

## RISK MANAGEMENT

One of the key components of The Audit Office of New South Wales' Governance Lighthouse is risk management.

Risk is the effect of uncertainty on objectives. Risk Management refers to the architecture (principles, framework and process) for managing risks effectively.


The Audit Office Risk Management Maturity Assessment Toolkit is based on the principles and guidelines of the International Standards on Risk Management AS/NZ ISO 31000 : 2009 Risk Management, the NSW Treasury Policy Guideline TPP 12-03 : Risk Management Toolkit for the NSW Public Sector, TPP15-03: Internal Audit and Risk Management Policy for the NSW Public Sector and the Committee of Sponsoring Organisations of the Treadway Commission's (COSO) Enterprise Risk Management Integrated Framework.

### Assessment of Risk Management Maturity

Levels of Risk Management Maturity

Maturity Matrix Rating Scale	
Maturity Rating	Description
<b>Initial</b>	There is no or minimal awareness of the importance of risk management and there are no processes in place across the entity. Risk management is usually left to the individual and performed on an adhoc basis. Risk management is more reactive than proactive.
<b>Inconsistent</b>	There is organisational awareness of the importance of risk management. There are some formal processes in place for a few risks. There is limited standardisation of risk management processes and risk management is conducted inconsistently across each risk and across each business unit.
<b>Consistent - Designed</b>	An enterprise risk management framework exists covering all major risks. Standardised risk management principles are defined and documented, basic training conducted. Consistent risk management processes with communication and accountability exist throughout the business but not all processes have been fully implemented.
<b>Consistent - Implemented</b>	Enterprise risk management is fully implemented across the business, consistently applied and used in decision making and day to day management. Risk management processes are measured, evaluated and fed back into continuous improvement. Principles and policies are implemented and aggregated reports are prepared and reported to those charged with governance. Risk management is proactive. Key Risk indicators are collected and monitored consistently.
<b>Optimised</b>	Risk management is fully addressed and embedded into day to day management. Sophisticated and advanced risk management processes are used for all major risk types. Risk management is used as a key value driver supporting decision making and pursuit of opportunities. Risks, including emerging risks are proactively identified and monitored through key risk indicators and predictive risk analytics

# Risk Management Maturity Assessment Tool

		Assessment Criteria	Strategy and governance	Process	Systems & Intelligence	Monitoring and Review	Culture
 <p><b>Maturity</b> <b>Scale</b></p>	<b>Optimised</b>	Leading edge, aligned risk management and mitigation strategies in place. Accountability and responsibilities for risk management functions clearly defined. Audit and Risk Committees committed to regular assessment of the risk management function. Three lines of defence articulated and implemented. Risk management incorporated in daily operations. Risk appetite and tolerance levels communicated.	Loss Prevention and risk management processes are standardised and integrated organisation-wide. Proactive audit and program compliance enforcement exists. Formal and comprehensive program of stress testing is conducted regularly on all key risks. Risk management process is auditable. Key Risk Indicators (KRIs) are used extensively across the organisation. Best practices achieved for risk management.	Highly automated and reliable information sharing capability organisation-wide enabling quick response, remediation and mitigation of risk incidents/issues. Fully integrated and advanced enterprise risk management (ERM) system. Use of sophisticated tools and data collection to quantify risks. Predictive analytics used extensively across the risk management framework.	Aligned strategic methodologies that emphasise continuous improvement exist. Fully implemented formal escalation process for all key risks across the organisation on a real time basis is fully implemented and working. Risk appetite delegations exist for all levels of the agency and used as a basis for risk acceptance or rejection. Governing Board and executive management oversight and monitoring visible.	Risk profiles linked to corporate and strategic goals. Governing Board and Executive management leading in risk management consciousness. Leading in key risk indicators which are related to strategic and corporate goals. There is a clear ownership of all risks and controls. Risk is considered an opportunity as well as a threat. Risk management is seen as an enabler. Staff have some component of their personal KPIs related to risk.	
	<b>Consistent-Implemented</b>	Strategic and risk management plans and policies drive actions in all levels of the organisation. There is organisation buy-in of risk management procedures. Chief Risk Officer or equivalent appointed.	Risk management processes standardised and enforced at all levels. Stress testing used in risk quantification and contingency planning. Risk management practices deliverables sustained. KRIs used as an early warning system.	A single main ERM system. High quality reporting of risk incidents and issues available through enabling technology solutions depending on the size and needs of the organisation. Improved controls and compliance reporting available for resource deployment and decision making.	Targeted and specialised programs focusing on elimination of root causes of loss/risk incident implemented. Exception reporting and predictive analysis improves resource allocation.	The Governing Board has a specific focus on risk management at all audit and risk committee meetings. Risk incidents are dealt with consistently. Risk management is an explicit part of business planning. Effective education and communication strategies integrated into organisations' governance and risk programs.	
	<b>Consistent-Designed</b>	Annual risk management plans created. Risk appetite statement and risk tolerance established. There is a well articulated risk management methodology together with relevant policies. No specific procedures exist. The three lines of defence are recognised across the organisation.	Risk and risk components are defined. Risk management processes defined at the business unit or division level. Aggregated KRI reports are produced. KRIs include some leading indicators.	Some capacities to track key milestones and compliance. coverage of data is not extensive and not real time. Some availability of risk incidents, issues and trend reports. Risk analytics process not fully implemented across the organisation.	Formalised risk monitoring and review methodologies allow improved analysis and response for critical decision making. Effective system of formal risk incident reporting and tracking and data repositories. Formal escalation process for risk related matters exist but not fully operational.	Systematic risk monitoring. The ERM framework includes the requirement for all risks and controls to have an assigned owner. Most employees are neutral regarding the value of risk management as it is not fully understood or practiced. Process of including risk related staff KPIs not fully embedded.	
	<b>Inconsistent</b>	There is a high level risk management methodology articulated. There is a separate audit function but no separate risk management function. Risk appetite statement is articulated qualitatively and no reporting exists.	Risk management processes and control management applied inconsistently. Some use of risk management and control assessment templates and risk register. Controls testing on an ad hoc basis.	A range of systems used with minimum tailoring capability. No integration of risk systems. Reports produced from various systems in excel and word. Limited analytics on historical data. Compliance and performance measured manually on annual basis.	Simple tools used inconsistently. Risk management often captured on spreadsheet and risk control strategies reliant on "word of mouth" delivery. Some areas of the organisation use risk incidents and issues to develop actions but are applied inconsistently.	The Governing Board discusses some risk matters but there is no specific agenda item for risk. Some risks do not have specific owners. Poorly communicated, risk management may be misunderstood and taken as proxy for conservatism and risk avoidance. Some risk related KPIs while most are qualitative.	
	<b>Initial</b>	Risk not addressed as a strategic opportunity. The organisation provides little risk management direction.	No standard Risk Management processes and procedures. No definition formalised and communicated to staff. Lack of operational controls leads to uncontrolled risk loss. Risk management often ad-hoc and reactive. No formal KRI process to track current levels of risk.	Critical information not available. No capacity to track risk management and exposure through incidents and events. No capacity to evaluate operational controls and compliance. Compliance and performance measured sporadically. Manual reporting with limited data integrity. No capability to conduct analytics.	Governing Board and senior management have no; or a very small level; of involvement in risk related matters. No risk compliance or performance monitoring methodology. No process for continuous improvement for risk management in the organisation. Unable to achieve predictive analysis.	No formal risk management and mitigation strategy. There is no clear ownership of risks and controls. Risk management serves to achieve organisational compliance. Risk management is considered a hindrance and an overhead.	