Treasury Risk Maturity Assessment Tool

Definitions

Attributes

(NSW Agency) Risk Operating Model	Definitions
INTEGRATION	**The integration** supports the application of risk management in the agency
Strategy and Business Planning	**Strategy & business planning** considers the key risks and their management as an integral part of developing the corporate and business planning process based on the external business environment.
Projects	**Projects** considers the key risks and their management as an integral part of delivering major projects and change initiatives that support the delivery of an agency's priorities.
Programs & Operational Performance	**Programs & operational performance** considers the monitoring of key risks and their management over time relative to defined tolerances to support the delivery of the agency's operations and government programs. This also includes the key risks related to managing the budget and resource planning (including capital expenditure, operating expenditure and associated assumptions)
Reporting and Communication	**Reporting and communication** considers the ongoing dialogue across the agency that support the flow of risk related data information and insights to those responsible and account for the management of key risks.
ENABLERS	**The enablers** support the risk identification, analysis, evaluation, treatment, monitoring, reporting and communication process.
Methodologies & Tools	**Methodologies and tools** consider the common approach to supporting the application of risk management framework and processes across the agency.
Data & Information	**Data and information** considers the data and information required by the agency to support the application of the risk management framework / processes on an ongoing basis and the systems to support the efficient and effective collection of data to support risk based decisions.
Capability & Training	**Capability and training** considers the risk capability and knowledge and experience of resources across the agency. Increasing capability assists with improving the risk management framework / process and manage key risks.
FOUNDATIONS	**The foundations** support the tone and structure of the Risk Operating Model
Risk Governance	**Risk governance** refers to the agency framework of rules, responsibilities, systems and processes by which risk management is structured in an agency. This also includes risk tolerance, which is the maximum level and type of risk the agency is willing to take or accept to deliver their objectives. Risk governance could include frameworks, policies, procedures and roles & responsibilities.
Risk Culture	**Risk culture** is the set of encouraged and acceptable behaviours, discussions, decisions and attitudes towards taking and managing risk in an agency.

Maturity Level

Maturity Level	Distinguishing Factors	Capability Description
Advanced	Continuously Improving Process	Risk management is optimised, delivers to stretch objectives and is subject to continuous improvement
Embedded	Predictable Process	Risk management is formally defined, predictable, consistently delivered and meets defined objectives
Systematic	Standard, Consistent Process	Risk management is proactively managed, supported by defined process and is stable and measurable
Repeatable	Disciplined Process	Risk management is established and repeatable, documentation is limited and continued reliance on individuals
Fundamental	Un-coordinated	Risk management is unpredictable, vague and highly dependent on individuals

NSW GOVERNMENT | Treasury

Treasury Risk Maturity Assessment Tool

Risk Maturity Matrix

		Maturity level				
Element	Attribute	Fundamental	Repeatable	Systematic	Embedded	Advanced
Foundations	Risk culture	There is limited or unclear accountability for risk management and key decisions only consider risk and reward on an ad-hoc basis. There is limited definition of the agency's desired risk culture and behaviours.	Risk culture is considered and communicated and there is an awareness of risk culture and the required behaviours to manage risks across the agency.	There is a defined approach to consider and manage risk culture across the agency. Risk behaviours that effectively manage risk to agreed tolerances are rewarded and poor behaviours managed. Drivers of the entity's risk culture are understood and reported on.	Executive decisions drive a positive risk culture and have early warning mechanisms in place to identify areas of poor behaviour. Key risks are owned by 1st line management and risk behaviour is directly linked to performance.	Executive management continuously improve culture through the operating model design, key decision making, performance management and effective communication. Collaboration on risk culture best practice occurs inter and intra agency.
	Risk governance	Key elements of risk governance are not defined, formalised, consistent or documented, nor repeatable. Positive risk outcome relies solely on well-intended individual efforts. Risk tolerance is considered on an ad-hoc basis and is not consistently applied across all risk classes.	Basic building blocks of risk governance are documented and roles and responsibilities for enterprise risk operating model elements are defined and agreed. Risk tolerance is understood for all material risks across the agency. Accountability for risk tolerance decisions and tolerances has been assigned.	Clearly defined risk governance procedures (including standard policies and procedures, roles & responsibilities) exist across the agency. Evaluation of risk governance is performed using relevant and appropriate key risk indicators. Proactive management of risk relative to tolerance by those accountable.	Policies and procedures are consistent across the agency and align to agency objectives. There are defined risk roles and responsibilities embedded in the organisational structures and risk is a core element of decision making and oversight of the agency. Early warning signals and data is monitored to allow changes to risk tolerance over time.	Risk governance practice is regularly reviewed and evolved by all those involved in risk management. Management and employees proactively review roles and responsibilities and take ownership for risk management at every level. All levels in the agency consider risk tolerance and dynamically determine risk responses.
Enablers	Capability & Training	Risk management depends on well-intended actions of individuals with limited 'risk management' capability. Risk roles, responsibilities and accountabilities are poorly defined and there is minimal training in risk management.	Risk is a required competency for specialised functions, and some formal risk management training may be offered to the wider organisation.	Standard risk management training is run for all staff with deeper training provided for specialists. All staff are expected to have a knowledge of risk management and apply it in their role.	The agency is recognised as employing experienced risk personnel with embedded knowledge & expertise in place. Risk training is provided in areas of emerging practice and comprehensive risk training is provided to all staff.	Risk management knowledge and skills are continuously upgraded and benchmarked against leading practice both in the NSW public sector and the corporate sector.
	Methodologies & Tools	No models / methodologies / tools used to support risk decision-making and heavy reliance upon key people and their instincts.	Simple risk models used for some risk decision making using measurement methods which are specified and documented.	Standardised risk models / methodologies consistently utilised for decision-making with defined measures of performance and process / risk variability. Evaluation and monitoring of risk management is performed.	Risk management uses reliable and proven models & methodologies for risk decision-making and utilises a range of risk tools to support a predictable and consistent risk management process. Evaluation of the effectiveness of the risk management framework and the management of risk by an agency is performed on a regular basis.	Enterprise-wide risk management methodologies and tools are consistently applied and are considered best in class. The agency is recognised as a leader in the field of risk management methodologies and tools.
	Data and Information	Data quality is inconsistent with limited confidence. Quality of risk information is low and therefore risk decisions are not based on quantitative evidence.	Some data collection undertaken that is used to evaluate and monitor risk on an ongoing basis. Stable set of data and information.	Standard suite of integrated risk data that supports consistent risk analysis across the agency allowing trend analysis and risk-based decision making.	Comprehensive set of data that allows dynamic risk management based on stable and high-quality data sets for all risk classes. The quality data enables agencies to identify lessons learnt and emerging risks and opportunities.	Advanced suite of analytics and data that enables dynamic risk management and monitoring with effective and intuitive dashboards based on a breadth and depth of high-quality data. Continuous development of data and analytics in line with leading practice.
Integration	Strategy & Business Planning	There is minimal focus on risk when developing or executing strategies or business plans. Where risk is considered it is inconsistently applied across the agency.	Risk is considered in strategies and business planning but is not consistently applied and is not consolidated across the entity.	Strategy setting and business planning consider risks in a consistent manner and document the responses.	Risk is integrated into planning and strategy across all business units and aligns to agency objectives. All key risk classes are considered when developing and implementing strategies and business planning.	Strategy and business planning process is dynamically sensitive to internal and external risk factors. Risk is considered on a consistent basis and aggregated to monitor changes to risk profiles over time.
	Projects	There is a minimal or ad-hoc consideration of project risks or the impact of projects on the risk profile of the agency.	Project risk accountability is assigned, and projects consider risk during project design and evaluation and throughout the project lifecycle.	A consistent and documented approach to risk management is applied to all projects. Ownership for project risk is understood and followed through.	Key project risks (e.g. interdependency, benefits management, staff impact, customer, budget, resourcing) are evaluated and combined to support risk-based decisions on a project and portfolio basis, covering both delivered and delivery risks.	Project portfolio is consistently evaluated for risks and interdependencies. Resourcing and funding are dependent on the effective risk management practices that assess all risk classes.
	Programs & Operational Performance	Program and process risk is not defined, formalised, consistent, documented, nor repeatable. Programs and process risk responses are reaction driven, unpredictable, and outcome relies solely on well-intended individual efforts.	Critical programs and processes have defined and documented financial and non-financial risk management procedures in place.	Defined, documented and consistent financial and non-financial risk management procedures are included in all programs & processes, including budgeting & resource planning.	Risk management is a critical input to program and operational performance and is considered a core competency. Programs and processes are dynamically risk assessed and developed in response to emerging risks.	Continuous benchmarking and improvement of how financial and non-financial risks are identified and managed is performed enterprise wide for all programs and processes. Proactive redirection of funding and resources occurs based on periodic monitoring of risk profile and assumption changes.
	Reporting & Communications	Reporting is sporadic, ad-hoc, and informal with reporting often incomplete, inaccurate, and untimely.	Risk reporting is performed with regular / actionable reports and key metrics identified based on a standard set of data.	Senior Management is comfortable with content and consistent format of risk reporting. Reporting identifies exceptions and "near misses".	Risk reporting uses dynamic risk measurements based on quantitative and statistically based data to allow responsive risk decisions to be made.	Fully developed & automated risk reporting supported by high-quality data and dashboards that are used to manage and monitor risks, and to proactively and dynamically drive continuous improvement in risk management across the business.