Treasury

August 2020

Risk Management Framework (TIPP5.01)

Version

Document number: A3457989	Version number: 2.1
Original issue date	November 2016
Revised:	July 2017; February 2018; August 2018, August 2020

Contact details

Name: Su-Lin Macdonald	Position: Director Internal Audit and Risk
Business Unit: Internal Audit and Risk Division: Financial and Operations Group	risk@treasury.nsw.gov.au

Table of Contents

1.1 Introduction

NSW Treasury's (Treasury) vision is to create a world class Treasury team that enables the Government to deliver on its promises to the people of NSW that the State will always be a great place to live and work. Our purpose includes the provision of strong and transparent risk management.

This Risk Management Framework (Framework) outlines NSW Treasury's approach to enterprise risk management. Risk management is an integral part of good management practice and an essential element of good corporate governance. This Framework should be read in conjunction with Treasury's Risk Management Policy and Risk Appetite Statement to obtain a holistic understanding of the Risk Management Strategy employed. This Framework should also be considered alongside Treasury's Compliance Framework, and Fraud and Corruption Prevention Framework documents as compliance risk (or legal and regulatory compliance risk) and fraud risk are considered risk categories in themselves.

Treasury's Leadership Team and senior management are committed to developing an informed risk management culture, where risk management is not seen as a separate exercise but rather, as an integral component to the achievement of our objectives and integrated into all our business activities and decisions. The integration of risk management into our business activities means staff are alert to risks, are capable of performing an appropriate level of risk assessment to accept risk within our risk appetite and are confident to report risks or opportunities perceived to be important in relation to Treasury's priorities and goals. All managers and staff (including temporary staff and contractors) are responsible for the management of risk in accordance with this Framework.

Treasury's Framework has been developed in accordance with the NSW Government's Policy Paper's TPP15-03 Internal Audit and Risk Management Policy for the NSW Public Sector (under Principle One) and TPP12-03 NSW Risk Management Toolkit for Public Sector Agencies. Examples have been placed throughout this document as further support for the reader.

Effective risk management processes are also required by the *Government Sector Finance Act 2018* and the *Work Health & Safety Act 2011*. The *Annual Reports (Departments) Regulation 2015* requires agencies to report on their risk management and insurance arrangements. Agencies must also attest annually to compliance with all of the core requirements of TPP15-03.

1.2 Objectives

Treasury has established the Framework for the management of risk across all parts of its operations and has adopted the definition of risk used in ISO 31000:2018: Risk management – Guidelines:

"The effect of uncertainty on objectives"

Risk can be applied in a strategic context including positive and negative impacts. When negative, it is these risks that have the potential to prevent the achievement of our goals and strategies.

The term "Risk Management" refers to having an overview of Treasury's risks, our risk appetite and the way we choose to manage our risks and how it is integral to our decision making.

This Framework deals with risk management by aiming to provide a standard for consistency in the language of risk including risk identification, analysis, evaluation, treatment, monitoring, communication, management and reporting that can be applied to strategic and business planning as well as project management. The aim of the Framework is to ensure that:

- the Secretary, the Leadership Team, the Extended Leadership Team and all managers can confidently make informed business decisions,
- change opportunities and initiatives can be pursued with greater speed, robustness and confidence for the benefit of Treasury and its stakeholders,
- to reduce exposure to 'surprises' with risks or increased exposure occurring,

- there is greater certainty in achieving strategic objectives, and
- daily decisions at the operating level are made within the context of Treasury's capacity to accept risk.

As a central agency of the NSW Government, Treasury may also apply the Framework to support a whole-of-government view (for example, when considering risks in the development of the Budget or state-wide accounting processes).

1.3 Scope

The Framework applies to all staff including contractors and consultants engaged by Treasury and any entities to which Treasury provides principle department-led shared arrangements for audit and risk committees.

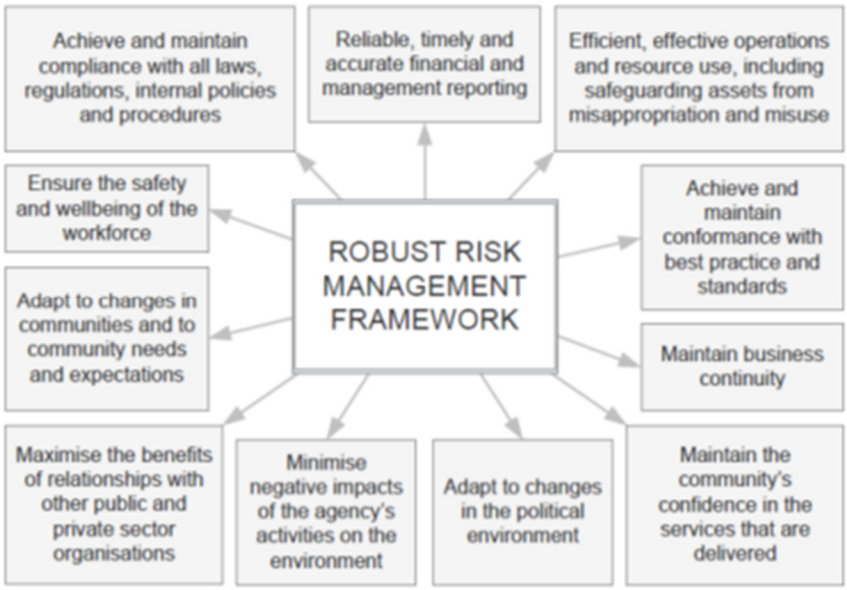
1.4 Background

1.4.1 Benefits of effective risk management

The successful identification, analysis, evaluation, treatment, monitoring, communication and management of key risks remove or minimise negative deviations from Treasury's objectives. It also assists with the early identification of opportunities. This Framework is intended to ensure that Treasury engages with risk at all levels in an effective, efficient, consistent and integrated manner.

Benefits of a robust risk management framework are summarised in Figure 1 below:

Figure 1: Benefits of a robust risk management framework



Source: TPP12-03 *Management Toolkit for NSW Public Sector Agencies*

1.5 Responsibilities

As an integral part of Treasury's management systems that covers all aspects of the business, ownership of the Framework rests with the entire Extended Leadership Team. In practice, however, the custody of this Framework rests with the Secretary who is responsible for ensuring that the Framework is implemented, tested, maintained and updated. The Secretary is assisted in this process by the Director of Internal Audit & Risk.

Accountability is central to an effective risk management framework. Table 1 identifies the key responsibilities regarding risk management within Treasury.

Table 1: Key Responsibilities

Extended Leadership Team (includes Leadership Team) and Business Unit Managers	• Owning and monitoring of the identified risks within their area of responsibility. Key requirements are:
	  ○ ensuring the completion, accuracy and updating of risk management plans within their area of responsibility,
	  ○ championing risk management and a culture of risk within their area of responsibility,
	  ○ ongoing monitoring and reviewing of identified risks (listed in developed risk registers) for completeness, continued relevance, and effectiveness of risk controls and treatment plans while taking into account changing circumstances, and
	  ○ operational responsibility for advising the Secretary and Treasurer on risks and opportunities in relation to State finances and economic drivers.

Project Sponsors and Project Managers	• Identifying, analysing, evaluating, treating, monitoring, communicating, managing and reporting on Project risks, advising the Project Management Office (PMO), the project steering committee and/or senior management.
All staff	• Understand and act on their responsibility to report new risks or increases in risk in a timely way and escalate as required. • Have regard to the organisation's risk appetite in the way staff perform their own work.
Secretary	• Governance responsibility for risk management and legal compliance within Treasury. • Strategic responsibility for advising the Treasurer on risks and opportunities for strengthening State finances and the policy settings driving the State economy. • Required to provide an annual attestation that Treasury complies with TPP15-03.
Audit & Risk Committees (ARC)	• Provides independent advice to the Secretary on risk management, governance, the control framework, and legal/regulatory compliance within Treasury. • As input to its advice, the ARC continually monitors: risk identification, assessment and treatment; Treasury's control framework; external accountability, particularly in relation to financial statements including the accounts of the Total State Sector; compliance with laws, regulations and policies; external audit findings; and the Internal Audit program, including management's progress in implementing agreed actions arising from both internal and external audit recommendations. • Oversees the implementation and operation of this Risk Management Framework, and assesses its adequacy. The ARC monitors the internal policies for identifying and determining the risks to which Treasury is exposed to in accordance with TPP15-03, with particular focus on reviewing the implementation of risk treatments.

Risk Appetite

Treasury's internally focussed risk appetite statement sets out the maximum acceptable level of risk / risk impact which combine to articulate Treasury's attitude towards risk and the level of risk Treasury is prepared to take in pursuit of its strategic objectives and ongoing operational commitments.

Our risk appetite should be used to support decision making and shape change activities whilst maintaining focus upon current business operations within the parameters described. The Leadership Team will use the risk appetite to review business decisions for Treasury the agency at an overall aggregate level.

Risk taking is a necessary and desirable part of doing business. The defining of our risk appetite is intended to support considered risk taking whilst maintaining Treasury's operational and financial stability and protecting our reputation. It is acknowledged that instances may occur where it is considered to be in Treasury's broader interests to act outside of one or more of the agreed tolerances set out in Treasury's Risk Appetite Statement, but this should nonetheless be subject to Leadership Team approval.

The Treasury Risk Appetite Policy (TIPP5.01A) provides further guidance on applying the Risk Appetite Statement (RAS) to assess Treasury's Risks. The tolerances defined in the RAS should be used as a guide for determining the acceptable level of risk associated with key business functions performed by Treasury. Risks that are foreseen to result in outcomes that fall outside of the RAS parameters therefore require additional treatment to mitigate these.

1.6 Control Assurance

The Framework is largely self-regulating. Control assurance is principally through the use of control self-assessment, practised by risk and control owners. These self-assessments are expected to take place using the online risk management system (Protecht) and are expected to be reviewed and updated as part of the ongoing revision of team risks and registers. Protecht can facilitate this process through the ability to proactively monitor controls. Control assurance is focused on validating this activity in terms of both the adequacy and effectiveness of controls.

See also 2.3.3 Risk Controls and Effectiveness. Where it is required, Internal Audit will review specific controls as part of the annual Internal Audit program.

2. Risk Management Requirements

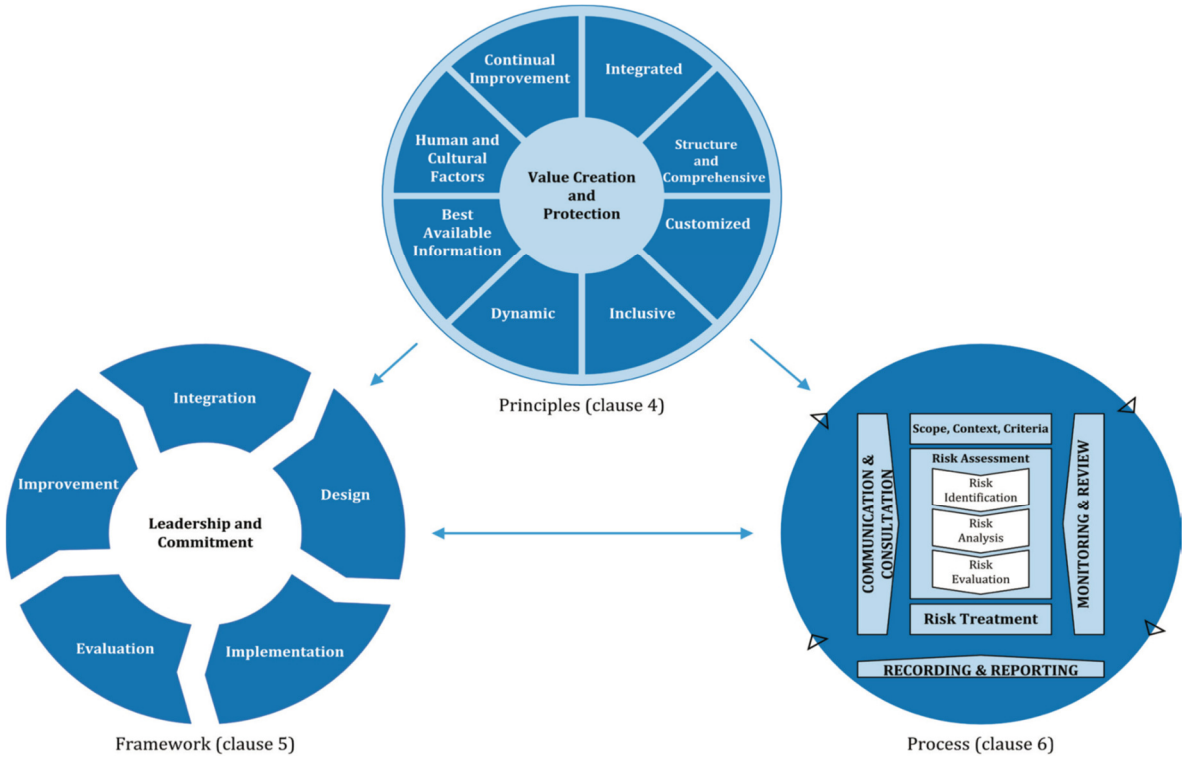
To provide the highest degree of consistency practicable in the management of risk across Treasury it is important to have a systematic means of establishing the context in which we are operating and for identifying, analysing, evaluating and treating risk in the most effective way within the demands of that context.

Treasury has adopted the seven interrelated elements of the ISO31000:2018 risk management process as the methodology for their risk management framework. Namely, these elements are:

1. Establishing the context
2. Identifying risks
3. Analysing risks
4. Evaluating risk
5. Treating risks
6. Monitoring and reviewing risks
7. Communication and Consultation plan

These elements and their interrelationships are shown in Figure 2 below. Note that risk identification, analysis and evaluation are collectively known as “risk assessment”.

Figure 2: The Risk Management - Principles, Framework and Process



Source: ISO 31000:2018

2.1 Requirement 1 – Establish the Context

Risk is the effect of uncertainty on Treasury's objectives. Because of this, the first step is to identify and understand those objectives.

Depending on the level at which we are identifying risk, the context may come from the Government's priorities, Treasury's strategic level planning, from a Division's business plan, or from a program or project plan. When identifying and evaluating risk, we also need an understanding of Treasury's internal strengths and weaknesses relevant to its goals and to the objectives that most closely concern us. Being aware of these strengths may assist with the identification of unforeseen opportunities.

The more we understand our internal and external operating environment, and the expectations of our stakeholders, the better prepared we are to identify and evaluate those risks which are likely to prevent the efficient achievement of our goals.
When assessing the internal environment, Treasury must identify aspects of the organisation that will impact on their ability to manage risks. Factors to consider in the external environment include the political environment, economic conditions, social norms and trends, technology, major international trends and laws and regulations. In its role as a central agency, Treasury also needs to consider the strengths and weaknesses of the structures and systems at its interface with other agencies.

2.1.1 Strategic Risks

Strategic risks relate directly to strategic planning and management processes across Treasury. Strategic risks are those which could significantly impact on the achievement of our vision and strategic objectives as outlined in Treasury's Strategy. These are high-level risks which are owned by, and therefore require, identification, treatment, monitoring and management by the Leadership Team and Extended Leadership Team. Strategic risks are highlighted to the Secretary as part of the Dashboard.

2.1.2 Operational Risks

Operational risks generally require oversight by each Group and associated Divisional head, or by the relevant program or project steering committee.

Operational risks are those which could have a significant impact on the achievement of the:

- strategic objectives and goals from the perspective of the actions undertaken by a particular Division, Business Unit or project, or
- individual programs or project management objectives.

Common causes of operational risks could include:

- Inadequate business processes or systems,
- Staff non compliance with key requirements of internal processes or procedures,
- Insufficient planning and resourcing, or
- Technology failures.

Each operational risk has a nominated Risk Owner who manages the risk and reports as required to the responsible Group or Divisional head. In some instances, these risks may require escalation to the Leadership Team.

All Divisions, Business Units and projects conduct formal reviews of operational risks at least annually, including the relevance and validity of existing risks and ratings, and the progress of risk controls and treatment plans. The reviews also involve identifying any new or emerging risks that might affect the achievement of plan objectives and budgets of the respective Division, Business Unit or project.

2.1.3 Project Risks

A major and/or priority project should have significant risks managed at the Sponsor, Group Head or Division / Business Unit area level depending on Treasury's exposure. In particular:

- all major projects are planned using a suitable risk assessment to focus their execution plan on the major sources of uncertainty/ risks
- the financial justification and business case for the project are subjected to a suitable risk assessment
- the project risk management plan is to be reviewed either annually, or at least once at each phase of the project life cycle; depending on what occurs more frequently:
    - pre-project
    - project initiation
    - project delivery
    - project close - for lessons learned, and for passing any remaining risks to business as usual management
    - and if major changes are made to the business case, scope, timeframe or budget.

During the project delivery phase of a project the critical controls should be subjected to an assurance assessment in accordance with Section 2.3.3.

2.2 Requirement 2 – Identifying Risks

2.2.1 Identify Risk

The next step is to identify and document all the key risks that may impact on Treasury's ability to achieve its objectives. A list of key risks is identified, based on those risk events that might prevent, degrade, or delay the achievement of our business objectives. Key areas to consider when identifying risks to the business objectives include staff, service delivery, financial, regulatory, external events (e.g. natural disasters, man-made disasters, and security), ICT, health and safety, government requirements, fraud and stakeholders.

Risk categories commonly used in Treasury include:

- compliance (i.e. with laws, regulations, Premier/Treasurer Circulars, NSW Government and Treasury policies)
- financial (i.e. the risk involves the department's or state-wide financial losses)
- reputational (a particularly important concern for any Treasury)
- fraud and/or corruption
- Information technology and security
- people/capability (i.e. key person risk)
- service delivery
- stakeholder engagement
- work health and safety
- business continuity (specifically, risks related to recovery after an incident)

Refer to Appendix 1: Risk Categories for a more comprehensive list of Treasury's common identified risks.

2.2.2 Identify Causes of Risk

It is important that the potential causes of each risk are identified and recorded. This allows for more informed decisions to be made regarding the treatment of risk.

For example, a cause behind the risk of *'an unsafe work environment'* may be the result of not being aware of the requirements of the relevant legislation, or that there are no checks to ensure that the relevant policies and procedures are being implemented.

In some cases, a cause may become a risk where it is considered that it requires its own controls and possibly its own risk treatment plan.

For example, a cause of the operational risk '*Fraud or corruption'* could be '*the gifts and benefits register not kept up to date and requirements not understood*'. This cause may also need to be dealt with as a risk at the operational level (Division / Business Unit), as it requires its own controls and treatments to manage.

2.2.3 Identify the Impact

It is also important to identify the potential impacts of a risk as part of determining the consequence, risk rating and risk level. It is quite possible for the impacts to occur in a number of risk categories (Table 3: Consequence Table), but also several times within an area of consequence.

For example, an impact of risk around *'Fraud or corruption'* may be rated highest as a '*regulatory non-compliance'* consequence but the impacts on the organisation could also include '*a reputation, financial, media interest/reporting, client/stakeholder negative feedback, etc*'.
Similarly, the highest impact of risk relating to *'providing incorrect advice to another government agency'* may be in the '*stakeholder engagement/ relations'* category, although the consequence of this risk occurring may also have impacts in the reputational, and people & capability categories.

2.3 Requirement 3 – Analyse the Risk

2.3.1 Consequence and Likelihood

To analyse a risk to determine its severity, a risk matrix is used to identify the **highest impact consequence** with **the likelihood of it happening**.

A consequence rating is determined from the Consequence Matrix, **Table 3: Consequence Table** based on the highest potential adverse impact on Treasury and its stakeholders. Where there is more than one type of consequence possible, the one that gives the most severe adverse consequences should be selected as the basis for the rating. A consequence can be rated as Insignificant, Minor, Moderate, Major, and Extreme.

Once the risk's consequence rating has been identified, a likelihood rating is determined **Table 2: Likelihood Table** based on the corresponding likelihood that Treasury and its stakeholders could be affected by that specific consequence. The likelihood of the consequence can be determined to be Rare, Unlikely, Possible, Likely, and Very Likely.

2.3.2 Risk Level

The risk level is the outcome of the combination of consequence and likelihood using the risk matrix (**Table 4: Risk Rating – The Risk Level Matrix**). To determine the overall risk level, (expressed as Extreme, High, Significant, Moderate and Low), the consequence and likelihood are multiplied together in the risk matrix**.**

For example, NSW Treasury is considering launching a potentially controversial project that some stakeholders may not consider to their benefit once publicised. *This may harm some important relationships.*

Consequence: *the highest impact of this particular risk occurring may be within the stakeholder engagement/ relations category, and may create temporary loss of credibility to clients or stakeholders (**moderate** consequence with a rating of 3).*

Likelihood: *This temporary loss of credibility to clients or stakeholders is likely to occur during the next twelve months (**possible** likelihood, a rating of 3).*

Risk Rating: *The consequence rating of moderate (3) and likelihood of possible (3), results in an overall risk rating of **moderate** (3 x 3 = 9).*

The final overall level of risk rating following the application of Controls is reviewed by the appropriate manager, based on Treasury's risk appetite and reporting requirements.

The risk levels are expressed as follows:

- **Inherent risk** level is the level of risk **before** controls and their effectiveness are considered.
- **Residual risk** level is the level of risk **after** controls and their effectiveness are included in the assessment.

The residual risk review and action requirements are outlined in **Table 5: Residual Action Requirements**.

2.3.3 Risk Controls and Effectiveness

As defined in ISO: 31000:2018, a control is a measure that modifies risk and can include a process, policy, device, practice or automated system. Any controls listed as a mitigating factor must then be assessed for their overall effectiveness (determined by looking at their design and performance effectiveness) when determining the residual risk. This ascertains how the appropriate residual risk level is rated compared to the inherent risk level. Refer to **Appendix 3: Control Assessment- Design, Performance & Effectiveness.**

The assessment of control effectiveness requires a robust and defensible assessment of controls. A quantitative assessment technique can be used to determine the adequacy of existing controls to mitigate a particular risk.

Refer to Diagram 1 for further guidance.

For example, a control to mitigate the risk of 'fraud or corruption' occurring, could be ensuring that there is a 'gift and benefits register in place'. The control, however, may only be rated **'partially effective'** (refer to **Table 8: Control Effectiveness**) because a survey of staff has been undertaken which indicates that the 'requirement to complete the gift register is not understood by all staff, particularly temporary staff'. As a result, the control is determined to be **weak** and does not adequately mitigate the risk. In this example, the recommended action would be that management implements further controls/actions to manage the risk and improve the standard of control effectiveness.

a) Control Design and Implementation

Assess the effectiveness of the control design and implementation. That is, if the risk functioned as intended at all times, will it completely prevent the risk from manifesting? Are the controls capable of managing the risk and maintaining it at an acceptable or tolerable level? Refer to **Table 6: Control Design** for the relevant matrix.

For example, there may be a risk of '*unauthorised spend of funds'*. A control in place is that your direct supervisor must sign off on a physical documented request to spend any money before the Accounts Payable team process the payment. However, because there is a chance that the Accounts Payable Team Member may be able to process the request in the finance system without the evidence of sign off as there are no real barriers, the control design may only be rated as **adequate.** Alternatively, if you must place the request to use funds through the financial system, and the system does not allow the request to be paid unless there is authorisation given by your manager via the system, it is unlikely that inappropriate funds will be paid as the manager must review the request. Therefore, the control's design instead becomes **very strong.**

b) Control Performance

When considering the performance of the identified controls should consider:

- Are the controls operating as intended?
- Have they been, or can they be, proven to work in practice?
- Are they being used as planned as part of the design?
- Are they cost effective?

Note: When considering "Failure Rate", it is the failure rate with respect to the Risk Appetite of failure for that control. It is understood many controls can fail, especially on high volumes of transactions. **Refer to Table 7: Control Performance** for the relevant matrix.

> For example, there may be a risk of '*unauthorised spend of funds'*. A control in place is that your direct supervisor must sign off on a physical documented request to spend any money before the Accounts Payable team process the payment. As part of discussion with the Manager, it has been determined that there have not been any funds on the team's budget that have been inappropriate or have not been pre-authorised. As there has not been any evidence of a failure to date, the control's performance may be rated as **strong.**

c) Control Effectiveness Rating

The overall Control Effectiveness rating is generated from the inputs you determined for (a) Controls Design and Implementation and (b) Control Performance. **Refer to Appendix 3: Control Assessment- Design, Performance & Effectiveness** for more detail.

> That is, in line with the Control Effectiveness Matrix, a control that has had its design rated as **adequate**, but its performance rated as **strong**, has an overall effectiveness rating of **partially effective.**

d) Control Categories

Mitigating controls can have one of two purposes. These are designed to either prevent or detect the risk from eventuating.

Preventative controls are proactive activities that deter risks from materialising at all. E.g. separation of duties, or appropriate authorisations.
Detective controls alternatively are reactive, and are activities that identify that a risk has materialised. E.g. spot checks, account reconciliations, or inventory counts.

The nature of the control is important in determining its impact on an identified risk, and the way that it affects the 'likelihood' and 'consequence' concepts introduced in Section 2.2.3. The changes in likelihood and consequence will then determine the residual risk.

That is, in instances where a control is partially or fully effective:

Nature of control	Likely impact
Preventative	Reduced likelihood of risk materialising
Detective	Reduced likelihood of risk materialising, AND/OR Reduced level of consequence

Inherent and Residual Risk Example:

If we revisit the below example:

NSW Treasury is considering launching a potentially controversial project that some stakeholders may not consider to their benefit once publicized. *This may harm some important relationships.*

Inherent Consequence: *the highest impact of this particular risk occurring may be within the stakeholder engagement/ relations category, and may create temporary loss of credibility to clients or stakeholders (**moderate** consequence with a rating of 3).*

Inherent Likelihood: *This temporary loss of credibility to clients or stakeholders is likely to occur during the next twelve months (**possible** likelihood, a rating of 3).*

Risk Rating: *The consequence rating of moderate (3) and likelihood of possible (3), results in an overall risk rating of **moderate** (3 x 3 = 9).*

The Project Sponsor may decide they were not willing to endorse the project as they determined that a risk rating of moderate was outside of Treasury's appetite. As a result, the Project Manager implemented a *control,* as they set up a working group with members of key stakeholder groups to manage and respond to any negative opinions of the project. It is the Project Sponsor's responsibility to ensure that these are taking place as scheduled, and that the Project Manager is completing any actions promised to these stakeholders.

The Project Sponsor assesses the control design, and determines that it is **adequate**. Both the Sponsor and Project Manager uphold their responsibilities with the agreed regularity, and find that stakeholders are responding well to the opportunity to provide input and the responsiveness of Treasury. Its performance is therefore considered **strong.**

Based on the control effectiveness matrix, the control in place is therefore **partially effective.**

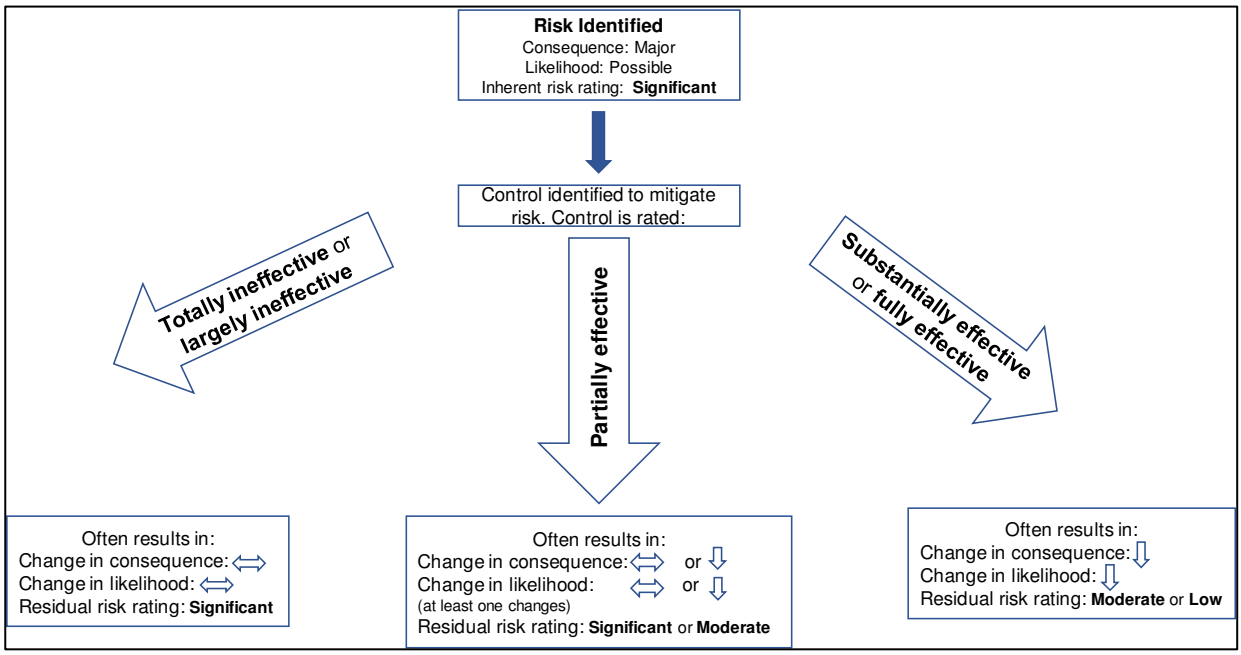
Following this judgement, the **consequence and likelihood of the risk should be reassessed.**

Residual Consequence: *As the control is preventative, and is only considered to be designed adequately, the consequence category remains the same, where there may be temporary loss of credibility to clients or stakeholders (moderate, a rating of 3).*

Residual Likelihood: *However, as mentioned, the control is preventative, and is performing strong, it is now unlikely that the risk is unlikely to occur for some time, with a less than 10% chance of this occurring within the next 12 months. (rare, a rating of 1).*

Therefore our **Residual** risk rating is now **Low** with a score of 3 (3 * 1).

Diagram 1



2.4 Requirement 4 - Evaluating Risk

The results of risk analysis are subjected to risk evaluation to make decisions about whether further treatment is required, which risks need treatment, treatment priorities and whether the risk must be escalated to the next level of management for review. (**Refer to** Table 5: Residual Action Requirements)

Generally, a risk review involves distinct steps, these being:

- comparison with similar risks
- in accordance with Table 5, escalation to the next level of management for review and acceptance, and then reporting and managing by an appropriate manager
- where required, the development of treatment plans to further reduce the residual risk level
- deciding whether a target residual rating needs to be identified, which can be achieved if additional treatments are implemented
- regular review as required by the residual risk level or following the implementation of treatments that are introduced as additional controls.

The decision to tolerate a risk and continue the exposure should be based on a consideration of the:

- willingness of Treasury to tolerate risks of that type and level
- need to escalate the risk to the next level of management to manage
- cost-effectiveness to further treat the risk

Risks may be accepted with minimal further treatment. They are to be monitored and reviewed periodically to ensure they remain tolerable.

2.5 Requirement 5 - Treating Risks

Risk treatment is the activity of selecting and implementing appropriate treatment measures to modify and reduce the risk. Risk treatment includes, as its major element, risk controls and includes the treatment options below. Any system of risk treatment should provide efficient and effective internal controls.

Treatment options, which are not necessarily mutually exclusive or appropriate in all circumstances, should be considered in the order below:

- Risk Avoidance: to avoid a risk with a detrimental consequence by deciding not to proceed with the activity likely to create risk (where this is practicable)
- Changing the likelihood of the risk: to enhance the likelihood of beneficial outcomes and reduce the likelihood of negative outcomes
- Changing the consequences: to increase the gains and reduce the losses, this may include emergency response, business continuity plans and disaster recovery plans
- Risk Transfer: this may include taking the appropriate insurances or the requirement for a warranty as part of a contract
- Risk Tolerance without further treatment: this involves an explicit decision to accept the risk.

Selecting the most appropriate treatment option involves comparing the cost of implementing each option against the benefits derived from it. In general, the cost of treating risks will need to be commensurate with the benefits obtained.

Several treatment options should be considered and applied, either individually or in combination. An owner for the treatment option, known as the 'control owner', should be allocated to hold accountability over the completion of the activity or control.

Additional treatments, in the form of treatment plans, or several specific treatment plans may be required if the residual risk level is unacceptable , refer to **Table 5: Residual Action Requirements**. Once treatment plans have been completed they may, if appropriate as an ongoing mitigation for a risk, become a control.

Once a risk treatment has been assigned to a particular risk, the risk team or action owner may choose to allocate Key Risk Indicators (KRIs) to this risk. These are 'indicators' to alert the agency of their exposure or potential for a risk to occur. KRIs are beneficial to determine the effectiveness of the treatment option selected by Treasury; that is, in instances where KRIs are constantly being exceeded, or does not improve following the implementation of a control, this may demonstrate that alternate treatment may be required. Each indicator must be allocated a period against which the benchmark applies.

The Key Risk Indicators are determined by the Internal Audit and Risk Team, along with the business and have been programmed into Protecht for allocation when recording a risk. Example Key Risk Indicators used by Treasury include:

	Key Risk Indicator	Tolerance	Relevant Period
1	Number of material omissions or errors detected in advice issued by Treasury	0	Semi -Annually
2	Value of unanticipated impacts on State Finances	+/- $1b	Semi-Annually
4	Number of significant workplace injuries or fatalities	0	Semi-Annually
5	Acceptable level of cost variations in project budget, including contingency funding and approved variations	<10%	Semi-Annually

2.6 Requirement 6 - Monitoring and Reviewing Risks

Each Division executive team member will review their operational risks and update the progress on the implementation of identified mitigation treatments at least annually. These discussions on the risks will be held with the internal audit and risk team and include:

- any significant changes in the risk profile (including emerging risks and the reasons for the changes
- an update on the progress and implementation of mitigation treatments
- any other specific risk issues or concerns.

Risks identified and owned by the Extended Leadership Team are accessible to the Leadership Team and reported to them by the internal audit and risk team periodically. The Audit and Risk Committee also have access to the Treasury risks and receive quarterly updates on these.

Separately, project steering committees will determine the timing of the review of project related risks which are more granular and sit outside of the Protecht system (one risk relating to the project will be captured in Treasury's risk register). The timing will be outlined in each project's governance arrangements.

2.6.1 Recording Risks

NSW Treasury records its risks through use of risk registers. Risk registers provide a view of all the risks that have been identified and assessed using the risk management process by various areas of the business. The creation of registers is facilitated through Protecht, Treasury's Risk Audit and Compliance Management system. All risks are to be recorded in Protecht, as the system allows for risk reports to be generated. See **Appendix 4: Risk Assessment Template** for an outline of the details required to be entered into Protecht.

Risk Owners and other selected users across Treasury can use this system to manage, track and report on risks. This requires being a licenced user of the system. If you are not a licenced user and require access to Protecht, email your request to the Internal Audit and Risk Team at risk@treasury.nsw.gov.au. Assistance can be requested from the Internal Audit and Risk branch to complete the risk recording process, or alternatively, user manual guides can be shared for your use.

2.6.2 Risk Register Review

Risk owners are to regularly review their risks, ensure that control owners and, where applicable, treatment plan owners are monitoring and reporting on their control and/or treatment plans.

It is the responsibility of management of each Division/ Branch to ensure that Treasury's risk register has been developed with their corresponding team with all relevant risks entered via Protecht. It is also their responsibility to ensure that the register exists as a live and ongoing document, with regular reviews to check that the risks are still complete and relevant, and that any inherent and residual risk ratings remain reflective of the risk.

2.7 Requirement 7 - Communication and Consultation Plan

The Treasury Intranet will include a Risk and Compliance page that has been designed to inform staff of their risk and compliance responsibilities. Leaders in the Loop may be used to inform the Extended Leadership Team of future requirements and to send out reminders.

2.7.1 Training Strategy

The Internal Audit and Risk branch will facilitate training of all relevant managers and staff (those identified as being users of the Protecht system) about the risk management processes and the online risk management system. The training is a major element of the implementation of the Framework. The training covers:

- awareness briefings on the Risk Management Framework and the Protecht system for all relevant managers, including project managers and staff
- an eLearning module on risk management for staff.

After the initial training program, refresher training will be conducted on a regular basis to ensure that existing users and new users are familiar with risk management within Treasury.

2.8 Related Policies and Documents

Issuer	Reference	Document Name
Director of Internal Audit and Risk	TIPP5.05	Business Continuity Plan Policy
Secretary	TIPP2.05	Code of Ethics and Conduct
Director of Internal Audit and Risk	TIPP5.15	Compliance Incident Management Policy
Director of Internal Audit and Risk	TIPP5.14	Compliance Management Framework
NSW Government	[No 17 of 1998]	State Records Act 1998 No 17
NSW Treasury	TPP15.03	TPP15-03 Internal Audit and Risk Management Policy for the NSW Public Sector
NSW Treasury	TPP15.03	TPP 12-03 - Risk Management Toolkit
Director of Internal Audit and Risk	TIPP5.09	Fraud and Corruption Prevention policy
Director of Internal Audit and Risk	TIPP5.10	Fraud and Corruption Prevention framework
Director of Internal Audit and Risk	TIPP5.08	Gifts and Benefits Policy
Manager Parliamentary Support and Information	TIPP5.04	Public Interest Disclosures Internal Reporting Policy
Director of Internal Audit and Risk	TIPP5.01A	Risk Appetite Statement Policy
Director of Internal Audit and Risk	TIPP5.02	Risk Management in Treasury Policy

2.9 Document Control

2.9.1 Document Approval

Name & Position	Signature	Date
Secretary	Endorsed	02/11/16
Executive Director, Corporate	Endorsed	02/18

2.9.2 Document Version Control

Version	Status	Date	Prepared By	Comments
1.0	Final	November 2016	Virginia Tinson	
2.0	Final	February 2018	Virginia Tinson	Remove LSC references; insert updated consequence table; insertion of new RAS; updating policies' section
2.0	Final	August 2018	Virginia Tinson	Align to ISO 31000:2018; reference introduction of target residual ratings
2.1	Final	August 2020	Su-Lin Macdonald	Updated to provide examples and to enhance readability for staff across agency

2.9.3 Review Date

This Framework will be reviewed every two years or earlier if required.
It may be reviewed earlier in response to post-implementation feedback from Divisions.

Appendix 1: Risk Categories

The risk categories are provided to assist with the identification and understanding of risks that may exist in Treasury's operations. The library is not an exhaustive list of all risks but is intended as a guide only.

Risk Category	Specific Risk	Key Risk Issue
Advice	Provision of advice	The risk that Treasury provides poor quality or inaccurate or inadequate financial/ economic/ commercial/budget/general policy advice.
Asset Management	Access and control of sensitive information	The risk that controls surrounding access to sensitive documents is inadequate to safeguard, track and restrict access to the sensitive information.
	Protection of cash and fixed / mobile assets	Controls over the custody of cash and assets may not be adequate and lead to loss, theft or mismanagement.
Business Continuity	Reliance on single supplier	Risk that supply of critical services or equipment is concentrated in a single supplier. May result in a significant disruption to Treasury's activities or ability to operate or adequately service clients if the supplier's business is unable to meet its contractual obligations.
	Back-up and (off-site) storage of records	Risk that data back-up arrangements are inadequate. As a result, critical data may not be regularly backed-up and stored securely off-site to ensure IT systems can be recovered in the event of an unexpected disruption.
	Terrorist or another physical event	The risk that Treasury is unprepared to respond successfully to a terrorist incident or major disaster
Compliance / Regulatory	Treasury policies and procedures	The risk of failing to develop necessary management protocols, e.g. policies, standards or codes etc with a resultant breach causing a financial loss or an impact to Treasury's image and reputation.
	Regulatory compliance	The risk of not identifying, complying with and monitoring requirements of legislation.
Contract Management (Outsourced and In-housed Services)	Adequacy of legal agreements	The risk that Treasury's legal rights are not enforceable due to the inadequate contractual documentation.
	Service requirements and performance of both parties Shared Services	The risk of cost and performance targets not being achieved by service providers due to insufficient or ineffective monitoring. The risk of inadequate Key Risk Indicators.
Corporate Governance	Governance	The risk that inappropriate oversight or practices impair the ability of the Treasury Extended Leadership Team to make appropriate decisions or fulfil its reporting obligations.
Financial	Budget setting and management	The risk of inadequate/poor quality budget setting and monitoring processes.
Information Technology	Fit for Purpose	The risk that existing Information technology infrastructure does not meet the business requirements of end users including functionality, cost, maintenance and security issues.
	Day to day availability	The risk of loss of connectivity will result in reduced productivity.
Work Health and Safety (WH&S)	Health and Safety	The risk of failing to provide documented guidance to managers to implement a safe workplace and practices.
Operations & Service Delivery	Delegations of Authority	The risk that the Delegations of Authority are unclear. This may be due to poor communication of the delegations, due to them being not fully documented or due to a lack of management oversight.

Risk Category	Specific Risk	Key Risk Issue
	Management reporting	The risk that management reporting is not available, inaccurate, incomplete or not delivered in a timely manner.
	Fraud and corruption	The risk that inadequate systems and security allows unauthorised access to information and/or misuse of position. Also, the risk that Treasury's systems or processes could be subject to sabotage with the objective of interrupting its operations.
	Organisational culture	The risk that inappropriate culture increases opportunity for fraudulent conduct. The risk that ineffective change management and inconsistent procedural compliance impact upon the objectives of Treasury.
People & Capability	Staff development	The risk that inadequate practices are in place to maintain staff core / other capabilities.
	Performance Management	The risk that inadequate practices are in place to assess staff's performance against organisational expectations including processes to address identified gaps.
	Employer of choice	The risk that Treasury cannot attract and retain appropriately skilled talented staff.
	Industrial Relations	The risk of industrial relations adversely affecting operations, damaging morale, flexibility and goodwill.
	Unfair dismissal and unfair work practices	Non-compliance with Code of Ethics and Conduct and Ethics, the Award and the GSE Act 2013 and established personnel practices.
	Resource management	The risk that the appropriate staff are not available to meet workloads.
Project	Adequacy of project management skills	The risk of failing to properly plan and/or implement a project successfully on time and within budget.
	Project approval process	The risk of lack of technical, risk assessment, financial or commercial rigour leading to projects, which would not otherwise have been undertaken.
Stakeholder Management	Stakeholder requirement	The risk of failing to meet stakeholder requirements and expectations.
Strategic	Image / reputation management	The risk that Treasury's image / reputation is diluted or damaged over time.
	Strategic alliances Strategic Goals	The risk that strategic alliance partners' objectives are inconsistent or in conflict with Treasury's strategic vision or the intended benefit/opportunity is not realised. The risk that Treasury's results do not meet goals thereby impacting on reputation / image of Government.

Appendix 2: Analysing Risk - Likelihood & Consequence rating

Table 2: Likelihood Table

Likelihood Rating	Description	Frequency	Probability
Very Likely (5)	The event will almost certainly occur within next twelve months.	Risk event could occur up to several times within the next twelve months or during project life, whichever is shorter.	80% or greater probability of the event occurring within the next 12 months, and / or the life of the project (where applicable for Projects).
Likely (4)	The event is likely to occur within next twelve months.	Risk event is likely to occur once in the next twelve months or during project life, whichever is shorter.	Less than 80% probability of the event occurring within the next 12 months, and / or the life of the project (where applicable for Projects).
Possible (3)	The event could occur in some circumstances.	Risk event may occur during the next twelve months or during project life, whichever is shorter.	Less than 50% probability of the event occurring within the next 12 months, and / or the life of the project (where applicable for Projects).
Unlikely (2)	The event is not expected to occur during normal operations.	Risk event is unlikely to occur in the next twelve months or during project life, whichever is shorter.	Less than 25% probability of the event occurring within the next 12 months, and / or the life of the project (where applicable for Projects).
Rare (1)	The event may occur only in exceptional circumstances.	Risk event is not expected to occur for some time or during project life, whichever is shorter.	Less than 10% probability of the event occurring within the next 12 months, and / or the life of the project (where applicable for Projects).

Table 3: Consequence Table

Scale Category	Insignificant (1)	Minor (2)	Moderate (3)	Major (4)	Extreme (5)
	Risk has negligible consequences and can be managed within existing resources and budget.	Risk has minor short-term impact on the achievement of objectives and can be resolved within existing resources and budget.	Risk may affect the achievement of some objectives and can be resolved through the reassignment of resources.	Major impact that would disrupt business activities and may threaten Treasury's ability to achieve organisational objectives.	Severe threat to Treasury's functions and ability to fulfil its purpose and organisational objectives, with extreme state-wide impact.
FINANCIAL Whole of Government	Minor errors in costings or accounting and/or the advice included in the budget. Projected shortfall in the State being able to eliminate unfunded super liabilities by 2030 is able to be addressed by remedial action by 2030.	Annual growth in general government expenses exceeds long-term revenue. The budget is not delivered on time. Rating agencies put the State's Triple-A credit rating on negative outlook. Projected modest shortfall in the State being able to eliminate unfunded super liabilities by 2030.	Agencies not adhering by <$100m to Treasury allocation letter limits and Treasury not adequately advising Government. Rating agencies include the State on a watch list. Projected large shortfall in the State being able to eliminate unfunded super liabilities by 2030. The forecasted budget result is not achieved by an amount between $100m and $250m.	A qualification of the accounts. Providing advice which causes a major breach of key legislation, for example the *Public Finance and Audit Act 1987*. Loss of State's Triple-A Credit rating. Agencies not adhering by $100m or > to Treasury allocation letter limits and Treasury not adequately advising Government. Projected extreme shortfall in the State being able to eliminate unfunded super liabilities by 2030.	Policy or investment advice to Government has severe state-wide implications on the economy, environment and/or threatens security and safety. The Treasurer/Minister has to resign as a result of continued poor advice from Treasury and loss of confidence in government. Extremely severe impact on State finances as a result of poor advice and administration by Treasury whereby the State cannot deliver on its obligations.
FINANCIAL **Treasury Agency**	Negligible under or over spend by, whichever is lowest, <$500K or <0.5% of full year total expenses budget Capital under or over-spend <3%	Minor under or over spend by, whichever is lowest, $500K to <$1m or 0.5% to <1% of full year total expenses budget, with minor impacts Capital under or over-spend 3% to <10%	Moderate under or over spend by, whichever is lowest, > $1m to <$5m or >1% to 5% of full year total expenses budget, with significant impacts Capital under or over-spend >10% to <15%	Major under or over spend by, whichever is lowest, $5m to <$10m, or 5% to <10% of full year total expenses budget, with major Treasury wide impact Capital under or over-spend >15% to <20%	Severe under or over spend by, whichever is lowest, $10m+ or 10%+ of full year total expenses budget, with severe Treasury wide impact Capital under or over-spend 20%+

Scale	Insignificant (1)	Minor (2)	Moderate (3)	Major (4)	Extreme (5)
REPUTATION, including: • Political	No media attention Negligible impact on reputation	Minor level adverse publicity in local media, no broader media reporting Readily controlled negative impact on reputation	Moderate adverse publicity with coverage in local and/or state-wide media only Treasurer's enquiries Verbal advice required to Treasurer's or Premier's Office or (big) Treasury	State-wide and/or national severe adverse publicity lasting for greater than one week Lead and/or major story in media, with potential for lasting damage to reputation of Treasury Written advice and follow up with Treasury Office and/or Premier's Office	Royal Commission inquiry, Major ICAC investigation/hearing, or adverse and published Auditor General findings
STAKEHOLDER ENGAGEMENT / RELATIONS	No loss of client or stakeholder confidence	May create some short-term, temporary concern amongst clients or stakeholders	May create temporary loss of credibility to clients or stakeholders Treasurer's enquiries	Serious loss of credibility with clients, Treasurer's Office and key stakeholders	Critical long-term loss of credibility with clients, Treasurer's Office and key stakeholders
PEOPLE & CAPABILITY. including: • Workplace Relations, and • Staff Morale and Engagement	Very limited/transient staff engagement problems No threat to critical skills or business knowledge No threat to attracting talented and retaining staff Little or no effect on operations	Minor staff engagement problems Short-term loss of skills and business knowledge, effect absorbed within routine operations Minor threat to attracting talented staff to a few key roles and the loss of a small number of key staff with minimal effect on the business	Key person loss Loss of a critical skill or some loss of skills and corporate knowledge with programs/strategies compromised Moderate threat to attracting talented staff to a number of key roles Some minor industrial disputes	Loss of critical skills and key people, programs/strategies cannot be delivered Capacity to attract quality staff is significantly compromised Major industrial disputes	Severe loss of critical skills, key people and business knowledge, programs/strategies are not delivered Widespread poor engagement and staff moral with high staff turnover Inability to attract talented staff to numerous roles Significant long-term industrial disputes involving union/large staff numbers
WORK, HEALTH AND SAFETY (Our people and the public)	Minor injury, first aid treatment, minimal or no lost work time	Moderate injury, medical treatment and lost work time resulting in compensation claim	Serious injury resulting in hospitalisation and/or significant compensation or public liability claim	Potential for multiple injuries Dangerous occurrence requiring notification to SafeWork NSW Multiple worker's compensation claims from Treasury employees or public liability claims	Extreme event involving multiple injuries or fatalities and/or dangerous occurrence from extensive/catastrophic damage to property and infrastructure Notification to and investigation by SafeWork NSW

Scale	Insignificant (1)	Minor (2)	Moderate (3)	Major (4)	Extreme (5)
COMPLIANCE including: • Regulatory, • Legislative, and • Environment • Staff Morale and Engagement	Negligible non-compliance with minimal impact on operational business processes Rare legislative non-compliance, little or no effect on business operations Negligible impact on local environment	Regulatory non-compliance requiring local staff effort to rectify Isolated legislative non-compliance, effect managed at operational level Minimal impact on local environment	Regulatory non-compliance requiring management effort to rectify and / or limited notification to a regulatory authority. Control failures resulting in frequent legislative non-compliance Significant effect on Treasury business operations requiring changes to business processes Some impact on local environment	Regulatory non-compliance resulting in notification by a regulatory authority Grossly negligent breach of legislation Formal investigations, disciplinary action, ministerial involvement Substantial impact on local and surrounding environments	Significant non-compliance which may result in fine to agency and/or prosecution Widespread serious or wilful breach Prosecutions, dismissals and Parliamentary scrutiny Severe impact on local and surrounding environments
PROJECT	No threat to overall timeframe Negligible cost increase <5% Scope increase/decrease barely noticeable Quality degradation barely noticeable Insignificant impact on benefits	Delay 5% to <19% of original timeframe 5% to <19% cost increase or <$100k, whichever is less Minor areas of scope affected Objective achieved but slight reduction in quality 5% to <19% benefits not delivered	Delay 20% to <39% of original timeframe 20% to <39% cost increase or $100k to <$250k, whichever is less Major areas of scope affected Objective achieved but quality reduced significantly 20% to <39% benefits not delivered	Delay 40% to <64% of original timeframe 40% to <64% cost increase or $250k to <$500k, whichever is less Scope increase/decrease unacceptable Quality reduction unacceptable with major impact on objectives 40% to <64% benefits not delivered	Delay 65% to 100%+ of original timeframe 65% to 100%+ cost increase or $500k+, whichever is less Product or services does not meet key requirements Quality issues lead to non-achievement of objectives and outcomes are not delivered 65%+ benefits not delivered

Scale	Insignificant (1)	Minor (2)	Moderate (3)	Major (4)	Extreme (5)
OPERATIONS & SERVICE DELIVERY **including:** • Fraud and Corruption	Minimal disruption to service delivery of operations Short infrequent disruptions to IT Services (<4 hours) No threat to reputation and managed within the business unit .	Minor disruption to service delivery and operations (1 to 2 hours) IT Services not available for <1 day Isolated fraud event by one employee Minor threat to reputation and managed within the business unit No press coverage (or very limited)	Moderate disruption to operations due to restricted supply or services, requiring some alternate arrangements by management IT Services not available for >1 day and <2 days Multiple fraud events by one or more employees for a limited period Moderate damage to reputation to Treasury with limited press coverage and external inquiry investigation by NSW Police and / or ICAC	Key Treasury operations / service provision disrupted Access to a Divisional office or several building levels/floors denied >2 days and <5 days IT services not available Treasury wide for >2 working day and <5 working days Multiple fraud events occurring for a sustained period by one or more employees Major damage to reputation to Treasury resulting in an external inquiry and investigation by ICAC and/or NSW Police resulting in prosecution of perpetuator(s) National news coverage	Total shut down of operations and or access to premises denied >5 days Long-term loss of business capability Very significant and long-term disruption to supply or services Very few or no alternate arrangements available Significant level of community, client and executive dissatisfaction Significant Treasurer and/or Secretary intervention and dissatisfaction IT Services not available Treasury wide for >5 days or more Systemic fraud across parts of the organisation for a sustained period and involving collusion of senior staff Severe damage to reputation to Treasurer and Treasury resulting in an external inquiry and investigation by ICAC and/or NSW Police and prosecution of perpetuator(s) with likely custodial sentence Sustained negative press coverage

Table 4: Risk Rating – The Risk Level Matrix

NSW Treasury Risk Matrix					
A	**Consequences**				
Likelihood	**Insignificant 1**	**Minor 2**	**Moderate 3**	**Major 4**	**Extreme 5**
Very Likely 5	**M 5**	**S 10**	**H 15**	**E 20**	**E 25**
Likely 4	**L 4**	**M 8**	**S 12**	**H 16**	**E 20**
Possible 3	**L 3**	**M 6**	**M 9**	**S 12**	**H 15**
Unlikely 2	**L 2**	**L 4**	**M 6**	**M 8**	**S 10**
Rare 1	**L 1**	**L 2**	**L 3**	**L 4**	**M 5**

Table 5: Residual Action Requirements

	Residual Review Requirements
E 20-25	**Extreme Risk:** Extreme adverse effect on Treasury **Immediate Action Required, for Secretary/Leadership Team attention** Treatment action plans should be put in place to reduce the risk level further
H 15-19	**High Risk:** Potential for high adverse effect on Treasury **Executive Management attention needed** Treatment action plans should be put in place to reduce the risk level further
S 10-14	**Significant Risk:** Potential for significant adverse effect on Treasury **Senior Management attention needed** Treatment action plans could be used to reduce the risk level further
M 5-9	**Moderate Risk:** Moderate potential for adverse effect on Treasury **Reviewed by the next level of management when initially rated** Manage by Standard Procedures
L 1-4	**Low Risk:** Low potential for adverse effect on Treasury **Ongoing control as part of a business as usual management.**

Appendix 3: Control Assessment- Design, Performance & Effectiveness

Table 6: Control Design

Rating Category		Control Design
1	**Very Strong**	Designed in such a way that will reduce risk substantially. High degree of automation or documented formalised processes.
2	**Strong**	Designed in such a way it will reduce risk substantially. Very automated or documented formalised processes. Rare exceptions. Places reliance on knowledge/actions of key persons.
3	**Adequate**	Designed in such a way it will reduce risk. Expected to fail at times, however within acceptable appetite. Places reliance on knowledge/actions of key persons.
4	**Limited**	Designed in such a way it will reduce some aspects of risk. Likely to fail requiring remedial effort and actions. Places heavy reliance on knowledge/actions on persons to manually address exceptions/incidents.
5	**Weak**	Poor design even where used correctly. It provides little or no protection. Only addresses part of the risk requiring additional work arounds or manual processes to make up for deficiencies. Extreme reliance on knowledge/actions of key persons.

Table 7: Control Performance

Rating Category		Control Performance
1	**Very Strong**	The control operates as intended and consistently. Never known to fail in the past, highly unlikely to fail in a short to mid-term.
2	**Strong**	The control operates as intended and consistently. Control is mature and unlikely to fail significantly within 12-month period. Has significantly addressed the risk.
3	**Adequate**	The control has experienced a failure in the past 12 months and is not expected to experience more. Rates of failure are deemed within appetite or risk tolerance but not outside acceptable risk tolerance levels.
4	**Limited**	The control has experienced failures in the past 12 months and is expected to experience more, potentially more frequently. Rates of failure are deemed outside acceptable risk tolerance levels.
5	**Weak**	Consistently not operating as intended, immature, operating inappropriately or inconsistently. Rates of failure are significant, and deemed outside acceptable risk tolerance levels.

Table 8: Control Effectiveness

Control Effectiveness						
		Control Performance				
		Very Strong	Strong	Adequate	Limited	Weak
Control Design	Weak	None or Totally Ineffective	None or Totally Ineffective	None or Totally Ineffective	None or Totally Ineffective	None or Totally Ineffective
	Limited	Largely Ineffective	Largely Ineffective	Largely Ineffective	Largely Ineffective	None or Totally Ineffective
	Adequate	Partially Effective	Partially Effective	Partially Effective	Largely Ineffective	None or Totally Ineffective
	Strong	Substantially Effective	Substantially Effective	Partially Effective	Largely Ineffective	None or Totally Ineffective
	Very Strong	Fully Effective	Substantially Effective	Partially Effective	Largely Ineffective	None or Totally Ineffective

Table 9 Control Effectiveness Definitions

Rating Category		Description
1	Fully Effective	Nothing more to be done except review and monitor the existing controls. Controls are well designed for the risk, address the root causes and Management believes that they are effective and reliable at all times.
2	Substantially Effective	Most controls are designed correctly and are in place and effective. Some more work may be done to improve operating effectiveness or Management believes that they are effective and reliable most of the time.
3	Partially Effective	While the design of controls may be largely correct in that they treat most of the root causes of the risk, they are not currently very effective or Some of the controls do not seem correctly designed in that they do not treat root causes, those that are in place are performing at least somewhat effectively.
4	Largely Ineffective	Significant control gaps. Either controls do not treat root causes or they do not operate at all effectively.
5	None or Totally Ineffective	Virtually no credible control. Management has no confidence that any degree of control is being achieved due to poor control design and/or very limited operational effectiveness.

Appendix 4: Risk Assessment Template

Business Unit:	

1. Risk Identification			
Risk No.:	1.	2.	3.
Risk Title: *Title should be short by clear*			
Risk Description:			
2. Risk Assessment			
Cause Factors: *Identify those factors that might lead to the risk/opportunity occurring*			
Impacts: *Identify the impacts on Treasury/State if the risk/opportunity occuringt*			
Inherent Likelihood Rating: *Use Likelihood Table*			
Inherent Consequence Rating: Use Consequence Table			
Inherent Risk Rating: *Likelihood rating combined with Consequence rating*			

3. Risk Assessment *(continued)*			
Existing Key Controls: *Identify key controls in place to mitigate risk*	1. 2. 3.	1. 2. 3.	1. 2. 3.
Control Description *Describe the control how it relates to this particular risk*	1. 2. 3.	1. 2. 3.	1. 2. 3.
Control Design Rating: *Is the design of the current controls adequate? Refer to control design rating table.*	1. 2. 3.	1. 2. 3.	1. 2. 3.
Control Performance Rating *Is the performance of the current controls adequate? Refer to control performance rating table.*	1. 2. 3.	1. 2. 3.	1. 2. 3.
Control Effectiveness Rating *Design rating combined with performance rating. Rating will be autogenerated in Protecht, based in Control Design and Performance.*	1. 2. 3.	1. 2. 3.	1. 2. 3.
Overall Control Rating *The overall effectiveness when all controls are considered*			

Residual Likelihood Rating:			
Residual Consequence Rating:			
Residual Risk Rating will be auto generated based on the combination of residual likelihood and consequences			
5. Risk Treatment – If risk is not accepted i.e. residual rating still too high			
Management Action: *As prescribed in the Framework*			
Additional Risk Mitigation Strategies / Treatments: *Identify those strategies in addition to the existing controls that will be implemented to further manage this risk.*			
Responsibility: *The position supervising the implementation of this risk treatment strategy.*			
Timetable: *When will implementation of the strategies be completed?*			

Risk Assessment Undertaken by:	
Risk Management Strategies Approved by:	
Date of Approval:	
Date of Review:	

Appendix 5: Glossary of Terms

Term	Meaning
Compliance risk	Compliance risk is exposure to legal penalties, financial forfeiture and material loss Treasury faces when it fails to act in accordance with industry laws and regulations, internal policies or prescribed best practices.
Compliance register	Tool for identifying and monitoring compliance with legislation, regulation or state-wide policy. Raises staff awareness of legal obligations and aims to embed/maintain a regard for regulatory compliance in the culture.
Consequence	Positive or negative impact on an objective
Controls	Currently existing processes, policy, procedures or other actions that act to minimise negative risks and/or enhance opportunities
Failure Mode	The manner by which a failure is observed; it generally describes the way the failure occurs and its impact on the operation of the system
Incident	An event that has the capacity to lead to loss of or a disruption to Treasury's operations, services, or functions – which, if not managed, can escalate into an emergency, crisis, or disaster.
Inherent Risk	Initial assessment of the consequence and likelihood a risk. Does not take into account the impact of existing controls.
Likelihood	The chance of something happening. May be defined, measured or determined objectively or subjectively and described verbally or mathematically.
Operational risks	Risks associated with day-to-day operational performance (e.g. staff safety or availability, mechanical or technological risks, most corruption risks, etc)
Project risks	Risks which may significantly affect the likelihood of a project being completed to planned time, quality and/or budget.
Residual risk	The consequence and likelihood of a risk when existing controls are taken into account.
Risk	The effect of uncertainty on Treasury's objectives
Risk assessment	The overall process of identifying, analysing and evaluating risks and their controls. May involve qualitative or quantitative assessment.
Risk avoidance	An informed decision to not become involved in or to withdraw from a risk situation
Risk management	The culture, processes, coordinated activities and structures that are directed to realising potential opportunities or managing adverse effects. It includes communicating, consulting, establishing context, identifying, analysing, evaluating, treating, monitoring and reviewing risks.
Risk management plan	A plan which takes the Risk Register further, considering Treasury's appetite for the risk, any gaps between existing controls and appetite, and proposing treatments for any remaining risks, which are assigned to owners, given deadlines and monitored. In Treasury, at cluster level, there is one document which is the Risk Register and Management Plan.
Risk owner	Person or entity with the accountability for a specified risk. In Treasury, the Secretary is accountable for all risks however individual or Group owns manage specific risks.
Risk register	System/document recording each risk identified, its rating and existing controls.
Risk tolerance/ Risk appetite	Risk tolerance is the amount of risk that Treasury is comfortable taking, or the degree of uncertainty that it is able to handle.
Risk transfer	Refers to the shifting of the burden of loss to another party through legislation, contract, insurance or other means. It can also refer to the shifting of a physical risk or part thereof elsewhere
Risk treatment	Actions planned and undertaken to deal with any gaps between existing controls and the agreed appetite for the risk.
Strategic risks	Internally or externally generated forces that may have a significant impact on the achievement of strategic objectives.