NSW GOVERNMENT | Treasury

September 2020

TPP

20-06

Treasury Risk Maturity Assessment Tool Guidance Paper

Preface

The **purpose** of the **Treasury Risk Maturity Assessment Tool** (Tool) is to support the improvement of risk management, culture and capability across the NSW public sector. The Tool provides agencies with a systematic, uniform approach for self-assessment that will allow agencies to measure risk maturity, identify areas to improve and communicate results to leadership teams (agency and cluster) and Audit and Risk Committees.

The **key benefits** of the tool include:

- helping agencies to assess their own maturity level
- identifying specific areas to improve risk culture and capability
- supporting whole of government improvements to risk management through a uniform tool and
- allowing agencies to compare their results over time.

The use of the Tool provides further assistance to agencies to meet their obligations under section 3.6 of the *Government Sector Finance Act 2018,* which requires the Accountable Authority (i.e. Secretaries and agency heads) "to establish, maintain and keep under review effective systems for risk management … that are appropriate systems for the agency." Refer to the below risk related policies and resources.

The **Risk Maturity Assessment Process** on page 5 explains how to conduct a risk maturity assessment using the **Risk Maturity Matrix** and supporting information. The accompanying **Spreadsheet** on the Treasury website enables agencies to apply this Guidance Paper to their agency and produce a summary of their risk maturity assessment. This includes presenting a current maturity state and a program of activities to reach the target maturity state.

The tool has been developed through a collaborative process sponsored by NSW Treasury. This involved collaboration from a working group[1] comprised of cluster and other key agency chief risk officers and risk managers, as well as input from Protiviti. These contributions are gratefully acknowledged.

Risk related policies and resources

The Tool supports agencies to meet their risk management requirements, based on the following foundational policies, standards and legislation:

- Internal Audit and Risk Management Policy for the NSW Public Sector (TPP15-03)[2] and supporting guidance:
  - Risk Management Tool kit for NSW Public Sector Agencies (TPP12-03a)
  - Risk Management Tool kit for NSW Public Sector Agencies (TPP12-03b)
  - Risk Management Tool kit for NSW Public Sector Agencies (TPP12-03c)
- AS ISO 31000:2018 Risk management – Guidelines
- *Government Sector Finance Act 2018*.

Michael Pratt AM
Secretary
NSW Treasury
September 2020

Note

General inquiries concerning this document should be initially directed to the:
Financial Management Governance & Analytics team, NSW Treasury - finpol@treasury.nsw.gov.au
This publication can be accessed from the Treasury's website www.treasury.nsw.gov.au

---

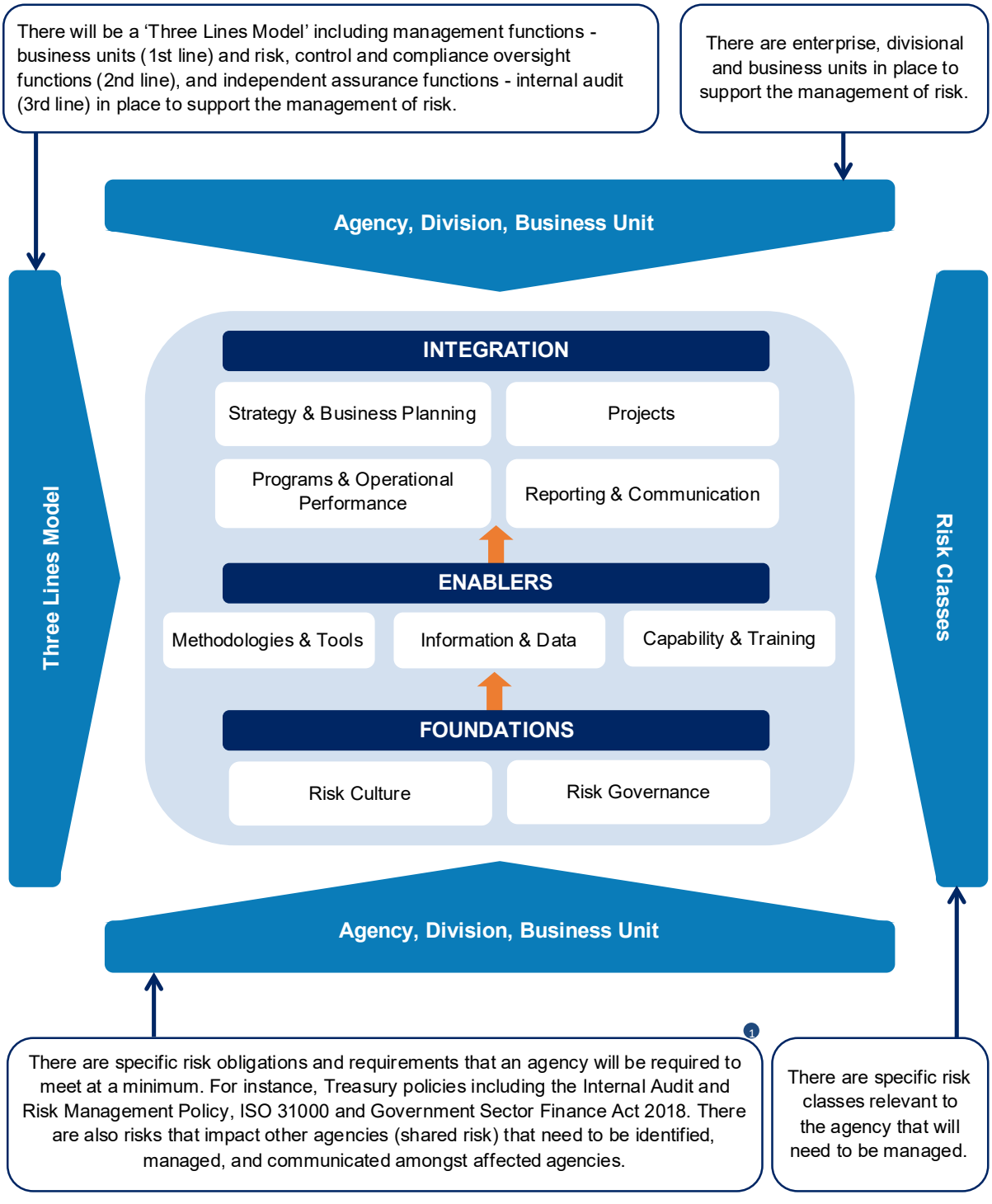
[1] The working group was drawn from the Enterprise Risk Management Community of Practice facilitated by icare.
[2] This policy is currently being revised and this link will be updated when the Internal Audit and Risk Management Policy for the General Government Sector (TPP20-XX) is issued.

Contents

NSW Agency Risk Operating Model

The Tool is based on the **NSW Agency Risk Operating Model** below which is the supporting methodology for the risk maturity assessment. It ensures that when users of the Tool (primarily agency risk management teams) conduct an assessment, all aspects contributing to the management of risk throughout an agency are considered.

NSW Agency Risk Operating Model



1 Note: The relevant risk management Treasury policies are listed above in 'risk related policies and resources.'

The Model demonstrates how agencies should consider the wider context of their agency when conducting a risk maturity assessment. This is through the outside sections of the Model reflecting the different aspects that contribute to managing risk including the minimum regulations and standards that apply to agencies, the relevant risk classes applicable to the agency and the various levels and divisions of an agency which manage risk including the 'Three Lines Model.' These factors should be considered when assessing the three elements and nine attributes contained in the **Risk Maturity Matrix** to determine the agency's maturity level.

The **outside sections** of the Model include:

Agency, Division, Business Unit	•the structure of the agency and its divisions and business units that support the management of risk
Risk classes	•all risk classes relevant to the agency (including shared risk)
Regulations & Standards	•relevant minimum risk related regulations and standards (including but not limited to Treasury Policies and AS ISO 31000:2018 Risk management – Guidelines) that agencies are required to comply with
Three Lines Model	•the 'Three Lines Model'* utilised by the agency to support managing risk. To be effective, a governance structure will be comprised of management functions; risk, control and compliance oversight functions; and independent assurance functions. These elements individually and together, contribute to an environment of effective governance and informed decision-making (refer below).

*Note: For a diagram and further information on the 'Three Lines Model', refer to the Internal Audit and Risk Management Policy for the General Government Sector (TPP20-XX)[3] when it is issued.

[3] This policy is currently being revised and this reference will be updated when the Internal Audit and Risk Management Policy for the General Government Sector (TPP20-XX) is issued.

Definitions

Attributes

NSW Agency Risk Operating Model	Definitions
INTEGRATION	**The integration** supports the application of risk management in the agency
Strategy & Business Planning	**Strategy & business planning** considers the key risks and their management as an integral part of developing corporate and business plans 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 the 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 resources (including capital expenditure, operating expenditure and associated assumptions).
Reporting & Communication	**Reporting & communication** considers the ongoing dialogue across the agency that supports the flow of risk related data, information and insights to those responsible and accountable for the management of key risks.
ENABLERS	**The enablers** support the risk identification, analysis, evaluation, treatment, monitoring, reporting and communication process
Methodologies & Tools	**Methodologies & tools** considers the common approach to supporting the application of a risk management framework and processes across the agency. This includes when and how the agency identifies, evaluates and assesses its risks, the relevant people involved and the reporting documentation, tools and templates used.
Data & Information	**Data & 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 availability of data to support risk based decisions.
Capability & Training	**Capability & training** considers the risk capability, knowledge and experience of people across the agency. Increasing capability assists with improving the risk management framework / process and management of 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 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 the 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 ad-hoc, unpredictable and highly dependent on individuals

Note: The definitions relating to risk and risk management are contained in the ‘related policies and resources’ listed above.

Risk Maturity Assessment Process

This process flow should be followed to conduct a risk maturity assessment using this Tool. The result will be a comprehensive program of activities that will assist agencies to move from their current maturity to their target maturity state. Each attribute should be assessed against the **Risk Maturity Matrix** in the next section.

Agencies should consider the context of the agency when determining its maturity (i.e. a larger more complex agency may have more complex risk governance needs than a smaller agency). Agencies may have a lower maturity score due to their size, risk profile or context which is acceptable. The purpose of the Tool is not to focus on a specific score or maturity level but to understand the activities required to move the agency from its current maturity to its desired maturity.

1 Gather supporting evidence

- **Gather risk evidence** to enable assessment of the current risk maturity level (examples of risk evidence are shown in the supporting information section).
- **Engage key risk stakeholders** in the 1st, 2nd and 3rd lines to discuss and comment on risk maturity.

2 Assess current state

- **Select the maturity level** that best fits the Agency's **current** position.
- **The maturities for each attribute are progressive** and elements of earlier maturities are assumed as maturity levels progress.
- **Appropriate evidence** gathered in step one should be used to support the selected maturity level.

3 Assess target/desired state

- **Select the maturity level** that best fits the agency's **desired target** state of risk management.
- The target risk maturity should **consider the complexity, context and constraints** faced by an agency.
- **Not all agencies** would be expected to have a target maturity state of advanced. This will depend on cost/ benefit, complexity and context of the agency.

4 Create a program of works

- **Determine the activities required** to move from current to target maturity state for each attribute in the operating model.
- **Develop a program of work** for the Agency to move from current to target maturity state recognising the interdependencies arising between different elements and attributes.

Overall maturity score

An overall maturity level can be assigned for both current and target maturity states by:

- allocating a score of 1 to 5 for each attribute
- calculate the average of the 9 attributes, and
- apply the average score to the below table to determine the overall maturity level.

Score	Maturity level
1	Fundamental
2	Repeatable
3	Systematic
4	Embedded
5	Advanced

The overall maturity level may be used for general discussion and comparisons but should not be the primary outcome for the Tool. The focus should be on understanding the activities required to move the agency from its current maturity to its target maturity. Refer to the accompanying Spreadsheet to calculate an overall maturity score and level.

How frequently should the assessment be performed?

The assessment should be conducted at least annually to use the results for planning meetings and decision making with leadership teams and Audit and Risk Committees, as well as enable agencies to measure improvements on a consistent basis.

Who should conduct the assessment?

The risk management team should conduct the assessment with their leadership team and be reviewed by the ARC. This supports assessing risk at all levels of agencies for a wholistic view of the agency (e.g. tone from the top compared to the operational level) and encouraging the use of the assessment results for planning and decision making as the leadership/senior management teams are part of the process.

Risk Maturity Matrix

The risk maturity matrix describes what an agency may be like at a specific maturity level for each attribute in the operating model. It is not definitive and should be considered in context. The **evidence and best practice examples** in the following section support assessing the risk maturity of an agency.

		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. The Executive are involved only in major issues or concerns relating to risk.	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 agency's risk culture are understood and reported on. There is "tone from the top" (e.g. Executive and Audit and Risk Committees) support of proactive risk management behaviours.	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, documented or repeatable. Positive risk outcomes rely solely on well-intended individual efforts. Risk tolerance is considered on an ad-hoc basis and is not consistently applied when assessing risk. There is a documented risk management and risk governance policy and procedures, with basic coverage of roles and responsibilities focussing only on Executive management and the risk function.	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 and are clearly understood across the agency. Evaluation of risk governance is performed using relevant and appropriate key risk indicators. There is 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 are monitored to allow changes to risk tolerance over time. Risk governance policies and procedures are regularly reviewed to maintain relevance to the agency's risk profile.	Risk governance practice, policies and procedures are 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.

		Maturity level				
Element	**Attribute**	**Fundamental**	**Repeatable**	**Systematic**	**Embedded**	**Advanced**
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 specialist function is established and requires risk competency. Some formal risk management training is offered to the wider organisation.	Standardised risk management training is run for all staff (role specific) with deeper training provided for specialists. All staff are expected to have a knowledge of risk management and apply it in their role. Risk management training content sets out all the key components of the risk management framework including policy requirements, risk management methodologies and tools.	The agency is recognised as employing experienced risk personnel with embedded knowledge & expertise in place. Risk training is provided in areas of emerging risk practice and comprehensive risk training is provided to all staff. Risk management training content is reviewed at least annually.	Risk management knowledge and skills are continuously upgraded through ongoing learning and development 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. A risk classification library is documented and is used as a basis for risk identification and evaluation across the agency. 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, the management of risk by an agency and the effectiveness of risk tools 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 low, inconsistent and with limited confidence. Risk decisions are made with low quality data.	Some data collection is undertaken and is used to evaluate and monitor risk on an ongoing basis. There is a 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. Risk management data guidelines are used to prescribe the agency's expectations regarding data quality, completeness, accuracy and availability.	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.

		Maturity level				
Element	**Attribute**	**Fundamental**	**Repeatable**	**Systematic**	**Embedded**	**Advanced**
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 and not actively reviewed in-line with strategy and business plan reviews.	Risk is considered in strategies and business planning but is not consistently applied and is not consolidated across the agency.	Strategy setting and business planning consider risks in a consistent manner and document the responses. Risk review outcomes are documented and reviewed and reported on an annual basis.	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, evaluation and throughout the project lifecycle.	A consistent and documented approach to risk management is applied to all significant projects. Ownership for project risk is understood and followed through.	Key project risks (e.g. interdependency, benefits realisation and management, staff impact, customer, budget, resourcing) are regularly discussed, evaluated and combined to support risk-based decisions on a project and portfolio basis and support the delivery of agency outcomes. This covers both delivered and delivery risks.	Project portfolio is consistently evaluated for risks and interdependencies. Resourcing and funding are dependent on effective risk management practices that assess all risk classes. There is a clear reference between project risks and the agency's risk profile.
	Programs & Operational Performance	Program and operational risks are not defined, formalised, consistent, documented or repeatable. Program and operational 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 plans / procedures in place.	Defined, documented and consistent financial and non-financial risk management procedures are included in most 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.

		Maturity level				
Element	**Attribute**	**Fundamental**	**Repeatable**	**Systematic**	**Embedded**	**Advanced**
	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. However, actions from reports are not consistently followed-up.	Risk reporting is consistent in format and content and is used for decision making and planning by Senior Management. Reporting identifies exceptions and “near misses”.	Risk reporting uses dynamic risk measurements based on quantitative and statistically based data and/or verifiable supporting information to allow responsive risk decisions to be made. Risk is reported and communicated appropriately across all levels of the agency.	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 decision making and continuous improvement in risk management across the business.

Evidence and best practice examples

The table below describes the types of information that could be referenced when assessing the risk maturity of an agency (note: the list of information is not considered exhaustive). When assessing maturity an agency should reference supporting information that is available in the agency and consider how this information will support selecting a particular maturity level. The Best Practice Examples help agencies to understand the nine attributes and provide a reference point for an increased level of maturity.

Element	Attribute	Supporting information	Best Practice Examples

Foundations	**Risk culture**	• Agency values and behaviours
		• Risk Culture Assessments (staff survey, internal review or internal audit)
		• Reward and recognition programs:
		  ○ Formal performance recognition feedback (e.g. program specific)
		  ○ Social recognition (e.g. social events, team meetings, conference, etc)
		  ○ Recognition through communication channels (e.g. emails, newsletters, etc)
		• Award certificates (e.g. individual award, team award, division award, business award)
		• Consequence management procedures
		• Incident and lessons learnt information
		• Risk roles and responsibilities (including risk champions)
		• Developed or use of prescribed learning & development programs
		• Developed or use of prescribed performance measures for risk management.
			• The Executive is regularly involved in significant risk-related discussions
			• The agency's desired risk behaviours and attitudes are defined and communicated across the agency
			• The agency has adopted appropriate methods to assess the level of risk culture across the agency and close gaps with desired risk culture
			• Risk culture elements (e.g. personal risk attitude and risk management competency) are considered when hiring / promoting staff
			• Staff report concerns about inappropriate or excessive risk taking and act without fear of retaliation or intimidation
			• The agency has programs to ensure the desired risk culture is built and driven across the agency (e.g. training programs, awareness initiatives, etc).

Element	Attribute	Supporting information	Best Practice Examples
	Risk governance	• Governance structures, roles and responsibilities • Developed or use of prescribed risk frameworks / operating models • Developed or use of prescribed policies, procedures, standards, checklists covering key risk classes, incident management, customer & complaint management etc • Emergency Management plans for Departments / agencies dealing with large groups of the public • Delegations of Authority • Terms of reference for key governance committees • Risk Tolerance Statements and guide on how risk tolerance is applied when assessing risks • Risk reporting related to tolerance • Audit and Risk Committee and Internal Audit Charters (reflective of Model Charters in the Internal Audit and Risk Management Policy) • Risk management is included in staff performance agreements • Hierarchy structure of Risk Registers for the organisation that links the detailed Operational Risk registers to higher level strategic and enterprise risks • Control design and operational effectiveness assessments (includes stress testing of controls).	• The role of the Executive / Audit & Risk Committee is formally defined in relation to its role and responsibilities on risk oversight • The agency has in place Management Committees which regularly meet to address and oversee all key risks • Roles, ownerships and responsibilities of risk management are clearly defined, assigned, communicated and understood across the agency • Risk escalation processes and related roles and responsibilities are clearly defined • The agency has a process to define, articulate and communicate specific tolerance for risk taking which is formally approved and periodically reviewed by the Executive / Audit & Risk Committee • All key decision-makers understand and act in accordance with the risk tolerance defined by risk management activities • Risk tolerance is communicated across the agency, guides decision making and is embedded in the risk matrix for the organisation • Regular risk forums are established which comprises of senior level representatives across the agency with a formal terms of reference which sets out the forums objectives, authority, composition, roles and responsibilities • Risk forums review material risk exposures and make decisions on the appropriateness of risk assessment • Risk forums consider control design effectiveness and control operating effectiveness assessments associated with the material risks identified across the agency and make decisions on the appropriateness of rectification actions having regard to the risk tolerance • Risk management is discussed as a regular agenda item at senior management meetings on an at least quarterly basis.
Enablers	**Capability & Training**	• Risk management competency and skills definitions • Induction / on-boarding risk training for new staff • On-going risk training programs for staff • Specific risk capability training for relevant staff responsible for risk management • Advanced risk training for specialist risk professionals to maintain capability • Performance assessment risk measures • Risk management accountability identified in position descriptions and performance reviews for relevant staff that manage risk.	• Hiring and development of management are periodically reviewed to ensure competency levels are appropriate and support the business objectives • Gaps in risk management competency are recognised and addressed to ensure capability evolves as the agency risk profile changes (internal / external) • Formal training and development of staff with a focus on agency wide risk management.

Element	Attribute	Supporting information	Best Practice Examples
	Methodologies & Tools	• Consistent risk management vocabulary • Risk assessment methodology (scales, likelihood, consequence, rating) • Root cause analysis / classification • Risk profile / register • Risk and control matrix • Specific industry / risk class models • Risk analysis and trending • Risk dashboards • A control library is documented and is used for categorising control instances. There is a documented control assurance program which prescribes the frequency and method of control assessment • Analysis of emerging issues or key risk indicators • Evidence based methods • Control design and operational effectiveness assessments (includes stress testing of controls).	• Guidelines, metrics or scoring scales / methods have been defined to help individuals understand how to assess risk (e.g. financial and reputational impacts, likelihood, velocity, risk management capabilities in place) • The agency's portfolio of risks is analysed to determine whether any risks are interrelated or whether a single event may have cascading impacts • Risk profiles are formally approved and periodically reviewed by the Executive / Audit & Risk Committee • The agency has implemented specific techniques and tools (which might include defined performance indicators) to evaluate and monitor top risk exposures and / or the effectiveness of risk responses • Risk analysis includes considering emerging risks and sensitivity analysis • Risk forums regularly evaluate the effectiveness of risk management frameworks, the management of risk by the agency including control design effectiveness and control operating effectiveness assessments and the effectiveness of tools.
	Data & Information	• Dedicated IT solutions for data collection, modelling, monitoring and reporting e.g. risk management information system • Risk specific analysis systems • Risk and incident management and reporting systems including automatic risk notification or alarm associated with reported issues • Data integrity and security systems • Quantitative and qualitative data analytics • Data governance procedures • Data and information stored in some form of online records management system.	• The agency has adopted systems to better support dynamic risk assessment and monitoring activities and to store risk-related data • Collection of quantitative and qualitative data (as required) assisting performance analysis and insightful value-added reporting to support decision making • Risk data is integrated with interrelated processes/systems such as business planning and audit to establish an advanced suite of quality data to support decision making • Integrated risk management system capturing data on governance, compliance, audit, project risk, business continuity, issues management and incident management etc.
Integration	**Strategy & Business Planning**	• Strategic risk profiles • Business plans include risk considerations that align with the agency • Business Plan risks align with Business Strategy Risks • Horizon risk scanning • Scenario analysis • Stress testing.	• The agency identifies and understands the potential risks and opportunities of each strategy being considered when evaluating strategic options. • The risk management function partakes in the strategy setting process • When conducting strategy and business planning, agencies should consider strategic and performance goals with reference to State Outcomes.

Element	Attribute	Supporting information	Best Practice Examples
	Projects	• Project risk registers • Risk and control matrices • Project risk committees (including terms of reference) • Gateway assurance reviews including risk management focus.	• The agency considers not only typical time, cost and quality risks but wider risks (program and project interdependency, benefit realisation and management, staff impact and customer) and the distinction between delivered and delivery risk. • Stronger project risk management supports improving the delivery of agency outcomes.
	Programs & Operational Performance	• Process flow diagrams and procedures • Risk profiles for critical processes • Risk and control matrices • Key Risk Indicator monitoring for critical processes.	• Critical financial and non-financial risks have key risk indicators that are monitored. Mitigations are in place as risks increase or emerge.
	Reporting & Communication	• Dynamic risk reporting • Risk dashboards • Risk heatmaps • Enterprise Risk Register (used to report to leadership team and ARC) • WHS Risk Register (potentially managed by Health and Safety Committee).	• Risk reporting is dynamic and undertaken in real time, allowing management to utilise a combination of heatmaps, dashboards and key risk indicators to proactively manage risk in the business. • Risk reporting is integrated into existing management systems and demonstrates alignment with objectives, performance measures, risk indicators and key risks.

Further information and contacts

For further information, please contact the:
Financial Management Governance & Analytics team, NSW Treasury
Email: finpol@treasury.nsw.gov.au

For further assistance in implementing the tool for your agency, please contact your cluster Department's risk management team or Chief Risk Officer.