



## FARM-01

# Risk Management Policy

References:	Australian New Zealand Risk Management – Principles and Guidelines (AS/NZS ISO 31000:2018) Australian New Zealand Risk Management Standard (AS/NZS ISO 31000:2009)
Associated Policies/Procedures:	Board Charter FARMC Charter FARM-02 – ACA Risk Appetite Statement
Associated Forms:	

### 1. Introduction

The Australasian Corrosion Association (ACA) is a not-for-profit membership association which promotes corrosion prevention and control through training, information and advocacy.

The ACA Board is committed to achieving best practice in the area of risk management throughout the ACA's operations and activities. In particular members, students and other key stakeholders expect continuous and professional services, prudent management and maintenance of a highly respected reputation and attainment of the Association's objectives.

### 2. Purpose

The aim of this policy is to ensure that the ACA makes informed decisions with respect to its activities by appropriately considering both risks and opportunities.

The application of this policy will enable risk management procedures to identify opportunities and threats and facilitate rigorous decision-making and planning.

### 3. Scope

This policy applies to employees and volunteers of the ACA; this group being referred to as 'staff' or 'staff members'. It also applies to third parties who interact with ACA, such as contractors and consultants.

### 4. Definitions

The *Australian New Zealand Risk Management – Principles and Guidelines (AS/NZS ISO 31000:2018)* defines risk as the effect of uncertainty on business objectives. For the purpose of this policy, 'risk' includes both occasions that will arise that present a hazard or danger to the Association as well as failing to ensure that opportunities are realised for the benefit of the Association and its Members.

'Risk' includes both internal hazards (which the Association can potentially prevent) and external hazards (which may be outside its control).

The *Australian New Zealand Risk Management Standard (AS/NZS ISO 31000:2009)* defines risk management as the "coordinated activities to direct and control an organisation with regard to risk".

## 5. Policy statement

Risk management is an essential element of good governance and management, enabling the ACA to best meet its organisational and strategic objectives. Risk arises in all aspects of the ACA's operations which offers both opportunities and threats and must therefore be managed appropriately. The ACA recognises that while risks may not be eliminated, they can however be identified, controlled, and managed.

The main objectives for managing risks are to:

- Assist the ACA in achieving its strategic objectives;
- Safeguard the ACA's assets – people, financial, property and information;
- Create an environment where all staff members assume responsibility for risk management; and
- Ensure the allocation of ACA's scarce resources prudently and efficiently to its various functions.

## 6. Risk Management Framework

The ACA's risk management framework is a set of components that provides the foundations and organisational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the Association. This framework consists of:

- This policy;
- The ACA Risk Appetite Statement; and
- Risk management procedures and tools.

## 7. Accountabilities & responsibilities

- 7.1. Board:** The ACA Board is ultimately responsible for approving, and committing to, the risk management policy and setting and articulating the ACA's appetite for risk. The Board is responsible for ensuring that appropriate resources, systems and processes are in place to implement the Risk Management Framework across the Association.
- 7.2. Finance, Audit and Risk Management Committee (FARMC):** FARMC is responsible for approving and reviewing the ACA's Risk Management Framework and Risk Register in accordance with the Committee's Charter. FARMC is responsible for reviewing and making recommendations to the Board regarding the Risk Management Policy. FARMC is also responsible for ensuring that key risks have been identified and are being managed appropriately.
- 7.3. Executive Officer (EO):** The EO is responsible for ensuring that the Risk Management Framework and Policy are being effectively implemented across the organisation. The EO is also responsible for providing independent assurance that the risk management controls are implemented and operating effectively.



- 7.4. Staff:** Staff may be risk owners and are responsible for developing an understanding of and becoming competent in the implementation of risk management principles and practices in their work areas.
- 7.5. Contractors and Consultants:** Consultants and contractors have operational responsibilities for the provision of services such as the delivery of courses and other services as required from time to time and are accountable to the ACA for adhering to standards specified in their engagement documentation.

## 8. Risk Management Procedure

### Risk Matrix

Risks will be assessed and rated based on the risk matrix whereby the following two elements of risk are considered:

1. **Likelihood rating for risk occurring** – This is an assessment of the potential frequency of occurrence without reference to management controls and mitigating processes; and
2. **Consequence rating for risk occurring** – This is an assessment of the potential impact, with reference to the relevant category of the risk.

### Risk Management Process

Risks will be assessed and managed based on:

1. **Communicate and Consult** – Effective communication, consultation and education in risk management are necessary to achieve a successful integration of the risk processes into the organisation.
2. **Establishing the Context** – The ACA considers both external and internal factors when identifying and managing risks associated with the achievement of strategic and operational objectives.
3. **Risk Assessment** – The overall process of risk identification, risk analysis and risk evaluation:
  - a. **Risk identification** – Involves considering risk items, in relation to the various risk categories, and their possible causes and impacts.
  - b. **Risk analysis** – Considering the range of causes, sources of risk, consequences, and likelihood to determine an inherent risk rating. Preventative and impact reduction controls can then be identified, along with the effectiveness of these controls, to determine the residual risk rating with these controls in place. The residual rating can then be used to guide further management by the ACA.
  - c. **Risk evaluation** – The residual risk is the level of risk that remains within the ACA after consideration of all existing mitigating practices/controls. The residual risk provides guidance on the required level of attention and when treatment plans are required to be developed to ensure ongoing management of the risk. Risk evaluation involves comparing the level of risk found during the analysis process with the established risk appetite to determine where additional action is required. This can lead to a decision to:



- do nothing further;
  - consider risk treatment options;
  - undertake further analysis to better understand the risk;
  - maintain existing controls; or
  - reconsider objectives.
4. **Risk Treatment** – Involves selecting one or more options for avoiding, removing or modifying risks, removing the source of a risk, changing likelihood or consequence of a risk and implementing those options. It involves identifying and evaluating existing controls and management systems to determine if further action (risk treatment) is required.
5. **Monitoring and Reporting** – Few risks remain static. Continual monitoring and reviewing of risks are essential in considering the adequacy of risk assessments and treatments, and to identify emerging risks. This will ensure the effectiveness of the controls in place and that the risk treatment plans are assessed to ensure changing circumstances do not alter risk priorities.

## 9. ACA Risk Register

The ACA risk register focuses on the specific areas of embedded and control risks associated with the processes which relate to the achievement of the ACA's risk management objectives. It incorporates detailed risk assessment ratings, control effectiveness ratings and risk treatment actions, along with allocation of a risk owner. The risk owner will usually be a staff member who will have responsibility for the management of the risk treatment of an identified risk.

The risk register is reviewed in conjunction with management and forms the basis for assessing residual areas of risks and specific risk control areas where further review, risk management action plans and internal audit may be necessary.

At minimum, the risk register will be reviewed every six months by the Finance Audit & Risk Management Committee and reported to the Board. Key Risk tolerance measures that have been developed within the Risk Appetite Statement will be reported on a quarterly basis.

## 10. Policy Review

FARMC will review the ACA Risk Management Policy at least every three years and the ACA Risk Appetite Statement on an annual basis. Any changes to policy or appetite will be submitted to the Board for approval.

Revision	Change details	Reviewed by	Date reviewed	Approved by	Approval date
1.0	Policy development	Audit, Finance & Risk Committee		Board	27 Aug 2016
1.1	Scheduled review	Audit, Finance & Risk Committee	Oct 2017	Board	11 Nov 2017
2.0	Complete rework of policy	FARMC	Aug 2023	Board	12 Nov 2023