Sydney Opera House Policy

Title:	Risk Management Policy
Policy Number:	SOH151
Effective Date:	10 December 2016
Authorisation:	Chief Executive Officer
Authorisation Date:	10 December 2018
Superseded Policy:	N/A
Accountable Director:	Director, Legal, Audit & Risk
Responsible Officer:	Head of Enterprise Risk & Program Management Office

1. CORE PROPOSITION

1.1. The Sydney Opera House (SOH) is committed to managing risks as an integral part of its corporate governance and operations. Risk management practices are underpinned by SOH values – safety, excellence, creativity, collaboration and accountability.

1.2. The Risk Management Policy (the Policy) outlines the risk management framework (the Framework) used by SOH to identify and manage risks and opportunities, in order to achieve its strategic objectives.

1.3. In line with *AS/NZ ISO 31000:2018 Risk Management – Guidelines*, the Framework provides a strategic, structured and consistent approach to risk that supports and complements the expertise of SOH employees, with a view to striking an appropriate balance between realising opportunities and minimising losses.

2. SCOPE

2.1. This Policy is relevant to all SOH business areas and applies to all employees (including permanent, temporary and casual employees), contractors and persons otherwise engaged to undertake work on behalf of SOH.

2.2. All SOH risk management materials and processes must be consistent with this Policy. Specific risk management procedures are in place for certain risks, including in relation to safety, performing arts, emergency response and environmental sustainability.

2.3. This Policy does not and cannot address every possible risk to SOH and its stakeholders.

3. DEFINITIONS

3.1. **Control** – a measure that modifies (changes the potential outcome of) a risk, including any process, policy, device, practice or other actions.

3.2. **Key control** – a control whose effectiveness *materially:*

- Modifies a risk that threatens the achievement of SOH's values and objectives; and/or
- Ensures regulatory or legal compliance.

(Material: effectiveness of control without which a risk would be unacceptable.)

3.3. **Owner** – person with the accountability and authority to manage a risk, control or action, e.g. risk owner, control owner.

3.4. **Risk** – effect of uncertainty on objectives.

3.5. **Risk appetite** – the amount and type of risk that SOH is willing to take on or accept. Risk appetite is set out in a statement endorsed by the SOH Trust (the Board).

3.6. **Risk and assurance function** – business unit within SOH responsible for facilitating, and assisting responsible officers with, risk management obligations. The Risk and assurance function is independent of line management.

3.7. **Risk champions** – an informal network of employees from across the organisation who champion risk management within their portfolio or on a project, helping to embed the consistent management of risk into culture, systems and processes. Generally, a Risk champion is an informal leader on risk management issues and is someone who:

- Has the skills, knowledge and leadership qualities required to support and drive a particular aspect of risk management;

- Has sufficient authority to intervene in instances where risk management efforts are being hampered by a lack of cooperation or capability; and
- Is able to add value to the risk management processes by providing guidance and support in managing difficult risks or risks spread across functional areas.

3.8. **Risk event** – an incident or event that occurred in which the risk materialised with consequences. Note: an incident without consequences is known as a “near miss”.

4. RISK MANAGEMENT FRAMEWORK

4.1. The Framework comprises the processes and procedures, business systems, reports, data, training requirements, delegations and governance structures that identify, assess, manage, mitigate and monitor all internal and external sources of risk that could materially impact SOH’s business or the interests of SOH stakeholders.

4.2. The Framework requires risk management to be implemented through:

- Assessing and managing risk when required by a process, e.g. safety, sustainability or procurement processes, when a matter is to be considered by SOH’s Executive Team (Executive) or the Board, or in the case of any other proposed substantive change;
- Taking a proportionate response to managing identified risks; and
- Being accountable for the responses to risks.

4.3 The risk management model adopted by SOH is the Three Lines of Defence (3LOD). Business areas may perform functions that sit across these lines, as set out in *Figure 1* and further explained below.

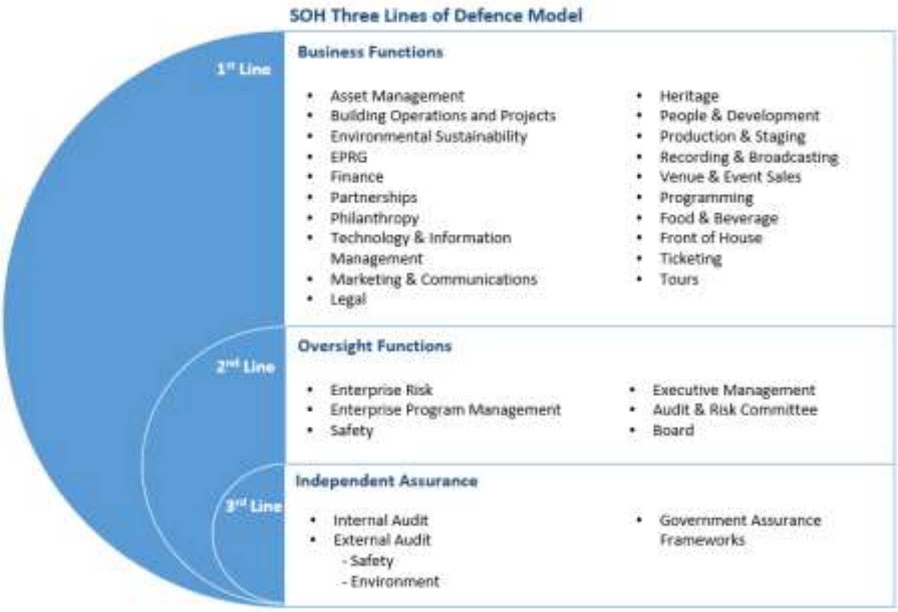


Figure 1. Three Lines of Defence model

First line: business operations

4.4 The first line of defence is made up of operational teams who identify, assess, control and report on the risks that exist in their operations. This line owns the risks and is accountable for their adequate management.

Second line: oversight functions

4.5 The second line of defence is made up of functions that oversee SOH’s risk management practice by facilitating, monitoring, and challenging the implementation of risk management by first line operational teams.

4.6 The Risk and assurance function forms part of the second line of defence, as the business unit responsible for oversight of the risk management process. This includes:

- Designing and reviewing risk management policies and procedures;

- Providing assurance through review of the risk management practices and controls implemented by the first line of defence;
- Facilitating and challenging risk assessment processes undertaken by the first line, and providing meaningful reports on material risks to the Audit and Risk Committee (ARC), Executive, clients and relevant management and employees; and
- Providing risk management training and advice across the organisation.

4.7 The Executive and the Board are each part of the second line and are responsible for management and governance respectively.

Third line: independent assurance

4.8 The third line of defence is independent, objective assurance designed to add value to and improve operational controls. This includes internal (Quality Assurance & Improvement (QAI) Program) and external audit.

4.9 The QAI Program is informed by the Enterprise Risk Profile (as set out in sections 6.5-6.6) and consultation with the first and second lines of defence, including the Executive. It is then endorsed by the ARC and approved annually by the Board.

5. RISK CULTURE

5.1 Everyone is responsible for ensuring that a suitable risk and control environment is established in their day-to-day operations. Risk is managed in accordance with SOH's values:

- **Safety** –work health and safety risks are SOH's greatest responsibility and managed in line with the *Procedure – Safety Risk Management* and SOH's risk appetite statement.
- **Creativity** – we look for creative risk management solutions;
- **Excellence** – we think about risk in accordance with this Framework whenever decisions are made;
- **Collaboration** – we involve all stakeholders to get the best outcome for SOH as a whole; and
- **Accountability** – we make sure risks are identified, managed and escalated as appropriate.

5.2 The Framework is underpinned by a proactive risk culture that includes: clear and usable risk documentation (including managing risk pages on Intouch); risk training; ongoing risk support and mentoring; and targeted risk advice through workshops, surveys and presentations, and, less formally, through the Risk champions network.

5.3 The Executive and the Risk and assurance function regularly evaluate how risk is identified and managed across SOH, ensuring SOH's proactive risk culture continues to evolve, including through providing:

- Active support for risk management practices;
- Clear roles and responsibilities within the Framework, promoting accountability for risk management within business-as-usual activities; and
- Clear communication, including ensuring that discussion and challenge are welcomed as part of risk assessment.

6. RISK GOVERNANCE

6.1 Ownership of risks and controls is determined by position within SOH. The Chief Executive Officer (CEO) is responsible and accountable for the management of risk across SOH, with the Executives holding day-to-day responsibility for key controls associated with their portfolios.

6.2 There are four essential elements to SOH's risk governance:

- **Risk appetite statement** sets out the acceptable upper limits of risk linked to activities and strategic objectives, based on a 1-5 scale (see Appendix 1 and section 6.3-6.4 below);
- **Enterprise Risk Matrix** is the methodology for assessing the likelihood and consequences of risk in order to determine the risk rating (see Appendix 2);
- **Enterprise Risk Profile** is an aggregated view of the key risks to the organisation, assessed in accordance with the Enterprise Risk Matrix (see section 6.5-6.7 below); and
- Portfolio and project **risk assessments** are required to identify the risks and controls to be implemented in the portfolio or in relation to any project, each developed in accordance with section 7.

Risk Appetite Statement

6.3 The risk appetite statement is most relevant for the Board, Executive and senior management, as it guides all strategic decision-making.

6.4 The risk appetite statement is reviewed by the Board every two years, or more often as required to reflect any material change in the SOH's strategic direction.

Enterprise Risk Profile

6.5 The Executive reviews the Enterprise Risk Profile at least three times per year. The Risk and assurance function facilitates these reviews, which are structured to identify emerging risks and reflect on the current risk profile, with a particular focus on controls, risk ratings and the status of risk modification activities. Key risks can also be escalated to the Enterprise Risk Profile from portfolio and project risk assessments.

6.6 The Risk and assurance function updates the Enterprise Risk Profile based on risk review consultation with relevant SOH stakeholders and distributes it to the Executive to update commentary on key controls, before it is reported to the ARC for discussion.

6.7 A severity-based escalation approach, as set out in **Appendix 2**, is in place to ensure appropriate management oversight of High and Very High risks. Escalations are not bound by regular risk reporting cycles and should be made as and when risk ratings are determined.

7. RISK ASSESSMENT PROCESS

7.1. The risk assessment process can be applied at strategic, enterprise, process or project levels and informs the guiding risk documents.

7.2. The components of the risk assessment process are listed below. Detailed descriptions of each key step are available at **Appendix 3**, with a step-by-step flowchart at **Appendix 4**.

- *Engaging in effective communication and consultation* – involve stakeholders and engaging in dialogue throughout the risk assessment process to inform decision-making and actions.
- *Establishing scope, context and criteria of the assessment* – before assessing particular risks, the scope and context for a risk assessment must be considered.
- *Assessing risk through a systematic process of risk identification, analysis and evaluation*:
  - *Identification* – process of finding, recognising and describing risks, including events, causes and consequences. Risk identification can be informed by historical data, informed expert opinions, stakeholder needs and theoretical analysis;
  - *Analysis* – rating consequence and likelihood against criteria and determining level of risk. SOH's risk assessment criteria is made up of the consequence, likelihood and risk rating matrices detailed in Appendix 2; and
  - *Evaluation* – whether the level of risk is acceptable and whether treatments are needed.
- *Modifying risk where necessary* – changing the possible consequences or their likelihood through the creation of new, or making changes to existing controls.
- *Monitoring and reviewing the risk and control environment* – detect changes and determine the ongoing validity of the rationale by which the risk ratings were determined.
- *Effective reporting and recording of the risk management process and its outcomes* - record outputs of the risk assessment process and report information accordingly to stakeholders.

7.3. While these steps are presented sequentially, parts of the process may need to be repeated as information changes. In particular, effective communication and consultation; monitoring and review; and effective reporting and recording are ongoing and will change over time as risks are identified and treatment plans developed.

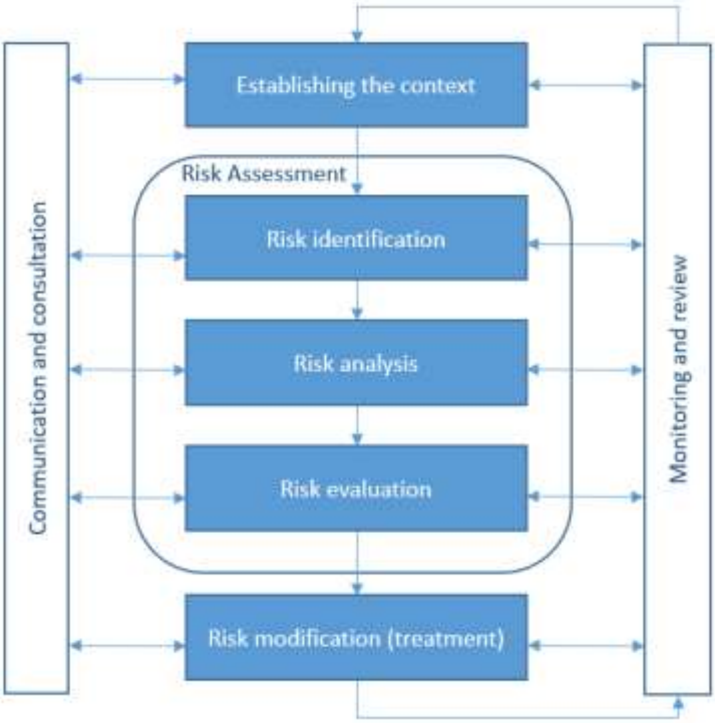


Figure 2: Risk management process.

Reproduced with permission: ISO 31000-2018 Figure 4 [partial]. © ISO and Standards Australia Limited. Copied by the Sydney Opera House with the permission of ISO and Standards Australia under Licence 1808-c080.

8. ROLES AND RESPONSIBILITIES

8.1. **Everyone** is responsible for:

- Managing risk in their day-to-day roles and seeking clarification regarding appropriate management of risk if there is confusion;
- Reporting risks to risk owners; and
- Reporting ineffective or inefficient controls.

8.2. **Employees with management and supervisory duties** are responsible for:

- Working to ensure a proactive risk culture in day-to-day operations;
- Identifying key business risks;
- Ensuring key controls are effective at the process level; and
- Proactively reviewing, updating and modifying key controls in order to capture changes.

8.3. The **head of the Risk and assurance function** is responsible for:

- Acting as SOH's champion of risk management at the strategic and operational levels, including providing frank and fearless advice about risk management to all levels of the organisation;
- Leading the development and maintenance of this Policy and the Framework;
- Designing and reviewing risk management processes and tools;
- Building the risk management culture within SOH, including appropriate employee training and development;
- Coordinating the various functional activities related to risk management across portfolios;
- Working with risk owners to achieve compliance with the Framework;
- Collating and reviewing risk registers for completeness and accuracy; and
- Preparing risk management reports for the ARC.

8.4. **Members of the Executive** are responsible for managing risk and ensuring that employees perform their duties and manage risk appropriately. This includes being responsible, within the sphere of their authority, for:

- Promoting awareness of responsibility for individual risks and controls;
- Identifying risks that will affect the achievement of SOH objectives;

- Reviewing policies, operating and performance standards, budgets, plans, systems and procedures to address identified risks and reduce them to acceptable levels;
- Monitoring the effectiveness of controls;
- Maintaining a portfolio risk assessment and risk management plan to embed risk into existing decision-making processes; and
- Nominating direct reports to take part in the Risk champions network.

8.5. The **Chief Executive Officer (CEO)** is ultimately responsible and accountable for risk management at SOH. More specifically, the CEO is responsible for:

- Ensuring an effective system of internal control over the financial and related operations of SOH;
- Approving this Policy and ensuring it is implemented and reviewed regularly;
- Ensuring appropriate resourcing and awareness of the importance of risk management; and
- Reviewing recommendations from the ARC.

8.6. The **ARC** oversees risk management at SOH as per the Audit and Risk Management Committee Charter.

8.7. The **SOH Trust (the Board)** is ultimately responsible and accountable for oversight of risk management at SOH, and approves the risk appetite.

9. RELEVANT LEGISLATION

- AS/NZ ISO 31000:2018 Risk Management – Guidelines
- Government Sector Employment Act 2013
- NSW Treasury Policy TPP 15-03 Internal Audit and Risk Management Policy
- Public Finance and Audit Act 1983
- Public Interest Disclosures Act 1994
- Work Health and Safety Act 2011

10. SOH SUPPORTING DOCUMENTS

- Audit and Risk Management Committee Charter
- Delegations of Authority Manual
- Sydney Opera House Trust Act 1961 (and Bylaws)
- Procedure – Safety Risk Management

Version History

Version	Approved by	Approval date	Effective date	Sections modified
1.0	Chief Executive Officer	10/12/2018	10/12/2018	New policy
1.1	Chief Executive Officer	08/04/2021	09/04/2021	Updates to incorporate the new Enterprise Risk Matrix.

APPROVED

Chief Executive Officer

Date: 08/04/2021

APPENDIX 1: SOH RISK APPETITE STATEMENT

PURPOSE

The Sydney Opera House (SOH) is committed to ensuring the effective identification and management of risk at every level of the organisation.

A key element of that commitment is the development of this risk appetite statement to provide organisational leaders with a common language for understanding and analysing the types and amount of risk the organisation is willing to accept.

The concept of risk appetite is most relevant at the Board, Executive and senior management levels. It is less relevant once strategic decisions have been made, and staff are in the operational execution or delivery phase.

APPLICATION

The table below sets out:

- SOH's objectives, drawn from the SOH Strategy, CEO and Director KPIs;
- Our risk appetite for each objective, ranging from 5 (ambitious) to 1 (averse). The higher our risk appetite for an objective, the more uncertainty (i.e. risk) we will accept to achieve that objective; and
- Examples of acceptable and unacceptable risks for each objective, as approved by the Board. Though not exhaustive, the unacceptable risk examples must not be entertained under any circumstances.

Objective	Risk appetite and definition	Example acceptable risk	Example of unacceptable risk
Artistic boldness Be as bold and inspiring as the building itself	5 = **Ambitious** We are eager to be innovative in achieving this objective. We will implement controls if available but will accept a **high level of uncertainty**	Bold performances such as parody and provocative content	Performances that could condone violence, encourage gambling or vilify
Attracting new visitors Renew our audience, attracting the next generation of visitors			
Visitor Experience Engage more deeply with all visitors, physically and online	4 = **Open** We will consider a range of options in achieving this objective. We will implement suitable controls and accept a **moderate level of uncertainty**	Staging circus shows with detailed and technical sets	Sharing information about patrons or staff without permission
Production Values Encourage innovation in the look and feel of the shows we stage			
Building Renewal Treasure and renew the House for future generations	3 = **Measured** We prefer measured options in achieving this objective. We will implement all practical controls to ensure a **low level of uncertainty**	Undertake detailed resource planning prior to venue closure to ensure business requirements are addressed and staff are adequately equipped for reopening	Failure to conduct due diligence resulting in negative publicity, e.g. engaging subcontractors who underpay staff or engaging a corporate sponsor who has acted unethically
Organisational capability Build and maintain a resilient and agile workforce with appropriate resources			
Our reputation Maintain a high media profile, but for the right reasons			
Financial performance On budget, consistent with forecast results	2 = **Cautious** We prefer well-controlled options in achieving this objective. We will only accept a **very low level of uncertainty**	Scope for renewal work balances disability access, planning, safety and heritage issues, including development of	Making decisions that are financially unsustainable or knowingly contravening legislation, e.g. deliberately ignoring DA requirements
Project delivery In scope, on time and on budget			
Compliance (including heritage)			

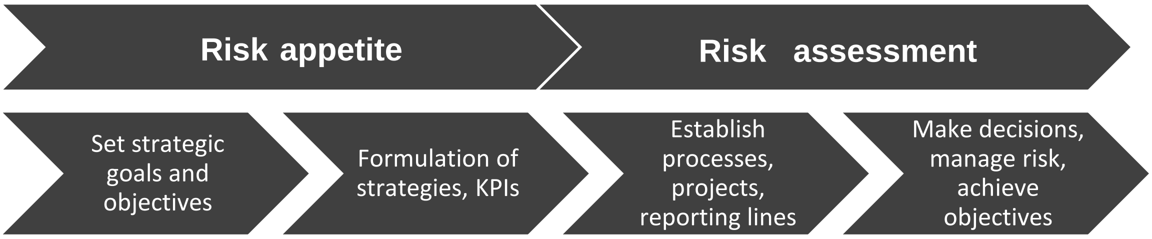
Objective	Risk appetite and definition	Example acceptable risk	Example of unacceptable risk
Comply with all of our various regulatory and policy obligations		performance solutions	
Work health and safety Safety is our greatest responsibility	1 = **Averse** All reasonably practicable controls must be in place for this objective. We will **eliminate uncertainty** as far as reasonably practicable	Vehicle-free Forecourt – we were prepared to inconvenience a small number of people to remove vehicles for safety and security reasons	Reckless actions by staff or contractors that put the safety or security of people on site at risk, e.g. allowing others to circumvent access controls
Fraud and corruption Unethical behaviour or misconduct is unacceptable			
Security Physically protect our staff, patrons and the building itself			
Data security Protect our business and customer data			

Key points

- We will consult the risk appetite statement whenever:
  - Developing a new strategy that requires Executive approval;
  - Diverging from current strategy; or
  - Developing CEO and Director key performance indicators (KPIs);
- Activities will usually involve a number of objectives and therefore different levels of risk appetite. For example, Vivid Live activations can be bold, but must also be safe. It is important to analyse all risks within the activity;
- The risk appetite is the maximum acceptable level of risk, i.e. a lower level of uncertainty/risk is also acceptable;
- Projects will proceed only if consistent with the risk appetite statement, i.e. no risk is at a greater level – once mitigated – than specified as acceptable in the statement; and
- The statement should be regularly reviewed and updated as necessary with Board approval.

From risk appetite to risk assessment

Once a strategic decision had been made consistent with the risk appetite statement, the next step is execution or delivery. In this phase, risk assessments are essential to ensure all risks have been identified and appropriate controls implemented to ensure successful delivery. The diagram and table below shows how this applies to several examples in practice.



Risk appetite

Risk assessment

Set strategic goals and objectives

Formulation of strategies, KPIs

Establish processes, projects, reporting lines

Make decisions, manage risk, achieve objectives

Example	Risk appetite	Risk assessment
New Enterprise Strategy	✓	✓
New CEO or Director KPIs	✓	✓
New business development opportunity	✓	✓
Whole of House food and beverage tender	✗	✓
Contemporary music act in the Concert Hall	✗	✓
New plant in the loading dock	✗	✓
New sponsor	✓	✓
Renewal of existing sponsor	✗	✓

APPENDIX 2: ENTERPRISE RISK MATRIX

1. Assess the consequence of the risk:

	Insignificant	Minor	Moderate	Major	Extreme
People	Loss of personnel/ corporate knowledge, does not impede processes or services. Individual complaint received or grievance lodged. Routine HR issues management.	Loss of key personnel and corporate knowledge, temporarily impeding non-critical processes or services. Several staff complaints received or grievances lodged, limited negative impact on culture and/or productivity. Isolated staff conduct incidents requiring investigation.	Loss of key personnel and corporate knowledge, resulting in short-term disruption to some critical processes or services. Formal proceedings brought by individual staff member. Threat of industrial action, and/or some negative impact on culture and/or productivity. Individual or isolated staff conduct incidents requiring investigation and formal disciplinary action (incl. termination).	Significant loss of key personnel and corporate knowledge, resulting in medium-term disruption to critical processes or services. Short-term industrial action, widespread negative impacts on culture and/or productivity. Several staff or multiple conduct incidents requiring disciplinary action (including termination).	Substantial loss of key personnel and corporate knowledge, resulting in cessation or long-term disruption of critical processes or services. Sustained or prolonged industrial action across multiple areas of SOH. Systemic and/or prolonged conduct incidents or issues.
Environment	Negligible reversible negative impact, limited to a small area, can be rectified without delay.	Reversible, localised short-term negative impact. Can be rectified within days within existing budget.	Reversible, medium-term (<1 year) negative impact. May require minor allocation of additional resources. Can be rectified within weeks. Stakeholders protest, requiring management attention.	Extensive, medium-term (1-5 year) negative impact, rectification may require significant allocation of additional resources. EPA notification required. Improvement notice issued by regulator.	Extensive, medium-, long-term or irreparable negative impact (5 years or longer) Requires significant allocation of additional resources. Penalties or fines issued by regulator.
Safety & Wellbeing	Physical injury/illness not requiring first aid assistance. Negligible adverse impact to psychological health, no intervention or time off work.	Minor physical injury involving first-aid treatment. Adverse impact to psychological health requiring intervention. No time off work.	Physical injury requiring medical treatment incl. hospital visit. Psychological injury resulting in temporary time away from work (days or weeks) or changes to work arrangements.	Serious physical injury requiring hospital admission. Long-term or permanent disablement with some functional restriction. Psychological injury resulting in extended time off work (months). *(WHS Critical Incident Level 3)*	One or more fatalities. Significant permanent disablement. Psychological injury resulting in inability to return to work. *(WHS Critical Incident Level 1-2)*

	Insignificant	Minor	Moderate	Major	Extreme
Financial	Below $50,000 effect on annual operating budget or reserves.	Between $50,000 and $250,000 effect on annual operating budget or reserves.	Between $250,000 and $1m effect on annual operating budget or reserves.	Between $1m and $5m effect on annual operating budget or reserves.	Greater than $5m effect on annual operating budget or reserves.
Image & Reputation	Negligible media attention, social media discussion or stakeholder concerns.	Isolated adverse media coverage. Minimal social media discussion. Stakeholder concerns resolved easily.	Moderate levels of media coverage, limited to local and metro outlets, minimal adverse impact on brand perception. Low level of social media discussion. Temporary adverse impact on key stakeholder relationships.	Sustained local and national adverse coverage across multiple media channels and/or widespread negative discussion on social media. Campaign put on hold for relevant activity. Medium-term adverse impact on brand perceptions (months). Medium-term adverse impact on key stakeholder relationships.	Sustained, local, national and international adverse coverage across multiple media channels and significant negative feedback on social media. Multiple campaigns put on hold beyond relevant activity. Ongoing adverse impact on brand perception (>12 months). Loss of or long-term adverse impact on key stakeholder relationships.
Artistic & Visitor Experience	No change in visitor and audience sentiment.	Up to 5% reduction in visitor and audience satisfaction rating. Visitors/audience acknowledge minor or isolated adverse changes in their SOH experience.	5-10% reduction in visitor and audience satisfaction rating. Visitors/audience feel there has been some adverse change in their SOH experience.	10-20% reduction in visitor and audience satisfaction rating. Visitors/audience perceive there has been a marked adverse change in their experience and this has flow-on effects.	20% or greater reduction in visitor and audience satisfaction rating. Visitors/audience perception of SOH is negatively transformed and this leads to operational changes.
Business Disruption	Negligible interruption to critical systems, access on site, or service from third party. Can be rectified without delay.	Brief or partial interruption to critical systems or access on site. Brief interruption, delay, or limit to service from third parties. Feasible workarounds. Interruption lasts less than 4 hours. Experiences, including performances, can continue across all venues with workaround.	Interruption lasting between 5-24 hours to critical systems, on-site access, or service from third parties causing operational delays. Single experience/ performance venue cannot operate for one day or less.	Disruption to critical systems, on-site access, third party service, or one or more experience/performance venues* with rectification taking up to 10 days. *(*up to 5 days if JST and/or CH)*	Critical system failure requiring bare-metal restore. Permanent loss of valuable data. Denial of access to precinct or structures. Prolonged severe interruption to operations and experiences across multiple venues* for 10 or more days. *(*5 days or more if JST and/or CH)*

	Insignificant	Minor	Moderate	Major	Extreme
Building	No irreversible or permanent damage to the building, its fabric or equipment. Repairs, if required, can be done without delay.	Manageable damage to the building, its fabric or equipment. Repairs can take a few days.	Damage to the building, its fabric or equipment. Repairs can take up to months/years.	Extensive damage to the building, its fabric or equipment causing some permanent damage. Repairs will take up to months/years.	Permanent or irreversible damage to the building or its fabric.
Heritage	No temporary or permanent negative impacts to tangible and intangible heritage values of the Opera House	Minimal temporary or permanent negative impacts to tangible or intangible heritage values of the Opera House	Some temporary or permanent negative impacts to tangible or intangible heritage values of the Opera House	Extensive temporary or permanent negative impacts to tangible or intangible heritage values of the Opera House	Long-term or permanent negative impacts to tangible and intangible heritage values of the Sydney Opera House
Legal / Compliance	Regulatory breach with minimal or no consequences – readily rectified.	Regulatory breach with minimal or no consequences – but cannot be readily rectified.	Regulatory breach requiring notification to relevant authority. Potential for moderate penalties, improvement notices and/or corrective action – which can be rectified.	Regulatory breach with significant penalties. Adverse finding by a regulatory or audit body – which cannot be readily rectified. Repeated compliance breaches indicate a systemic or cultural failure. Major litigation.	Significant breach with prosecution and/or significant fines. Potential for criminal convictions resulting in imprisonment. Repeated compliance breaches result in cessation of some core operations. Serious litigation including large scale class action.

2. Assess the likelihood of the *particular consequence*:

LIKELIHOOD	Probability of consequence occurring (in a 12 month period)	Description
Almost Certain	91-100%	Expected to occur within the next 12 months or life of project. Expected to occur more than once a year. Has occurred more than once at SOH in similar control environment. Absence of effective key controls.
Likely	61– 90%	Expected to occur within the next 2 years or within life of project. High chance of occurring at least once a year. Has occurred at SOH in similar control environment. The majority of key controls are not effective or only partially effective.
Possible	41 – 60%	Could occur under usual operational or project circumstances. Could occur once every 2 to 3 years. Has occurred at SOH and in similar organisations, but not at SOH in the current control environment. Some key controls are effective but a significant portion is not effective or only partially effective.
Unlikely	11 – 40%	Slight chance of occurring under usual operational or project circumstances. Once in every 3 to 10 year event. Has occurred in other organisations, but not at SOH in the current control environment. Key controls are mostly effective, with a few partially effective.
Not expected	0 – 10%	Conceivable but rare, would only occur under exceptional operational or project circumstances. Not expected to occur more than once in 10+ year period. Has not occurred in the known history of SOH. Key controls are effective.

3. Rate the Residual Risk:

LIKELIHOOD	CONSEQUENCE				
	Insignificant	Minor	Moderate	Major	Extreme (Note 1)
Almost Certain	Low	Medium	High	Very High	Very High
Likely	Low	Medium	Medium	High	Very High
Possible	Low	Medium	Medium	High	Very High
Unlikely	Low	Low	Medium	High	Very High
Not expected	Low	Low	Low	Medium	High

Note 1: In relation to Safety risks all reasonably practicable steps must have been taken to avoid the risk.

4. Escalate and manage by residual risk rating:

🟩 **LOW –** Monitor and manage as usual

🟨 **MEDIUM –** Requires Manager attention and Senior Leadership Team awareness

🟧 **HIGH –** Requires Executive attention and mitigation action

🟥 **VERY HIGH –** Requires immediate CEO attention, mitigation action plan and escalation to Audit and Risk Committee

Additionally, any Safety risk with a *Major or Extreme* consequence, where the only available controls are Administrative (including but not limited to SWPs, SWMSs, signage) or wearing of PPE, need to be escalated to a Director, irrespective of residual risk rating (i.e. after application of controls).

APPENDIX 3: RISK ASSESSMENT PROCESS

1. Communication and consultation

1.1. Communication and consultation are imperative throughout the risk assessment process. It is vital to involve internal and external stakeholders, as appropriate, at each stage of the risk management process and concerning the process as a whole, because:

- People will need to take (or not take) particular actions to effectively manage uncertainty;
- People will have most of the knowledge upon which the process will rely; and
- Some people will have a right to be informed or consulted.

1.2. This part of the process should involve a dialogue with stakeholders rather than a one-way flow of information from the decision-maker to the stakeholders and ensure that those with vested interests understand the basis on which decisions are made and why particular responses are required.

2. Scope, context and criteria

2.1. Before assessing particular risks the scope, context and risk criteria for a risk assessment must be considered as follows.

Scope

2.2. The scope of the activity, decision, project or change should be carefully defined alongside its objectives. Generally it is to provide support for a decision or to enable a change to take place. Assessments may also take place when a material external change is detected or anticipated.

2.3. The objectives must be subordinate to the relevant high-level objectives and values of the Opera House as a whole, which should also be defined in the scope.

Context

2.4. Both internal and external contexts must be taken into account when defining scope and objectives for a risk assessment.

2.5. Internal context includes the Opera House's:

- Culture, including our vision, mission and values;
- Strategy, objectives and policies;
- Structure and accountabilities;
- Data, information systems and reporting;
- Contractual matters; and
- Capability, knowledge and resources (including budgets).

2.6. External context includes:

- Environmental factors such as social, political, legal, regulatory, financial and technological factors;
- Relationships with external stakeholders, including their perceptions, values, needs and expectations;
- Key drivers and trends affecting the organisation; and
- Complex networks and interdependencies, bearing in mind the possibility of unintended consequences.

Criteria

2.7. To set risk criteria for a decision, the following must be considered:

- The nature and types of uncertainty that can affect outcomes and objectives;
- The nature and magnitude of the different possible scenarios;
- Consistency in the use of measurements;
- How consequences and likelihood will be measured; and
- The Opera House's risk appetite statement, which sets the upper limits of acceptable risk for anyone completing a risk assessment

2.8. The Enterprise Risk Matrix provides guidance for impacts ranging from insignificant to extreme across a number of business areas, and defines likelihood scales from unexpected to almost certain. It is acceptable to divert from this in certain circumstances where the Enterprise Risk Matrix does not work – there will be limited examples where this may be the case, e.g. security threat assessment, climate change risk assessment.

3. Risk assessment

3.1. The assessment itself comprises three steps: risk identification, risk analysis and risk evaluation. There are various tools available at the Opera House for this step, including Bow Tie analysis, Structured What-If Technique (SWIFT) and the Step-by-Step Guide.

Risk identification

3.2. This involves looking for risks and opportunities at the highest level in order to reveal what, where, when, why and how something could occur and the range of possible effects on objectives it could have. Forming a comprehensive view is critical, because any sources of uncertainty not identified at this stage will not be considered further. Therefore it is important to consider all sources of uncertainty, including those outside the direct control of the Opera House.

3.3. This step should involve a structured conversation with stakeholders, with outcomes and conclusions recorded.

Risk analysis

3.4. Analysis underpins risk evaluation and is about understanding the risks by drawing upon and investigating the:

- Information gathered during risk identification;
- Effectiveness and reliability of controls that enable the organisation to achieve its objectives;
- Available supporting historical data and experience, results of predictive modelling, expert judgment; and
- The Opera House’s risk criteria and risk appetite.

3.5. Once this step has been completed, it should be clear whether new controls must be created or existing controls modified.

Risk evaluation

3.6. Risk evaluation involves using the information generated in the identification and analysis stages to make decisions about whether the level of risk is acceptable or whether further modification is required. The Enterprise Risk Matrix is the tool used to combine possible consequences and the likelihood of these occurring to provide a risk rating.

3.7. Risk ratings are calculated taking into account the controls in place at the time.

3.8. The level of risk determined using the Enterprise Risk Matrix determines the escalation and approvals required.

4. Risk modification

4.1. Risk modification involves changing the possible consequences or their likelihood through creation of new, or making changes to existing controls. This process involves creative consideration of options and detailed design to find the best possible solutions.

4.2. Decisions on the need for risk modification will be based on cost-benefit analysis unless specific criteria are required by legislation or an Opera House policy.

4.3. When creating or amending controls, the means of testing these so that any unintended consequences can be identified should be considered. Good controls are those that can be easily verified, including through self-assessments where people applying the controls are asked to certify the efficacy of the control.

4.4. Risk modification takes place in two distinctive contexts:

- Proactively, where the Opera House has successfully integrated the risk assessment process into a management system, and risk modification is integral to and effectively indistinguishable from decision-making; and
- Reactively, when the Opera House is looking retrospectively at the level of risk created by decisions taken previously and implemented so that any modification are remedial in nature.

4.5. In either case, where the level of risk is unacceptable then action should be taken.

4.6. Timeframes for taking action relate to the risk rating. The higher the rating, the more important it is to modify the risk as soon as appropriate. Factors such as cost and time must be taken into account alongside potential consequences.

5. Monitoring and review

5.1. These are two distinct processes to detect changes and determine the ongoing validity of assumptions. Both monitoring and review are necessary to ensure that the Opera House maintains a current understanding of the effect of uncertainty on its objectives and that levels of risk remain acceptable. Both require a systematic approach, integrated into the Opera House's management systems to reflect the speed at which change occurs.

5.2. Management must monitor risk ratings and the ongoing effectiveness of controls and modifications. Monitoring should be considered as an integral and ongoing part of control design.

5.3. Management must also formally review the risk assessment itself at regular intervals and take into account any changes in the environment. The period for formal review must be based on the level of risk.

6. Recording and reporting

6.1. Outputs of the risk management process must be recorded to:

- Preserve the results of discussions, agreements, analyses and conclusions;
- Provide the basis for the allocation and tracking of modification actions;
- Provide the basis for control assurance; and
- Satisfy governance requirements.

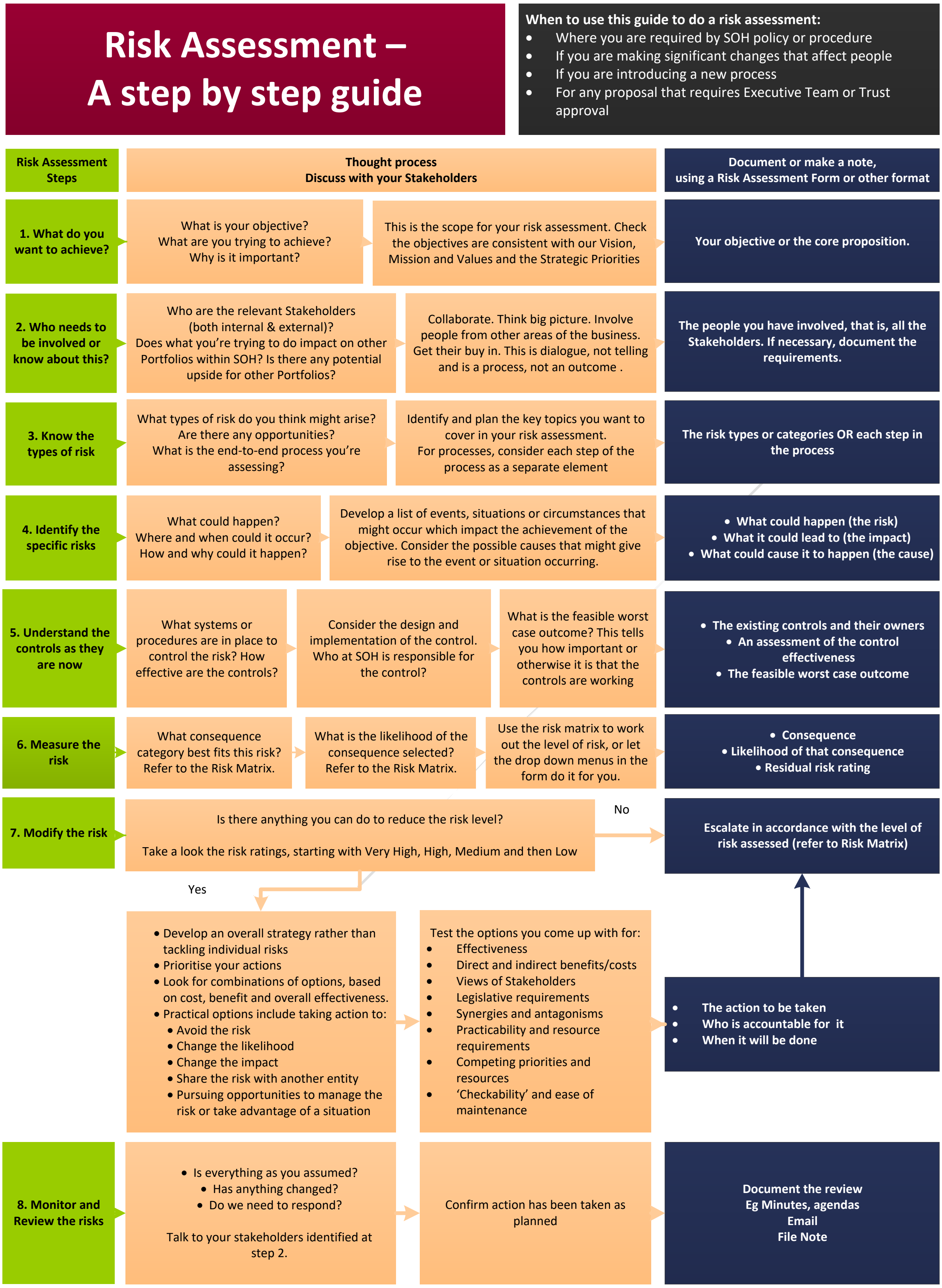
6.2. The information to be preserved for each risk includes:

- A description of what could happen;
- Who is the risk owner;
- The causes;
- What this could lead to in terms of the objectives affected;
- Any existing controls;
- Who the control owner is;
- Control effectiveness;
- Ratings for the consequences' likelihood based on current controls; and
- The level of risk

6.3. Modification plans must also be kept and should contain:

- Actions required;
- Name/s of the persons accountable for the completion of those actions;
- Completion dates.

APPENDIX 4: RISK ASSESSMENT – A STEP BY STEP GUIDE



Risk Assessment – A step by step guide

When to use this guide to do a risk assessment:

- Where you are required by SOH policy or procedure
- If you are making significant changes that affect people
- If you are introducing a new process
- For any proposal that requires Executive Team or Trust approval

Risk Assessment Steps

Thought process
Discuss with your Stakeholders

Document or make a note, using a Risk Assessment Form or other format

1. What do you want to achieve?

What is your objective?
What are you trying to achieve?
Why is it important?

This is the scope for your risk assessment. Check the objectives are consistent with our Vision, Mission and Values and the Strategic Priorities

Your objective or the core proposition.

2. Who needs to be involved or know about this?

Who are the relevant Stakeholders (both internal & external)?
Does what you're trying to do impact on other Portfolios within SOH? Is there any potential upside for other Portfolios?

Collaborate. Think big picture. Involve people from other areas of the business. Get their buy in. This is dialogue, not telling and is a process, not an outcome .

The people you have involved, that is, all the Stakeholders. If necessary, document the requirements.

3. Know the types of risk

What types of risk do you think might arise?
Are there any opportunities?
What is the end-to-end process you're assessing?

Identify and plan the key topics you want to cover in your risk assessment.
For processes, consider each step of the process as a separate element

The risk types or categories OR each step in the process

4. Identify the specific risks

What could happen?
Where and when could it occur?
How and why could it happen?

Develop a list of events, situations or circumstances that might occur which impact the achievement of the objective. Consider the possible causes that might give rise to the event or situation occurring.

- **What could happen (the risk)**
- **What it could lead to (the impact)**
- **What could cause it to happen (the cause)**

5. Understand the controls as they are now

What systems or procedures are in place to control the risk? How effective are the controls?

Consider the design and implementation of the control. Who at SOH is responsible for the control?

What is the feasible worst case outcome? This tells you how important or otherwise it is that the controls are working

- **The existing controls and their owners**
- **An assessment of the control effectiveness**
- **The feasible worst case outcome**

6. Measure the risk

What consequence category best fits this risk? Refer to the Risk Matrix.

What is the likelihood of the consequence selected? Refer to the Risk Matrix.

Use the risk matrix to work out the level of risk, or let the drop down menus in the form do it for you.

- **Consequence**
- **Likelihood of that consequence**
- **Residual risk rating**

7. Modify the risk

Is there anything you can do to reduce the risk level?

Take a look the risk ratings, starting with Very High, High, Medium and then Low

No

Escalate in accordance with the level of risk assessed (refer to Risk Matrix)

Yes

- Develop an overall strategy rather than tackling individual risks
- Prioritise your actions
- Look for combinations of options, based on cost, benefit and overall effectiveness.
- Practical options include taking action to:
  - Avoid the risk
  - Change the likelihood
  - Change the impact
  - Share the risk with another entity
  - Pursuing opportunities to manage the risk or take advantage of a situation

Test the options you come up with for:

- Effectiveness
- Direct and indirect benefits/costs
- Views of Stakeholders
- Legislative requirements
- Synergies and antagonisms
- Practicability and resource requirements
- Competing priorities and resources
- 'Checkability' and ease of maintenance

- **The action to be taken**
- **Who is accountable for it**
- **When it will be done**

8. Monitor and Review the risks

- Is everything as you assumed?
- Has anything changed?
- Do we need to respond?

Talk to your stakeholders identified at step 2.

Confirm action has been taken as planned

Document the review
Eg Minutes, agendas
Email
File Note