIREMENTS FOR THE SPECIFIC PURPOSE OF HELPING ORGANISATIONS UNDERTAKE A PRELIMINARY CHECK OF THEIR READINESS FOR AN ISO 31000:2009 RISK MANAGEMENT PRINCPLES AND GUIDELINES ASSESSMENT.

COMPASS
-ASSURANCE SERVICES-

ISO 31000 RISK
Certified System

ISO 31000:2009 RISK MANAGEMENT – PRINCIPLES AND GUIDELINES CHECKLIST

Use this self-assessment checklist to show how close you are to being ready for an ISO 31000:2009 certification assessment from Compass Assurance Services and which processes you still need to implement in your organisation. The checklist is laid out in sections which align with the requirements of the standard.

Mark your answers ✓ for yes as you work through the checklist to identify which processes are in place or areas which might need attention.

NOTES

4. Framework

4.2 Mandate and Commitment	
Have we: (a) defined and endorsed a risk management policy (b) determined risk performance indicators (c) aligned risk objectives and indicators to organizational objectives and indicators (d) ensured legal and regulatory compliance	
4.3 Design of Framework	
4.3.1 Organization and its context In designing our risk framework have we: (a) evaluated external context (b) evaluated internal context	
4.3.2 Risk Policy Does our policy include: (a) rationale for managing risk (b) accountabilities (c) how conflict of interest is dealt with (d) links between organizations objectives and risk policy (e) commitment to resource risk management (f) how risk performance managed, measured and reported (g) commitment to review and improve the policy	

4.3.3 Accountability Have we established accountability, authority and competence for managing risk? Do we (a) identify risk owners (b) identify responsibility for our framework (c) identify risk responsibilities (d) establish performance measures and reporting and escalation processes (e) ensure appropriate levels of recognition	
4.3.4 Integration into Organisation Processes Is risk management embedded into our practices and processes in a way that is relevant, effective and efficient?	
4.3.5 Resources Have we allocated appropriate resources for risk management? Including a consideration of: (a) people (b) organizational processes, methods and tools (c) documented processes and procedures (d) information and knowledge management systems (e) training	
4.3.6 Internal Communication and Reporting Have we established internal communication and reporting mechanisms for risk management?	
4.3.7 External Communication and Reporting Have we determined and implemented how we will communicate with external stakeholders?	

4.4 Implementing Risk Management	
4.4.1 Implementing the Framework In implementing our framework can we show we have: (a) applied risk management policy to organizational processes (b) complied with legal and regulatory requirements (c) ensured decision making is aligned with risk management processes (d) held information and training sessions (e) communicated and consulted with stakeholders	
4.5 Monitor and Review	
Do we: (a) measure risk management performance against indicators (b) measure progress against risk management plans (c) review whether the framework and policy are still appropriate (d) report on risk (e) review the effectiveness of the framework	
4.5 Continual Improvement	
Do we continually improve the risk policy, framework, plans?	

5. Process

5.1 General	
Is the risk management process: (a) an integral part of management (b) embedded in culture and practices (c) tailored to our organisation	

5.2 Communication and Consultation	
Can we demonstrate communication and consultation with external and internal stakeholders at all stages of the risk management process?	
5.3 Establishing Context	
Can we demonstrate we have considered internal and external context, factors and how they relate to the scope of the particular risk management process?	
5.3.5 Defining Risk Criteria	
Have we defined the criteria to be used to evaluate the significance of risk?	
5.4 Risk Assessment	
5.4.2 Risk Identification	
Have we identified sources of risk, areas of impact and their causes and potential consequences?	
Have we applied risk identification tools and techniques?	
Do we use people with appropriate knowledge for risk identification?	
5.4.3 Risk Analysis	
Do we have processes to consider causes and sources of risks, their consequences and the likelihood of the consequences to occur?	
5.4.4 Risk Evaluation	
Do we compare the level of risk found during analysis process (5.4.3) to our risk criteria to determine the need for treatment or further analysis?	
5.5 Risk Treatment	
5.5.2 Selection of Risk Treatment Options	
Do we have processes for selecting treatment options that consider stakeholders, legal, regulatory and context?	
Do we have processes to identify new risks introduced through treatment?	
Does the treatment plan identify priority order for risk treatments?	

5.5.3 Preparing and Implementing Risk Treatment Plans	
Do we document how our risk treatment will be implemented?	
Do we include	
(a) reasons for selection and expected benefits	
(b) responsibilities	
(c) proposed actions	
(d) resource requirements	
(e) performance measures	
(f) reporting and monitoring requirements	
(g) timing	
5.6 Monitoring and Review	
Have we included regular checks or surveillance in our risk processes at all levels?	
Have we defined responsibilities for monitoring and review?	
Do we check progress of risk treatment plans?	
Do we report results of monitor and review?	
5.7 Recording	
Are our processes traceable?	
Have we retained suitable records?	