

Risk Management Plan

Version 1.0

March 2016

Table of Contents

[Table of Contents i](#_Toc448647780)

[List of Figures i](#_Toc448647781)

[List of Tables i](#_Toc448647782)

[General 1](#_Toc448647783)

[Purpose 1](#_Toc448647784)

[Scope 1](#_Toc448647785)

[Definitions 1](#_Toc448647786)

[Ownership 1](#_Toc448647787)

[Review 1](#_Toc448647788)

[Why Risk Management is Important to AAA 2](#_Toc448647789)

[General 2](#_Toc448647790)

[Roles and Responsibilities for Risk Management within AAA 2](#_Toc448647791)

[General 2](#_Toc448647792)

[Board 3](#_Toc448647793)

[CEO 3](#_Toc448647794)

[Risk Manager 3](#_Toc448647795)

[Managers 3](#_Toc448647796)

[Risk Management Process 4](#_Toc448647797)

[General 4](#_Toc448647798)

[Communication and Consultation 4](#_Toc448647799)

[Establish the Plan 5](#_Toc448647800)

[Risk Identification 6](#_Toc448647801)

[Risk Analysis 7](#_Toc448647802)

[Risk Evaluation 8](#_Toc448647803)

[Risk Treatment 9](#_Toc448647804)

[Monitoring and Review 10](#_Toc448647805)

[Document 10](#_Toc448647806)

[Risk Reporting within AAA 10](#_Toc448647807)

[Conclusion 11](#_Toc448647808)

[List of Attachments 11](#_Toc448647809)

List of Figures

[Figure 1 - Risk Management Process 4](#_Toc448647810)

List of Tables

[Table 1 – AAA Likelihood Rating Matrix 5](#_Toc448647903)

[Table 2 - AAA Risk Targets 6](#_Toc448647904)

[Table 3 – Authority for Acceptance above Risk Targets 6](#_Toc448647905)

[Table 4 – Risk Description Structure 7](#_Toc448647906)

[Table 5 – Risk Scoring Matrix 7](#_Toc448647907)

[Table 6 –Effectiveness of Control Measures 8](#_Toc448647908)

Finance Brokers Association of Australia - Risk Management Plan

General

1. The Australian Association of Associations’ (AAA) mission is: ***to facilitate engagement between associations impacted by a particular public policy in order to generate a strong coordinated response***.
2. As a member based entity, AAA is an organisation where its very survival is contingent on the quality of its outcomes, where any impact on reputation could have devastating consequences. The management of risk within AAA is an important enabling function that will help the organisation meets the expectations of our many stakeholders and provide quality services to our client base.
3. Our understanding and management of risk will provide greater certainty and security for stakeholders, our employees and our customers. We will be better informed, more decisive and move with increased confidence to the achievement of our specified outcomes and objectives.

Purpose

1. The purpose of this Plan is to define the procedures, roles and responsibilities, monitoring and reporting requirements for the management of risks within AAA.

Scope

1. This Strategic Risk Management Plan is to be applied across not only head office but to all AAA chapters.

Definitions

1. Definitions applicable to this plan are detailed in the Glossary at **Attachment 1**.

Ownership

1. The Risk Management Plan is owned by the AAA CEO.

Review

1. The document is to be reviewed annually by the CEO. The purpose of the review is to determine:
	* + - 1. If there have been any changes to the AAA environment during the preceding period; and/or
				2. Whether the current risk criteria (Likelihood and Consequence) are still appropriate;
2. Such reviews are critical in ensuring the ongoing integrity of the Risk Management Program within AAA.

Why Risk Management is Important to AAA

General

1. It is not possible to eliminate all risk, however organisations that actively identify and manage risks are more likely to be better prepared to respond quickly to take advantage of an opportunity or to re-focus effort when things go wrong.
2. Accordingly, risk management within AAA is about managing uncertainty and creating an environment where surprises are minimised. When our management of risk goes well it often remains unnoticed. When it fails, the consequences can be significant and high profile.
3. From a AAA perspective, effective risk management can:
	* + - 1. Prevent loss of life/injury;
				2. Prevent loss or damage to reputation;
				3. Protect assets/resources;
				4. Prevent disruption to AAA operations;
				5. Prevent financial loss, including theft and fraud; and
				6. Raise AAA’s credibility amongst our membership base.
4. Risk management will improve AAA’s performance by identifying and then mitigating events and issues that would hinder the achievement of its objectives. The management and communication of risks needs to be an integral part of existing processes and procedures to realise maximum benefit.

Roles and Responsibilities for Risk Management within AAA

General

1. Responsibility for risk management within AAA is held by:
	* + - 1. AAA Board;
				2. CEO;
				3. Risk Manager; and
				4. Other Managers.
2. These roles and responsibilities are detailed more specifically below.

Board

1. The Risk Management Program is one of the primary governance programs within AAA. Its primary purpose is to provide assurance to the Board that all risks are being managed effectively. The Board is responsible for:
	* + - 1. Oversight of risk management practices within the AAA;
				2. Reviewing quarterly all key risk management information including the AAA risk management corporate risk profile and, as they arise, any major decisions affecting AAA’ risk exposure;
				3. Management of AAA strategic risks; and
				4. Review of all strategic risk and significant operational risks on an annual basis.

CEO

1. The CEO has a significant interest in the outputs of the AAA Risk Management Program and is responsible for the following:
	* + - 1. Leadership of the AAA Risk Management Program;
				2. Ensuring that the Risk Management Program is resourced appropriately;
				3. Maintaining visibility of operational risks within AAA; and
				4. Providing reports to the Board on the status of strategic and operational risks.
2. The CEO is assisted in this role by the AAA Risk Manager.

Risk Manager

1. The role of the Risk Manager within the AAA risk management framework is to provide advice on risk management and guidance to Directors and Managers.
2. The Risk Manager acts as the liaison between the CEO and Managers on risk matters and is the custodian of the AAA Risk Register.

Managers

1. Managers have a significant role to play in ensuring that all of the requirements of the AAA Risk Management Program are implemented effectively across their areas of responsibility. Specifically, Managers are responsible for ownership/accountability for risks within their areas of responsibility.
2. The AAA Risk Management Program will only be effective if Managers take a strong leadership role in not only its implementation, but also its ongoing management.

Risk Management Process

General

1. The Risk Management process to be followed within AAA is shown in Figure 1 below and is in accordance with the AS/NZS ISO 31000 *Risk Management – Principles and Guidelines* 2009.

**Communicate and Consult**

**Monitor and Review**

**Establish the Plan (defined in Risk Management Manual/Plan)**

* Objectives
* CSFs
* Risk Criteria
* Evaluation Criteria
* Risk Matrix

**Identify Risk**

* Review organisation’s Plan.
* What event(s) can happen that will have an adverse impact on objectives?
* How can it happen?
* What are the effects if it does happen?

**Analyse and Evaluate the Risks**

* Review controls
* Assign likelihood rating
* Assign consequence rating
* Determine level of risk
* Rank risks and compare against evaluation criteria

**Treat the Risks**

* Identify options
* Conduct cost/benefit analysis
* Select best option/s
* Develop implementation plans
* Implement

**Risk Assessment**

Figure 1 - Risk Management Process

1. This section of the Plan provides a detailed overview of the application of the above process to AAA.

Communication and Consultation

General

1. Communication of risk and consultation with the stakeholder community is essential to supporting sound risk management decisions.
2. To that end, all stakeholders are to be identified for each AAA risk and, where appropriate they are to be consulted in relation to the management of the risk.

Establish the Plan

General

1. Establishing the Plan defines the basic parameters within which risks will be managed within AAA and sets the scope for the rest of the Risk Management process. This step is needed to identify the criteria against which the risks will be assessed and evaluated within AAA.

Risk Criteria

1. Risk criteria are the likelihood and consequence ratings that are used in order to assess the level of the risk to determine whether treatment is required.

#### Likelihood

1. AAA will utilise the likelihood rating system shown in Table 1 when analysing risks:

|  |  |
| --- | --- |
| **Rating** | **Descriptors** |
| **Almost Certain** | Expected to occur in most circumstances***Guide:*** *Is expected to occur multiple times within a year* ***or*** *incident is clearly imminent* |
| **Likely** | Probably occur in most circumstances***Guide:*** *Is expected to occur approximately once per year* |
| **Possible** | Could occur at sometime***Guide:*** *Likely to occur approximately once every 5 years* |
| **Unlikely** | Not expected to occur***Guide:*** *Likely to occur approximately once every 5-10 years* |
| **Rare** | Exceptional circumstances only***Guide:*** *Likely to occur with less frequency than once every 10 years* |

Table 1 – AAA Likelihood Rating Matrix

#### Consequence

1. For risk assessments to be effective there needs to be a structured approach across the organisation to assessing consequence. To do this, the Consequence Criteria for AAA are provided at **Attachment 2**.
2. The level of consequence for each risk is to be determined for all of the categories in the consequence matrix.

#### Evaluation Criteria (Determining if a Risk Requires Treatment)

1. Once a risk has been analysed, it needs to be compared with Table 2 below. If the assessed risk level is above the acceptable/tolerable level for that category of risk then treatment may be required. If it is equal to or below the acceptable/tolerable level for that category of risk then the risk can be accepted.

|  |  |
| --- | --- |
|  | **What level of residual risk (after treatment) are we willing to retain in the pursuit of our objectives** |
| **Critical Success Factor** | **Low** | **Medium** | **High** | **Very High** |
| **Reputation** | ♦ |  |  |  |
| **Safety** | ♦ |  |  |  |
| **Financial** |  | ♦ |  |  |
| **Legislative Compliance** |  | ♦ |  |  |

Table 2 - AAA Risk Targets

1. It should be noted that it would be impracticable for AAA to adopt a target level of ‘**low’** for all impact areas as this would create a significant resource burden in attempting to reduce all risks to ‘low’ and an administrative burden to escalate all risks above that level.
2. The intent therefore, is not only to introduce control measures to minimise residual risks to the stated target level or below, but to ensure that all residual risks above the defined target level are escalated and assigned to the appropriate level of authority within AAA.
3. The table below identifies those with the authority for the acceptance of these risks:

|  |  |
| --- | --- |
|  | **Authority for the acceptance of risk above the target level** |
| **Critical Success Factor** | **Low** | **Medium** | **High** | **Very High** |
| **Reputation** | ♦ | Functional Manager/Chapter President | Chief Operations Officer | CEO |
| **Safety** | ♦ | Functional Manager/ Chapter President | Chief Operations Officer | CEO |
| **Financial** |  | ♦ | Functional Manager/ Chapter President | Chief Operations Officer |
| **Legislative Compliance** |  | ♦ | Functional Manager/ Chapter President | Chief Operations Officer |

Table 3 – Authority for Acceptance above Risk Targets

Risk Identification

General

1. The aim of risk identification is to develop a comprehensive list of events that may occur and, if they do, are likely to have an impact on the objectives of AAA. The identification process asks the following questions:
	* + - 1. What might happen or, more simplistically - what can go wrong (risk event)?
				2. What would cause it to happen?
				3. What would the effect on objectives be?
2. In order to ensure their effectiveness, risk identification activities are to involve members of the wider stakeholder community.

### Common Risk Description Structure

1. After identifying a risk, it is crucial that it is captured in a manner that allows the risk to be fully understood by the entire stakeholder community. The method to be used for describing a risk within AAA is as follows:

|  |  |
| --- | --- |
| **Name:**  | Relate name to system impacted and explanation of cause. |
| **Cause/s:**  | Explanation of what might cause the risk event to occur (list each cause). |
| **Consequence:** | Identify local consequences and attempt to identify how these affect major areas |
| Table 4 – Risk Description Structure |

Risk Analysis

General

1. The main objective of risk analysis is to separate the minor acceptable risks from the major ones, and to provide data to assist in the evaluation and treatment of the risk.
2. Risk level is determined by combining the estimates of effect (consequence rating) and cause (likelihood rating) in the Plan of the existing control measures.
3. To ascertain the overall risk level for a particular risk, the likelihood and consequence scores for the risk are extrapolated into the matrix below.

|  |  |
| --- | --- |
| **Likelihood** | **Consequence** |
|  | **Insignificant** | **Minor** | **Moderate** | **Major** | **Severe** |
| **Almost Certain** | Low | Medium | High | **Extreme** | **Extreme** |
| **Likely** | Low | Medium | High | High | **Extreme** |
| **Possible** | Low | Medium | Medium | High | High |
| **Unlikely** | Low | Low | Medium | Medium | High |
| **Rare** | Low | Low | Low | Medium | Medium |

Table 5 – Risk Scoring Matrix

1. As previously stated, identified risks are to be assessed against **all** CSFs. It is not practical to give the risk four different ratings for the risk, therefore, the highest consequence rating against the CSFs is to be used.

Controls

1. When determining the Likelihood or the Consequence of a risk occurring, it is important to take into consideration existing control measures.
2. Controls are those policies, processes and systems that have been designed and implemented over time in response to issues that have occurred. Most risks identified will not be new or unique and there may be some controls already in place to manage them. It is possible that these controls might also be effective in controlling other emerging risks.
3. Controls fit into three distinct types as detailed below:
	* + - 1. **Preventative Controls**. These controls are aimed at preventing the risk occurring in the first place. They include: plans, policies, procedures .etc.
				2. **Detective Controls**. These controls are used to identify failures in the preventative controls. They include: audits, stocktakes, reviews .etc.
				3. **Corrective Controls**. These controls are aimed at minimising the consequences that arise from the issue/incident. They include: Business Continuity Plans and Disaster Recovery Plans, insurance .etc.
4. Once existing controls have been identified, it is necessary to evaluate them for effectiveness.
5. Experience has demonstrated that there is a direct correlation between the effectiveness of an existing control and the likelihood of the risk occurring and/or the impact of the risk. Therefore, the outcome of this evaluation should then influence further analysis of the likelihood and potential consequences of the risk.
6. The following table provides a useful methodology for the assessment of the effectiveness of existing controls:

|  |  |
| --- | --- |
| **Not Effective** | Not effective at all in mitigating the risk (will not have any effect in terms of reducing the likelihood and/or consequence of the risk) |
| **Negligible** | Partial control in some circumstances (will have very little effect in terms of reducing the likelihood and/or consequence of the risk) |
| **Reasonably Effective** | Partial control most of the time (will have some effect in terms of reducing the likelihood and/or consequence of the risk) |
| **Mostly Effective** | Effective in most circumstances (will have a reasonably significant effect in terms of reducing the likelihood and/or consequence of the risk) |
| **Effective** | Fully effective at all times (will significantly reduce the likelihood and/or consequence of the risk at all times). |
| Table 6 –Effectiveness of Control Measures |

Risk Evaluation

1. The purpose of Risk Evaluation is to determine whether a risk requires further treatment. To do this, the risk level established during the Risk Analysis process is compared with the Evaluation Criteria for AAA.
2. It should be noted, however, that simply earmarking a risk for treatment is not necessarily an indication that it will be treated. There will be circumstances whereby, despite the risk level, risks cannot be treated. These circumstances are detailed in the Risk Treatment section below.

Risk Treatment

General

1. Risk treatment consists of determining what will be done in response to the identified, analysed and evaluated risks including identifying resource implications for the implementation of these actions.

Treatment Options

#### General

1. There are four broad treatment options available for the mitigation of identified risks. These are outlined in the following paragraphs.

#### Avoid

1. This option seeks to treat the risk by avoiding the event that would lead to the risk. There will be very few, if any, risks identified within AAA where this treatment strategy will be an option.

#### Mitigate

1. Under this option, responsibility for the treatment of the risk is kept in-house. Risk Treatments that will reduce the likelihood and/or consequence of the risk are developed and recorded in the Risk Register.
2. It needs to be remembered, however, that risk treatments are only effective if they are completed. To that end, all risk treatments need to be adequately resourced in terms of funding and allocation of personnel. In addition, to ensure accountability within AAA, all risk treatments are to have an owner assigned.
3. Upon completion of the risk treatments, the Risk Register is to be updated to reflect completion of the treatment and the risk is to be reassessed as to whether these actions have been successful in reducing the likelihood and/or consequence.

#### Share

1. Risk transfer/share involves devolving responsibility for the management of an activity for which risk have been identified to another party, or, transferring certain consequences (usually financial) to another party. Examples of transferring or sharing of risk include contracting and insurance.
2. The overarching tenet in relation to risk sharing is that if AAA owns the function it still owns the risk.

#### Accept/Retain

1. Risks are accepted or retained for a number of reasons:
	* + - 1. There are no treatment options available (i.e. the risk event is outside AAA’s sphere of influence);
				2. The level of the risk meets the stated target for that type of risk;
				3. The level of the risk is above the target level, however, an informed decision is taken to accept the risk at that level; or
				4. Risk treatment would cost more than the consequences of the risk (but not just in dollar terms).
2. Where a decision to accept a risk is taken, the risk is still to be recorded in the Risk Register along with the reasons behind the decision not to treat the risk.

#### Residual Risk

1. Residual risk is the risk level that remains after all current controls are effective and any new treatments have been implemented and are operating as planned.
2. For risks where the decision is taken to accept the risk, the residual risk level (i.e. post-mitigation) will be the same as the pre-mitigation risk level.

Monitoring and Review

1. As few risks remain static, they need to be regularly reviewed for currency and accuracy. Risk assessment, treatment strategies and the effectiveness of mitigation actions need to be monitored to ensure changing circumstances do not alter priorities or expected outcomes.
2. Risk Owners are to monitor the currency and status of the risks that have been allocated to them and report on them in accordance with the requirements of this plan. This monitoring is to include obtaining assurance that the controls associated with the risk are effective.

Document

Risk Register

1. A critical element for any Risk Management Program is the recording of risks. Risks that are not recorded are not able to be managed and the risk exposure of AAA is unlikely to be reduced. The most effective means of capturing risk is through the use of a Risk Register.
2. The Risk Register captures all of the information necessary to ensure the risk can be effectively managed. An effective Risk Register follows the Risk Management Process as defined in the Standard and allows for the capture of all identified risks, the controls and their effectiveness, the assessed risk level, the treatment strategy and individual treatment actions.

Risk Reporting within AAA

General

1. In order to ensure the ongoing maintenance and effectiveness of the Risk Management Program a report will be provided to the Board at each meeting.
2. The reports that are to be provided are:
	* + - 1. Strategic Risk Report; and
				2. Operational Risk Report.
3. Formats for these reports are provided at **Attachment 3 and 4** respectively.
4. Should a risk be realised, the Board is to be informed immediately.

Conclusion

1. The AAA Risk Management Plan provides the guidance and tools necessary for the consistent and effective management of risk across AAA. In applying the requirements of this Plan, AAA will advance a more systematic approach for the management of risk, which clearly focuses on improving AAA’s risk management culture.
2. The protection of our people, our assets, our reputation and the provision of services to our customers that meet their expectations are the key outcomes of AAA. To that end, the effective identification and management of risks in accordance with this Plan will assist us to achieve these outcomes.

**Jennifer Marsden**

CEO

 March 2016

List of Attachments

1. Risk Management Glossary
2. AAA Consequence Matrix
3. Format of Strategic Risk Report
4. Format of Operational Risk Report