Risk Management Policy and Framework

STATE LIBRARY®
NEW SOUTH WALES

Policy No:	**PD/60**	**TRIM File No:**	**55159**
Version:	**1.0**	**Last Amendment:**	**13 September 2016**
Policy owner/sponsor:	**Director, Operations and Infrastructure & CFO**		
Branch contact:	**Project and Planning Officer, Operations**		
Approved by:	**Executive**		
Date approved:	**13 September 2016**		
Next review:			

1. Introduction

The Risk Management Policy and Framework has been developed in accordance with the NSW Government *Internal Audit and Risk Management Policy for the NSW Public Sector* (TPP15-03) and *NSW Risk Management Toolkit for Public Sector Agencies* (TPP12-03). The Library's approach to risk management is consistent with the Australian/New Zealand Standard *Risk Management – Principles and guidelines* (AS/NZS ISO 31000:2009).

Effective risk management processes are also required by the *Public Finance and Audit Act 1983* and the *Work Health and Safety Act 2011*. The *Annual Reports (Statutory Bodies) Regulation 2015* requires agencies to report on their risk management and insurance arrangements and attest annually to compliance with the core requirements of TPP15-03.

2. Policy Statement

The State Library is committed to developing a risk management culture, where risk management is seen as integral to the achievement of our objectives at all levels and where all staff are alert to risks, are capable of an appropriate level of risk assessment and confident to report risks or opportunities perceived to be important to our priorities.

3. What is Risk and Risk Management?

A risk is defined as the effect of uncertainty (either positive or negative) on organisational objectives. Risks can be Strategic (external context) e.g. political, economic, social, technological, legal or reputational, or Operational (internal context) affecting physical premises, people, procedures, processes, compliance or reporting. Negative consequences can contribute to strategic, operational, systems or financial failures or deficiencies.

Risk management involves "the activities and actions taken to ensure an organisation is conscious of the risks it faces, makes informed decisions in managing these risks, and identifies and harnesses potential opportunities."

4. When is Risk Management used in the Library?

Risk management should be incorporated into all of the Library's functions and responsibilities in order to identify and manage opportunities and risks that should be considered during:

- Strategic, business, service and workforce planning
- Budget planning and monitoring
- Planning, development and implementation of new service delivery methods,

programs or projects

- Changes to service delivery, projects or agreed levels of activity
- Planning, development, implementation and maintenance of new and existing information and communications technology hardware and software systems
- Development and implementation of new or revised policies, procedures and guidelines
- Planning and implementing capital projects and programs
- Procurement and acquisitions processes.

5. Risk Management Framework

The Library recognises that there is the potential for risks in various aspects of our operations. However, it is also important to consider the potential opportunities or benefits that can be achieved. The Risk Management Framework describes the process for managing risk throughout the Library. It provides a structure for a consistent approach to identifying and categorising risk and for embedding risk management across all of the Library's operations. The Framework accommodates strategic, operational and project risks.

Strategic risks are those risks that apply to the Library as a whole and could adversely affect the achievement of our strategic outcomes and/or damage the Library's reputation. These risks are managed by the State Librarian & Chief Executive and the Directors.

Operational risks relate to the risks that may impact delivery of specific services and programs and are managed by the relevant division, branch or program manager.

Project risks may affect the delivery of a project on time, within budget, or within acceptable quality parameters. They are managed by the project manager in consultation with the project sponsor. The Library's Project Management Framework includes risk assessment and management criteria, and all projects have a risk register that is documented during the planning phase, monitored during program development and reviewed at the project execution or completion stage.

6. Guiding Principles for Risk Management

- All State Library staff have a responsibility to identify and manage the risks that relate to their particular areas of work, in a manner consistent with the Library's policies and guidelines on risk management
- Risk management is used on a consistent and systematic basis in all areas and major programs and business processes, with risks rated in accordance with the matrix in Attachment 2
- Risk management in the Library is consistent with the Australian/New Zealand Standard *Risk Management – Principles and guidelines* (AS/NZS ISO 31000:2009 and the Library's *Code of Ethics and Conduct*
- The level of response to a risk needs to be proportionate to the level of the risk and risk appetite
- Where appropriate, the Library will use risk-sharing as a means of managing risk e.g. by using insurance in contracts with third party providers
- The Library is responsible for ensuring that staff and managers have the necessary skills and risk management tools to undertake effective risk management on a consistent basis across the Library.

7. Risk Appetite

Risk appetite defines the amount and type of risk that the Library is willing to accept in pursuing our objectives. There will be a range of appetites for different risks which need to align with corporate priorities and objectives. Risk tolerance describes the level of risk the Library will cope with or bear.

Overall the Library adopts a conservative, informed and measured risk-taking approach in managing the organisation. The Library has:

No appetite for:

a) Deliberate or reckless non-compliance with government policy and regulatory requirements
b) Compromising staff, public or contractor safety and welfare
c) Fraud, collusion or acts that lead to reputational damage.

A **low appetite** for:

a) Failure to meet stakeholder and donor commitments
b) Systems failures or information security breaches
c) Failure to safeguard the collections
d) Failures in decision making that compromise the long term financial stability
e) Failures in rigour and transparency in the public libraries funding and grants processes.

A **moderate risk appetite** in terms of the operational risk associated with the implementation of change and key strategic plans, and risks that could affect the Library's ability to build and sustain reputational strength with key stakeholders.

A **strong risk appetite** for:

a) Organisational or process improvement
b) Stakeholder engagement and community participation in consultation and service delivery improvements
c) Actions that promote NSW Government Core Values and the Library's *Code of Ethics and Conduct*
d) Innovation and sustainability.

There are no absolute tolerance limits available in making decisions about risk. Identifying, assessing and managing risk requires the exercise of informed, careful and prudent judgment, taking account of the controls that are in place to prevent risks from occurring, or preventing or mitigating the consequences if the risk event did occur. There is also a need to consider the potential opportunities and benefits that can be achieved.

The Executive Committee will formulate the Library's risk appetite in the context of the Library's strategic plan and recommends its approval to the Library Council. Each review of the *Business Risk Map* should include discussion of risk appetite to assist with understanding the limits to risk taking and the parameters around opportunities. This will ensure the appetite remains within the bounds of available funding and the strategic plan, and to ensure consistency across the Library.

8. Risk Delegations and Escalation

The following delegations apply to the management of risks:

- For risks rated as Very High or High – management strategies should be approved by the Executive Committee
- For risks rated as Medium or Low – management strategies should be proposed by

managers as part of their normal operations and approved by the relevant director.

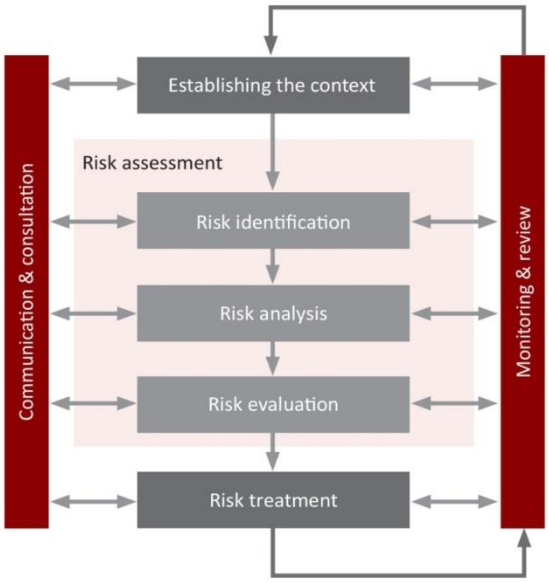
There is a direct link between the severity of a risk and the management level to which it should be escalated for action. If a risk is beyond the manager's control or delegation to effectively control or mitigate it, the manager should escalate the risk to an appropriate, more senior level of management.

The Executive Committee may escalate risk issues to the Audit and Risk Committee and Library Council if a risk rated greater than Very High or unusual is identified through the risk management process, the audit process or some other activity or event. It may be necessary to escalate such risks quickly and outside of the regular review process. The appropriateness of risk delegations is evaluated during the review of the *Business Risk Map*.

9. Risk Management Process

The risk management process occurs at both an organisation level ('top-down') and business unit level ('bottom-up'). All divisions and branches should apply risk management and categorise and rate risks in line with the *Business Risk Map*. The level of response to a risk should be proportionate to the level of the risk and take into account its effects and the cost of mitigation.

The risk management standard (AS/NZS ISO 31000:2009) illustrates the risk management process as follows:



Communication and consultation
Effective communication, consultation and education in risk management are essential to achieve a successful integration of risk processes into functional activities. Documenting these processes through the *Business Risk Map* provides a consistent and accessible approach to risk management for all staff. It also provides a framework for identifying and managing unexpected risks.

Communication and consultation should take place throughout the risk management process. The *Business Risk Map* review may involve managers, staff and stakeholders to ensure understanding of the basis on which decisions are made and risks are assessed. Consultation with internal and external stakeholders can also assist with developing the risk profile and ensuring that impacts and potential risks and opportunities are identified.

Establishing the context
Because risk is the effect of uncertainty on objectives, the first step is to understand what those objectives are. It means understanding the goals and objectives in the Library's strategic and operational plans and the Library's operating environment such as the political, economic, social, environmental, technical and policy context and their potential affect. It may include review of available resources and impacts such as legislation and government policy obligations.

Risk assessment
Risk identification determines what, where, when, why and how risks could arise, and the effect this would have on achieving objectives. A range of internal and external sources may be used to assist in the identification of risks, such as business and project plans and policies or the outcomes of internal audits, program reviews or research projects. The Library's relationships with stakeholders, clients, supporters and the broader community and its profile in the government, arts and cultural sectors are also influences.

The Library's risk categories are classified as strategic, operational or fraud and corruption risks, and the current categories are listed in Attachment 1. The risk categories are reviewed and updated regularly.

Risk analysis involves considering the range of potential causes or triggers, the sources of risk, any existing controls that may be in place to prevent or deal with the risk and assessing their effectiveness.

This helps to produce a risk rating that is calculated from two risk elements:

i. **Likelihood** rating - an assessment of the potential frequency of occurrence without reference to known management controls and mitigating processes; and
ii. **Consequence** rating - an assessment of the potential people, financial, reputation, compliance or business process/system impact.

These elements form the risk matrix against which each risk that has been identified through risk analysis is ranked and prioritised and by which the need for treatment is assessed. The Library's risk matrix and the ratings tables are at Attachment 2.

Risk evaluation determines those risks that are acceptable and those that require further treatment, taking into account the established context, risk ratings and agreed organisational risk appetite. For example, if the risk falls into the Low category, it may be accepted with minimal further treatment. Other reasons for accepting a risk may be that the cost of treatment outweighs the benefit or that opportunities may exceed the threat to the extent that the risk is acceptable. These risks should be monitored and periodically reviewed to ensure they remain acceptable.

Managing risks
Risks are usually managed by controls, which are the measures or procedures in place to manage the risks either by maintaining their current rating or implementing mitigation strategies to reduce or manage the level of risk. The Library's distributed governance model allocates responsibility for managing the controls and measuring the effectiveness of mitigation strategies to the relevant Directors and managers, who report through the review of the *Business Risk Map*.

Risk treatment requires assessing and selecting one or more options for mitigating risks and implementing the selected options through a treatment plan, taking funding and other resource considerations into account. Risk treatment also involves formulating responses to

deal with unacceptable risks, including actions to reduce the likelihood or consequences of an event and formulating contingency plans.

The treatment plan is documented in the risk register and includes the risk ratings derived from the risk matrix as follows:

Previous (or initial) risk rating
This is the risk assessed at the time the risk was first identified and in the absence of any controls or mitigation strategies; or is the rating that was assigned at the previous review. This rating will assist in determining the importance of existing controls and the extent to which they are relied on to manage the risk.

Residual (or target) risk rating
The residual risk rating will reflect any change in the previous risk rating arising from any additional controls or mitigation strategies put in place since the previous review. This rating reflects the expected future level of the risk if and when all treatments (including those currently in train) are successfully implemented.

When a new risk is identified it is possible that the initial and current risk rating will be the same, until such time as the identified controls or treatments begin to be implemented.

The risk register template is at Attachment 3.

Monitoring and review is a continual process that confirms that risks and the effectiveness of the controls and risk treatments are monitored and reported to ensure that any changing context and priorities are managed and any emerging risks are identified. The effectiveness of the controls impacts the risk and its rating.

The Executive Committee reviews the *Business Risk Map* twice each year to ensure that appropriate controls and mitigation strategies are being implemented, to assess that the target or residual risk ratings are being achieved or to take remedial action if the ratings are under threat of not being achieved.

The Audit and Risk Committee oversees the Executive Committee's risk assessment findings and makes recommendations to the Library Council. The assessment is also used to identify areas of focus for the internal audit program and may inform the research and evaluation program.

10. Communication and training

All staff should be informed about the Risk Management Policy and Framework and have the opportunity to discuss risks and opportunities in their area of work. The Library's risk appetite should be understood and taken into account during strategic and business planning. This document is accessible on the website and changes will be communicated through the usual staff communication channels.

Risk management awareness training should be provided to managers and staff with responsibility for major projects through the Project Management Framework. It should be included in the learning and development program.

11. Responsibilities

The **Executive Committee** has overall responsibility for managing risk and assessing the performance and effectiveness of controls through reviewing and monitoring of the *Business Risk Map*. Material cross-divisional risks should also be reflected on the *Business Risk Map* and monitored by the Executive Committee.

The **State Librarian & Chief Executive** is accountable for all risks and:

- Championing a risk management culture that includes a focus on continuous improvement and identifying opportunities as well as risks
- Ensuring the *Business Risk Map* is current and risk management strategies are implemented to mitigate risk
- Ensuring appropriate resources are allocated to risk management and to implementing controls and mitigation strategies
- Integrating risk management into the Library's corporate planning and governance processes.

The **Director, Operations and Infrastructure & CFO** is responsible for:

- Maintaining the *Business Risk Map* and reporting to the Audit and Risk Committee and Library Council
- Communicating the Risk Management Policy and Framework throughout the Library
- Providing support, assistance and learning and development in risk management.

Directors are accountable for overseeing the implementation of the Risk Management Policy and Framework within their Division. This includes:

- Ensuring that risks pertinent to the business processes within their control are identified and managed
- Reviewing the progress of their Division's risk management processes and reporting issues as appropriate
- Participating in the Executive Committee's review of the *Business Risk Map*.

Managers and Supervisors are responsible for applying the Risk Management Policy and Framework and relevant mitigation strategies within their areas of control. This includes:

- Reviewing their risk management processes and reporting issues as appropriate
- Implementing recommendations of internal audits related to their areas of responsibility
- Supporting and encouraging staff in managing hazards and risk in the workplace.

All **staff** are responsible for complying with the Risk Management Policy and Framework, including:

- Proactively identifying areas of risk and opportunity
- Reporting incidents, near-misses, and other areas of concern to managers and supervisors
- Complying with policy and procedural requirements to minimise the Library's exposure to risk.

The Library Council of NSW, the Audit and Risk Committee and the Library Executive Committee are core committees with responsibility for overseeing risk management processes and performance.

The **Executive Committee** establishes and reviews the *Business Risk Map* and confirms the risk ratings through discussion of the Library's risk appetite and tolerance and assessment of performance in implementing the controls and mitigation strategies. Cross-divisional risks are also considered.

The **Audit and Risk Committee** will monitor that the Risk Management Policy and Framework is embedded into the Library's corporate governance processes, assess the risk appetite and provide strategic oversight and monitoring of risk activities and performance through the *Business Risk Map*. The Committee reviews and recommends approval by the Library Council.

The **Library Council** discusses the recommended risk ratings and the risk appetite for specific business risks and is responsible for approving the Risk Management Policy and Framework and the *Business Risk Map*.

12. Definitions

Risk: The effect of uncertainty on the achievement of objectives. The chance of something happening that will have an impact on objectives. It is measured in terms of likelihood and consequence.

Risk management: The culture, processes and structures that are directed towards realising potential opportunities whilst managing adverse effects. The process of planning, organising, directing and controlling resources and activities in order to minimise potentially adverse consequences at the least possible cost in accordance with AS/NZS ISO 31000:2009.

Risk management process: The systematic application of policies, procedures and practices to the tasks of communicating, establishing the context, identifying, analysing, evaluating, treating, monitoring and reviewing risk.

Risk appetite: The amount and type of risk the Library is prepared to pursue or retain. The Library's risk appetite is influenced by the risk ratings assigned to the core business risk categories in the *Business Risk Map*.

Residual risk: The remaining level of risk after risk treatment measures have been taken.

Control: An existing process, policy, device or practice that acts to minimise negative risk or enhance positive opportunities.

13. Key legislation and policies

- Internal Audit and Risk Management Policy for the NSW Public Sector. NSW Treasury Policy and Guidelines Paper (TPP15-03)
- Risk Management Toolkit for the NSW Public Sector. NSW Treasury Policy and Guidelines Paper (TPP12-03)
- Public Finance and Audit Act 1983
- Work Health and Safety Act 2011
- Annual Reports (Statutory Bodies) Act 1984 and Regulation 2015
- Code of Ethics and Conduct (Staff and Library Council)

Risk related policies and procedures
There is an extensive range of related Library plans, policies and procedures that support effective risk management and seek to address risk including:

- Internal Audit Plan
- Audit and Risk Committee Charter
- Governance Framework
- Insurance program
- Fraud and corruption prevention policies, including conflict of interest and gifts and benefits policies and registers
- Legislative Compliance Register and Policy
- Financial and administrative delegations
- Policy Management Guidelines
- Project Management Framework
- Business Continuity Plan and Disaster Recovery procedures
- Work Health and Safety policies and processes, including security measures relating to staff, clients, collections, facilities and information and digital assets; incident and hazard

reporting procedures, and emergency evacuation policies and procedures that have been tested and evaluated
- Procurement and asset management plans.

References

1. Audit Office of NSW (2015). Governance Lighthouse – Strategic Early Warning System, 2015.
2. Audit Office of NSW (2002). Performance Audit Report: Managing Risk in the NSW Public Sector, 2002.
3. Standards Australia Ltd/Standards New Zealand (2009). Australia/New Zealand Standard: Risk Management – Principles and guidelines (AS/NZS ISO 31000:2009).
4. Standards Australia Ltd/Standards New Zealand (2013). Handbook: Risk management-Guidelines on risk assessment techniques (SA/SNZ HB 89:2013).

Attachments

1. State Library of NSW Risk Categories
2. State Library of NSW Risk Matrix template, likelihood and consequence assessment tables
3. State Library of NSW risk register template

Document History and Version Control

Version	Date approved	Approved by	Brief description
1.0	13 September 2016	Executive Committee	
1.0	10 October 2016	Audit and Risk Committee	

State Library of NSW Risk Categories

The agreed risk categories as at August 2016 are:

Strategic risks

1. Funding – Operational (S1)
2. Funding – Capital (S2)
3. Expectations of Clients and Stakeholders (S3)
4. Implementation of the Digital Excellence Program (S4)
5. Cyber Security Risk (S5)
6. Relationship with Public Libraries and Local Councils (S6)
7. Enterprise Resource Planning System (S7)

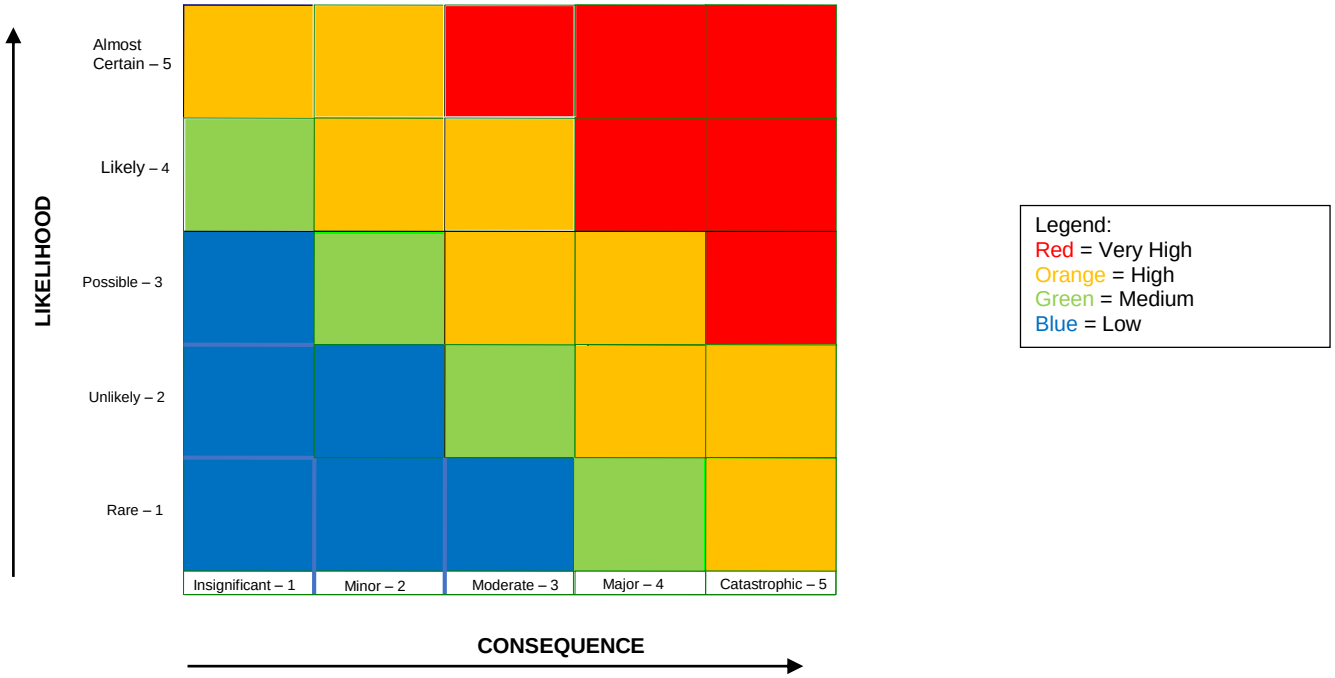
Operational risks

1. Workforce Planning (O1)
2. Collection Management – Physical Security (O2)
3. Collection Management – Digital (O3)
4. Business Continuity Management / Disaster Recovery Planning (O4)
5. Work Health and Safety (O5)
6. Contract and Procurement Management (O6)
7. Building Maintenance (O7)
8. Financial Management (O8)
9. Information Management Compliance (O9)
10. IT Systems Management (O11)
11. Collection Storage (O12)
12. Collection Management (O14)

Fraud and corruption risks

1. Fraud and Corruption (F1)

State Library of NSW Risk Matrix



Legend:
Red = Very High
Orange = High
Green = Medium
Blue = Low

Likelihood and Consequence Ratings Guide (as at April 2016)

Likelihood assessment table

	Descriptor	Description
Likelihood	**Almost Certain**	The event is expected to occur within the next year.
	Likely	The event is more than likely to occur at some stage within 1-2 years.
	Possible	The event may occur at some stage during the next 2-5 years.
	Unlikely	The event is not expected but could occur within the next 5-10 years.
	Rare	There is almost zero probability of the event occurring within the foreseeable future.

Consequence assessment table

	Descriptor	Impact				
		Safety	**Property**	**Financial**	**Services & Operations**	**Reputation**
Consequence	**Catastrophic**	**Multiple losses of life**	Significant financial loss/damage to Property, Plant, Equipment and resultant loss of **$10 Million** or greater	Self-generated revenue financial loss **of $1 Million** or greater	State Library **unable to continue** operations for the foreseeable future	Sustained widespread **international and national adverse media attention** and/or long term damage to reputation
	Major	**Death** to any person	Major financial loss/damage to Property, Plant, Equipment and resultant loss of between **$5 - $10 Million**	Self-generated revenue financial loss of between **$500,000 - $1 Million**	State Library operations seriously disrupted for extended periods of time i.e. maximum of **1 month**	Sustained **national and local adverse media attention** and/or medium term damage to reputation
	Moderate	**Multiple extensive injuries** / hospitalisation of personnel	High financial loss/damage to Property, Plant, Equipment and resultant loss of between **$2.5 - $5 Million**	Self-generated revenue financial loss of between **$250,000 - $500,000**	State Library operations disrupted for a moderate period of time i.e. maximum of **1 week**	Concentrated **Local adverse media attention** and/or short term damage
	Minor	**Injuries sustained** / external medical treatment required, extended trauma	Minor financial loss/damage to Property, Plant, Equipment and resultant loss of between **$100,000 - $2.5 Million**	Self-generated revenue financial loss of between **$100,000 - $250,000**	Minor disruption to State Library operations i.e. maximum of **1 day**	**Limited adverse media attention** and/or limited short term damage to reputation
	Insignificant	**First Aid treatment** required / trauma sustained to a person	Minimal financial loss/damage to Property, Plant, Equipment and resultant loss of less than **$100,000**	Self-generated revenue financial loss less than **$100,000**	**Nil disruption** to State Library's operations	**Nil adverse media attention** and nil damage to State Library's reputation

Attachment 3

Risk register template

Risks Identification, Analysis and Mitigation

Risks have been assessed by **likelihood** of occurrence and the possible **consequence** of an occurrence. Together these measures provide the **residual risk rating.**

Initial Risk Assessment				**Recommended Mitigation Procedures**				**Management Comments**	
Risk Description	Likelihood	Consequence	Initial Risk Rating	Mitigation Procedures	Likelihood	Consequence	Residual Risk Rating	Value for Money? (consider alternative options)	**Comments**