Risk Management Policy

Commencement Date
1 July 2014

1.0 Purpose
This policy describes the Guild’s risk management objectives and processes to assist with achieving strategic and operational goals and to guide decision-making and performance.

2.0 Scope
This policy applies to all employees of the Guild and to other parties conducting business on behalf of or acting as a representative of the Guild. It applies to all strategic, academic and operational activities.

Employees in all areas and activities of the Guild are responsible for applying risk management principles and practices in their work areas;

Employees in supervisory and managerial positions are responsible for ensuring that risk management principles and practices are applied by those under their supervision.

3.0 Objectives
To provide a risk management approach to every day business that will enable opportunities and benefits to be realised. This policy provides the basis for:

- staff to undertake risk management practices;
- inherent risks to be identified, analysed, treated, monitored and reported;
- rigorous decision-making and planning;
- better identification of opportunities and threats;
- improved compliance with relevant legislation.

4.0 Implementation
The Guild will ensure that risk management will be incorporated into the business, strategic and operational planning processes at all levels within the Guild. The Guild will ensure that:

- current and future Guild activities are to be risk assessed prior to commencement and risk managed throughout the activity’s duration
- risk identification, analysis, evaluation and treatment are to be reported and updated within the Guild’s risk register
- business plans and data are informed via appropriate risk management
- risks will be assigned an owner who is responsible for monitoring and ensuring that adequate controls and treatments are being applied so that risks are brought within tolerable levels
- Higher level risks receive appropriate attention and focus
- Appropriate mitigation strategies and controls are implemented and maintained

Incident Management and Reporting
The Guild commits to reporting of all incidents as a key component of the risk management system. This will support:

- Immediate response, containment, stabilisation and mitigation of risk events;
- Investigation and analysis of events to an appropriate level;
- Rectification from a risk event;
- Improvements in the prevention and management of risks;
- Monitoring, review of existing risk management strategies.

5.0 Definitions

Consequence - The outcome of an event expressed qualitatively or quantitatively, being a loss, injury, disadvantage or gain. There may be a range of possible outcomes associated with an event.

Control - Any action taken by management, the board, and other parties to manage risk and increase the likelihood that established objectives and goals will be achieved.

Cost - Of activities, both direct and indirect, involving any negative impact, including money, time, labour, disruption, and goodwill, political and intangible losses.

Contingency - Budget (cost benefit) or time (duration) that may be used in the event of a risk occurrence.

Event - An incident or situation, which occurs in a particular place during a particular interval of time.

Frequency - A measure of the rate of occurrence of an event expressed as the number of occurrences of their event in a given time. See also Likelihood and Probability.

Inherent risk - High inherent risks that are well controlled may fall out of our field of view if only the residual risk is assessed. The purpose of assessing inherent risk is to ensure that we maintain focus on compliance with controls.

Likelihood – A qualitative description or synonym for probability or frequency.

Probability - The likelihood of a specific event or outcome, measured by the ratio of specific events or outcomes to the total number of possible events or outcomes.

Risk – the chance of something happening which will have an impact upon objectives. It is measured in terms of consequence and likelihood.

Risk acceptance - An informed decision to accept the consequences and the likelihood of a particular risk.

Risk analysis - A systematic use of available information to determine how often specified events may occur and the magnitude of their consequences.

Risk appetite - The level of risk that is acceptable to the board or management. This may be set for the organisation as a whole, for different groups of risks or at an individual risk level.

Risk assessment - The overall process of risk analysis and risk evaluation.

Risk avoidance - An informed decision not to become involved in a risk situation.
Residual risk - The remaining risk after management has taken action to alter the risk’s likelihood or impact.
Risk identification - The process of determining what can happen, why and how.
Risk Treatment – Selection and implementation of appropriate options for dealing with risk.
Risk Management Process – The systematic application of management policies, procedures and practices to the tasks of establishing the context, identifying, analysing, evaluating, treating, monitoring and communicating risk.
Risk Register / Risk Management Plan - The summary report of all individual risks within each assessment, which include: risk ratings (inherent and residual), level of control, risk decision, risk owner and summary of key controls and/or mitigating actions.
Stakeholders - Those people and organisations who may affect, be affected by, or perceive themselves to be affected by, a decision or activity.

Note: Definitions are based on the Australian & New Zealand Risk Management Standard AS/NZS 4360:2004.

6.0 Related policies and procedures
- Risk Management Framework
- Risk Management Register
- Business Plan and Strategic Plan

7.0 Review

Three years from commencement.

8.0 Accountabilities

The Committee of Management is responsible for review and approval of this policy.

The Risk Management Policy places responsibility upon employees at all levels within the Guild.

Committee of Management
The Committee of Management oversees the risk management and business continuity framework, management and implementation, on behalf of the Guild. The Committee:
(a) are responsible for ensuring that the Guild executives comply with appropriate risk management and business continuity policies and practices;
(b) ensure that risk management and business continuity policies, procedures and framework are established, implemented and maintained;
(c) identify and monitor strategic and significant operational risks that impact upon the Guild’s strategic objectives;
(d) delegates oversight of academic compliance with regulatory requirements to the Academic Board;
(f) reviews risk management and business continuity management incidents as they occur.
(g) establishes and administers a Guild-wide risk register.
Employees
Employees are responsible for applying risk management principles and practices in their work areas. Employees in supervisory and managerial positions are responsible for ensuring that risk management principles and practices are applied by those under their supervision.

(a) to report risks with the potential to impact upon their work area or the wider Guild to the relevant area of the Guild’s management;
(b) to participate in Guild risk management and business continuity education and training activities relevant to their level of responsibility.

All Employees
All employees are responsible for:
• to act responsible of one’s own actions and not place others in harm’s way;
• guide staff or students as to health and safety requirements in the Guild campus and/or off campus locations (e.g. live performances at an external venue);
• report concerns of risks and apply risk management practices accordingly;
• participating in risk management to decrease AGME accountability;

Education and Training
A strategy towards planning clear and decisive risk management processes. To include training of staff in implementation of risk management.

9.0 Revision History

Date Created: 14 May 2014

<table>
<thead>
<tr>
<th>Approval Authority</th>
<th>Contact Person</th>
<th>Revision Due Date</th>
<th>Revision Date</th>
<th>Approved Date</th>
<th>Version No.</th>
<th>Revision Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Committee of Management</td>
<td>President</td>
<td>30/6/2017</td>
<td>20/5/14</td>
<td>1</td>
<td>Development of new policy.</td>
<td></td>
</tr>
</tbody>
</table>