QAO risk management maturity model

QAO developed a risk management and maturity model after extensive research into current developments in the public and private sectors in Australia and overseas. It outlines five levels of maturity across six key attributes of risk management and is a useful framework for self-assessment. Clients are encouraged to consider their internal risk management practices against the various attributes of risk as an internal control and discuss their self-assessments with their QAO engagement leader.

QAO most recently used the model in the *Results of audit: education sector entities 2015* (Report 18: 2015-16) where we assessed the maturity of the universities' risk management practices.

Leadership — Senior management's commitment and approach to risk management as a key governance mechanism				
Basic	Developing	Established	Integrated	Optimised
Senior management demonstrates awareness of the need to appropriately manage risk, however does not commit dedicated resources to risk management. There is no relationship between risk management activities and senior management's decision making. Senior management approaches risk management reactively, with limited proactive risk assessments.	Senior management reviews the entity's risk management framework on an ad hoc basis, and provides input into the approaches adopted for managing risks. Senior management commits some resources to risk management. Risk management activities are aimed at the entity's compliance with laws and regulations, but are not linked to strategic and operational decision-making. Senior management focusses on risk avoidance, not managing new opportunities. When managing risk, there is limited emphasis on long term business and planning objectives.	Senior management promotes the entity's risk management framework across the entity. Senior management makes explicit its risk appetite, tolerance to risk and capacity for risk taking. Ownership of risk management is vested in a senior person and is appropriately resourced. Risk management processes include the identification of opportunities. There is some evidence of risk management being factored into senior management's decision-making processes, but risk management is not formally embedded.	Senior management demonstrates ongoing commitment to risk management activities and their ongoing development across the entity. Senior management is proactive in ensuring that risk management is adequately resourced. Senior management encourages managed risk taking associated with innovative approaches to the entity's activities and to new business opportunities. Senior management considers risk as part of its strategic planning process.	Senior management drives the integration of risk management at both strategic and operational levels. Risk is incorporated into all senior management decision making and when setting objectives for the entity. Senior management commits to continual improvement in its approach to risk management and has adopted relevant leading practice.

People and accountability — How well the entity's responsibility structures support risk management

Basic	Developing	Established	Integrated	Optimised
Some staff are aware of the need to assess and manage risk. These staff have basic knowledge of risk management principles. There is no central coordination of risk management for the entity.	Key staff are provided training and guidance material to assist in the management of risk. A central person/team leads risk management, but there is little input from across the entity more broadly.	Key staff have the skills and knowledge to manage risk effectively. Staff are given clear responsibility for managing risk, but there is no formal accountability mechanisms to monitor how risk management is being applied. Staff are engaged from across the entity in risk management activities and there is representation from all major business units.	Most staff have relevant skills and knowledge to manage risk effectively. Regular training is available to staff to enhance their risk management skills. Staff are accountable for managing risk and their roles in risk management have been clearly articulated to them. There is ongoing specialist risk management support available for staff. A central risk management team has formal risk management responsibilities.	All staff have responsibility for risk management and see it as a part of all the entity's processes. Responsibility for risk management is incorporated into duty statements, performance agreements and annual performance assessments. A central risk management team has been established and has developed leading practice methodologies to support ongoing risk management activity.

Process integration — The depth of integration of risk management in key business processes, practices and systems

Basic	Developing	Established	Integrated	Optimised
Risk assessment processes are stand-alone activities and are not supported by established policy or procedures. Risk management activities are managed manually or in simple tools that are developed in isolation of the entity's operational context.	Risk management processes are being developed but they are applied inconsistently across the entity and are not integrated into key business processes and planning.	Risk management processes have been implemented in key areas. Specific risk assessments have been undertaken in areas of potential high exposure (e.g. fraud risk assessments).	Standardised risk management processes are an integral part of the entity's core operations. The entity's systems have the capacity to meet the ever-changing business and risk environment.	Risk management strategies and processes are integrated as part of all business processes. Risk management activities are managed within sophisticated systems that highlight exceptions, report risk events and prompt staff for remedial action when required.

Response — The processes in place to ensure treatments are effective				
Basic	Developing	Established	Integrated	Optimised
Risk treatments have been identified for some risks but there is no formal mechanism for assessing their effectiveness.	Risk treatments are assessed to ensure that risks are managed in accordance with the entity's risk appetite and risk framework.	Risk treatment plans include alternative courses of action and cost/benefit analyses of treatments. There is a formal process of monitoring treatments.	Responses to risks are commensurate to the level of risk, including risk appetite and tolerances to risk defined across the entity (risks are not under or over controlled). Responses address the root cause of risks. Treatments are assigned to a specific risk owner.	Exception reports highlight instances where risks fall outside the maximum tolerances. There is an independent review of all risks and treatment plans to ensure consistent treatment. The results of an assessment of treatment effectiveness are shared across the entity.

Monitoring — The extent of ongoing activity to monitor the entity's risk profile				
Basic	Developing	Established	Integrated	Optimised
Risk policies and basic risk registers are provided to senior management for review on an ad hoc basis, but no risk performance monitoring reports are provided to senior management. Risk is a standing agenda item for the risk management committee.	Senior management review and discuss risk as part of management meetings on a regular basis. Risk performance monitoring reports are provided to senior management.	Risk is a standing agenda item for executive management meetings. Concise reports (backed up by more detailed information as required) highlighting exceptions are provided to allow senior management to focus on issues that require attention.	Senior management routinely reviews and discusses the risks that could cause the greatest impact on the entity and on achieving its strategic objectives. These discussions are supported by integrated risk, performance and financial information linked to the entity's objectives. There is a process for monitoring changes to the external environment that may impact the entity's risk profile, but the process is not systematized.	Systems are in place to support the ongoing review of the entity's risk management strategies, including key risk performance indicators that allow management to monitor the effectiveness of risk management activities. The entity's risk management framework is regularly benchmarked to external best practice. There is ongoing environmental scanning to identify trends and external factors that may impact the entity.

Achieving outcomes and innovation — The entity's culture supports well-managed risk taking to foster improvements and innovation				
Basic	Developing	Established	Integrated	Optimised
Focus is only on achievement of business objectives. There is minimal or no focus on the benefits of effective risk management and no recognition of its linkage to innovation.	The risk assessment process is used to identify new opportunities and improve business practices, but this happens in an ad hoc manner.	The entity's culture supports open discussion of lessons learnt and supports managed risk taking to foster improvements and innovation.	Proactive procedures and approaches are in place to maximise identification of opportunities in line with the entity's risk appetite and tolerance levels. Risk management contributes to improved and innovative service delivery and outcomes.	The entity has a record of maximising opportunities and innovation through effective and well managed risk taking. Risk management drives improved service delivery and outcomes.

Contact

Queensland Audit Office:

07 3149 6000

qao@qao.qld.gov.au

www.qao.qld.gov.au

PO Box 15396, City East QLD 4002

Join us on LinkedIn

Research material

COSO Integrated Framework, Framework and Appendices May 2013
ISO 31000:2009
Australian National Audit Office, Heads of Cultural Organisations Meeting, Risk Management, 15 December 2005
National Audit Office, Report by the Comptroller and Auditor General, Supporting Innovation: Managing risk in government departments, August 2000
National Audit Office, Good Practice Managing risks in government, June 2011
HM Treasury, The Orange Book: Management of Risk – Principles and Concepts, October 2004
HM Treasury, Risk management assessment framework: a tool for departments, July 2009
Queensland Government, Financial Management Framework: A Guide to Risk Management, July 2011
APRA Prudential Practice Guide: SPG 220 – Risk Management, July 2013
Auditor General Victoria, Good Practice Guide, Managing risk across the public sector, 2004
Department of Treasury and Finance, Victorian Government Risk Management Framework, March 2001
Australian Government, Comcover, Better Practice Guide, Risk management, June 2008
PWC A practical guide to risk assessment, December 2008
Australian National Audit Office, Better Practice Guide, Innovation in the Public Sector, December 2009
COSO Enterprise Risk Management, Understanding and Communicating Risk Appetite, Thought Leadership in ERM
Crowe Horwarth Risk: Appetite & Tolerance, 2011