WATERCO
water, the liquid of life

Risk Management Framework

Waterco Limited

Adoption date: 1 July 2020

1. INTRODUCTION

1.1 ASX Recommendations

ASX Recommendations 7.1 – 7.4 require a listed entity to establish a sound risk management framework and periodically review the effectiveness of that framework to ensure that it continues to be sound and that the entity is operating with due regard to the risk appetite set by the Board.

1.2 Alignment with Australian New Zealand standards

This document outlines the processes involved in conducting Risk Assessments and risk management in the Waterco Group. This framework is aligned to the Australian/New Zealand and International Risk Management Standard AS/NZS ISO 31000:2009 Risk Management – Principles and Guidelines, and The Committee of Sponsoring Organizations of the Treadway Commission (COSO) Enterprise Risk Management – Integrated Framework.

1.3 Purpose of policy

(a) Due to the size of the group, the Waterco Group have not established a separate risk management committee. This policy sets out the risk management framework, overseen by the Board, which guides the Board and Employees in efficiently and effectively monitoring, managing and dealing with sources of risks and risk mitigation measures.

(b) The application of the Risk Management Policy and Framework will provide the basis for the following:

(i) a consistent approach by all staff in identifying, assessing and managing risk across the Waterco Group;

(ii) making risk management part of the day-to-day decision making and planning of staff;

(iii) identifying potential problems before they occur so that risk management activities may be planned and carried out to mitigate adverse impacts on achieving Company objectives;

(iv) pro-active rather than re-active management of risks;

(v) promoting a culture of risk awareness;

(vi) strengthening internal controls to mitigate risk; and

(vii) ensuring the Waterco Group meets its risk management obligations.

(c) the risk management framework provides the foundation for designing, implementing, monitoring, reviewing and improving risk management within the Waterco Group of Companies. While the ultimate responsibility for the Company's risk management framework rests with the Board, it guides all staff in effectively identifying, assessing and managing risk in day-to-day decision making and planning.

1.4 Who does this policy apply to?

This policy applies to the Waterco Group and its Personnel.

1.5 Definitions

(a) **ASX** means the Australian Securities Exchange.

(b) **ASX Recommendations** means ASX Corporate Governance Principles and Recommendations (4th Edition).

(c) **Board** means the Board of directors of Waterco Limited.

(d) **Company** means Waterco Limited ACN 002 070 733.

(d) **Controls** means measures that modify risk.

(e) **Employee** means any person employed by the Waterco Group on a full-time, part-time or casual basis.

(f) **Establishing the Context** means defining the external and internal parameters to be taken into account when managing risk, setting the scope for risk management processes and criteria against which the risks will be assessed respectively.

(g) **Event** means an incident or occurrence from an internal or external source that affects the achievement of objectives. Events can have negative impacts, positive impacts, or both. Events with a negative impact represent risks and events with a positive impact represent opportunities.

(h) **Impact** means the outcome of an Event the effect it has on objectives.

(i) **Inherent Risk** means a risk in the absence of any controls management might take to reduce the risk's impact and likelihood.

(j) **Level of Risk** means the magnitude of a risk and expressed in terms of a Risk Priority Number.

(k) **Personnel** means all Waterco Group Employees, directors, contractors, suppliers and consultants.

(l) **Residual Risk** means the risk that remains after application of controls i.e., the net risk or risk after putting in place controls.

(m) **Risk** means any uncertain Event which, should it occur, will have an effect on the achievement of objectives. It is measured in terms of Impact and likelihood of occurrence. Risks can arise due to external and internal influences:

(A) External risks are exposures that result from environmental conditions that the organization cannot influence, such as regulatory, environmental, weather and market conditions.

(B) Internal risks are exposures that derive from decision-making and the use of internal and external resources, including the organization's operations and objectives.

(n) **Risk Appetite** means the amount of risk an entity is willing to accept in pursuit of its objectives. It is established by management and is linked to the entity's corporate objectives. Risk appetite is not the same for all objectives; in one objective, management may be risk-seeking to seize the potential for high returns while in another objective, management may be risk-averse in exchange for greater protection.

(o) **Risk Assessment** means the overall process of risk identification, risk analysis and risk evaluation.

(p) **Risk Criteria** means the basis against which the significance of a risk is evaluated. Without a standard of comparison (or benchmark) it is not possible to evaluate risk.

(q) **Risk Owner** means a person that has been given the authority to manage a particular risk and is accountable for doing so.

(r) **Risk Priority Number** means a tool to measure the size of the risk and set priorities for Risk Treatment. It is calculated by a combination of Impact and likelihood. A high number means that the risk is high and has top priority in Risk Treatment.

(s) **Risk Profile** means the description of the entity's top risks, the controls to manage those risks and the acceptable Level of Risk the entity is prepared to accept. It determines how the entity's willingness to take risk will affect its overall decision-making strategy.

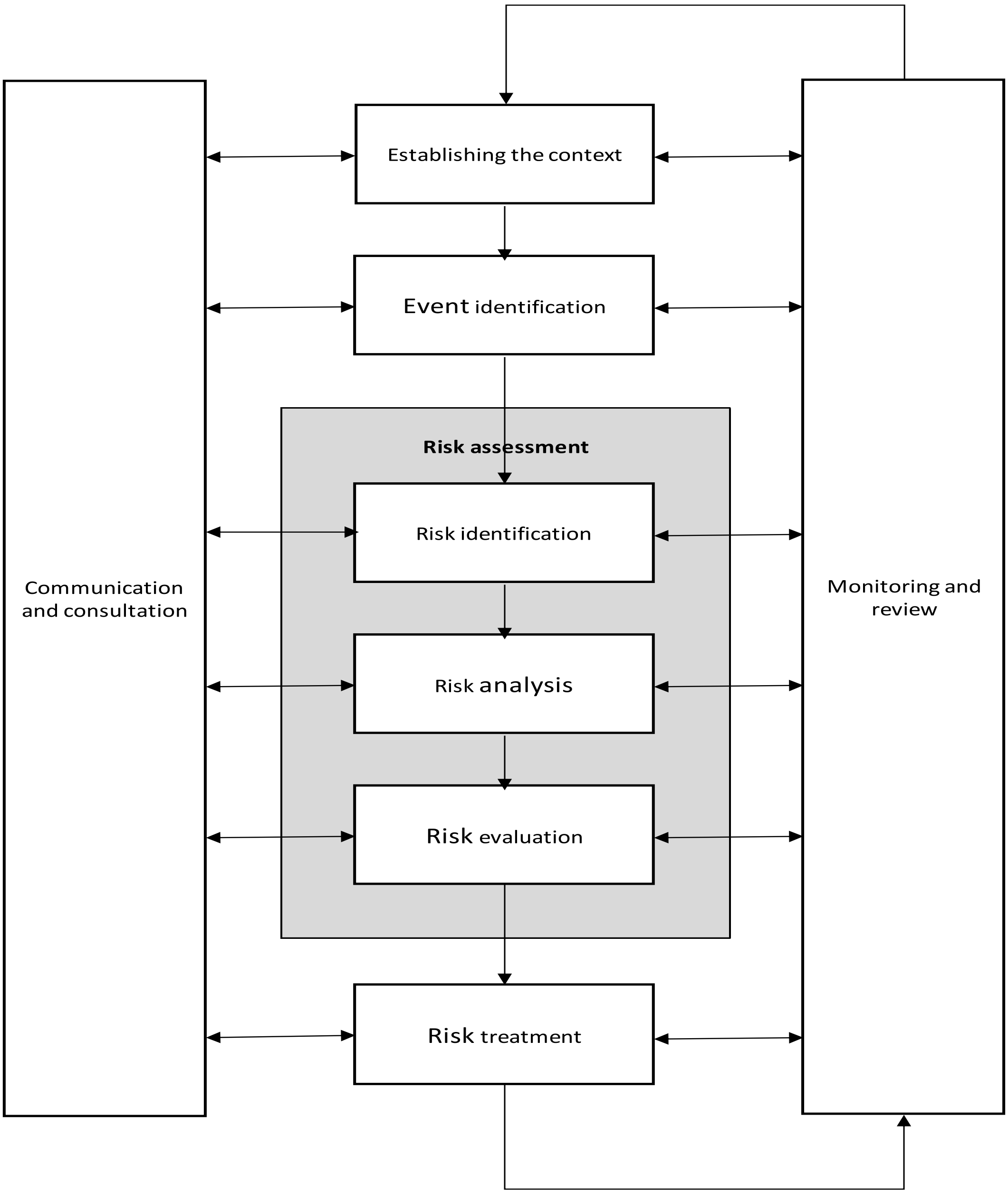
(t) **Risk Register** means the spreadsheet to record, manage and monitor all the identified risks that affect the achievement of objectives, including the existing controls to mitigate the risks, impact on objectives, probability of occurring, risk priority number, Risk Treatment action plan, Risk Owners, time frame for implementing the Risk Treatment action plan, and status of the Risk Treatment action.

(u) **Risk Tolerance** means the amount of variation in risk that the entity is willing to bear in pursuit of its objectives i.e., how much they are willing to deviate from their objectives.

(v) **Risk Treatments** means the processes to modify risk.

2. RISK MANAGEMENT PROCESS

The risk management process is designed to ensure that risk will be assessed and managed in a consistent manner, and a common language is used and understood across all entities within the Waterco Group. The risk management process consists of eight elements, as shown in the diagram below.



2.1 Communication and consultation

At all stages of the risk management process there should be communication and consultation with external and internal stakeholders. This involves providing, sharing and obtaining information to address issues relating to the risk, its causes, its consequences, and the measures being taken to treat it, to ensure that staff responsible for managing risk understand the basis on which decisions are made, the reasons why particular Risk Treatment options are selected and why certain risks are accepted or tolerated.

2.2 Establishing the Context

Establishing the Context is defining not only the corporate and business objectives of external and internal stakeholders but also the external and internal parameters, scope and Risk Criteria to ensure risks are assessed in a consistent manner. Both the external and internal context should be established because risk can arise from Events which are external or internal to the organization.

2.3 Establishing the external context

The external context is the external environment in which the organization operates and seeks to achieve its objectives. Understanding the external context is important in order for the objectives and concerns of external stakeholders to be considered when developing Risk Criteria. It can include, but is not limited to:

(a) the social, cultural, political, legal, regulatory, financial, technological, economic, natural and competitive environment; and

(b) relationships with, perceptions and values of external stakeholders, such as customers, suppliers, and regulatory authorities.

2.4 Establishing the internal context

The internal context is the internal environment in which the organization functions and seeks to achieve its objectives. It can include, but is not limited to:

(a) the modelling of behaviour amongst individuals in management;

(b) oversight by the Board;

(c) strategies, systems and procedures in place to achieve objectives;

(d) risk consciousness, integrity, ethical values and competence of its people;

(e) the organization's risk management philosophy, Risk Appetite, and Risk Tolerance;

(f) roles, authority, responsibility and accountability of the people clearly defined in the organization structure; and

(g) the way management assigns authority and responsibility, and organizes and develops its people.

3. OBJECTIVE SETTING

3.1 There must first be objectives before management can identify, analyse and evaluate risk, and take necessary action to treat the risk. The organization has four categories of objectives namely, strategy, operations, reporting and compliance.

3.2 Vision and mission statements set out in broad terms what the organization aspires to achieve. From this, management sets strategic objectives, formulates strategy, and establishes operations, maintains compliance and evaluates and reports on outcomes.

3.3 **Strategic objectives** are high level goals, aligned with and supporting the organization's vision and mission.

3.4 **Operations objectives** relates to the effectiveness and efficiency of the organization's operations, including performance and profitability goals (Key Performance Indicators - KPIs) and safeguarding assets against loss.

3.5 **Reporting objectives** relates to the reliability of reporting. They include internal and external reporting.

3.6 **Compliance objectives** relate to adherence to relevant laws and regulations.

3.7 Objectives should be **SMART**:

(a) **Specific** – should be clear and precise, not vague.

(b) **Measurable** – should be able to measure whether the organization is meeting the objective. If it is not measurable, it is not possible to know whether the organization is meeting the objective.

(c) **Achievable** – should be achievable and not be beyond reach. Goals can be stretched but not unachievable. Setting goals that are not achievable will reduce motivation and lead to people applying little energy or enthusiasm to what they find as a futile task.

(d) **Relevant** – should be relevant and aligned to the organization's vision and mission.

(e) **Time bound** – should have a deadline for the achievement of the objective. Setting deadlines for when a task should be completed adds a sense of urgency to the task to the task and prompts action.

4. RISK IDENTIFICATION

4.1 Risk identification is the first subset of Risk Assessment.

4.2 The identification of risks is a critical activity at both a strategic and operational level. It needs to include all significant Events that affect the achievement of objectives, including those beyond the organization's control. If a risk/threat is not identified, it will not be included for Risk Assessment and treatment. The objective of this step is not to create an onerous and lengthy list of all possible risks, but to identify all significant risks that could impact the organization.

4.3 Risk can be identified through the use of focus groups, brainstorming approaches, workshops and interviews with respective people.

4.4 In identifying the risk, consideration should be given to the following questions.

(a) **What could happen** – what might go wrong or what might prevent the achievement of objectives? What Events or occurrences could threaten the achievement of objectives?

(b) **How could it happen** – is the risk likely to occur at all or happen again? If so, what could cause the risk Event to recur or contribute to it happening again?

(c) **Where could it happen** – is the risk likely to occur anywhere, in any environment or place? Or is it a risk that is dependent on a location, physical area or activity?

(d) **Why might it happen** – what factors would need to be present for the risk to occur again?

5. RISK ANALYSIS

5.1 Risk analysis is the second subset of Risk Assessment.

5.2 Once the risks have been identified the next step is to look at the strengths and weaknesses of existing controls to mitigate the identified Events (risks), measure the Impact of the risk and likelihood of occurrence after taking into account the existing controls that are in place, and rank the risk by assigning a risk priority number. The process involves the following steps:

(a) **Identify the existing controls** – determine what controls are already in place to mitigate the Impact of the risk and likelihood of the risk's occurrence. Controls may include policies and procedures, management reviews, segregation of duties, authorizations, physical barriers, and IT application controls.

(b) **Assess the Impact** – assess the Impact or consequences if the risk Event occurred on a scale of 1 to 5 according to the criteria set out below.

Score	Impact Criteria	Explanation
5 (Extreme)	• Financial	• Financial loss more than $500,000
	• Reputational	• International long-term negative media coverage; irrecoverable loss of market share
	• Regulatory	• Significant prosecution and fines, litigation including class actions, incarceration of management
	• Health, Safety, Environment	• Significant injuries or fatalities to Employees or third parties, such as customers or vendors
	• Employee and Operational	• Multiple senior leaders leave
4 (Major)	• Financial	• Financial loss between $250,000 and $500,000
	• Reputational	• National long-term negative media coverage; significant loss of market share
	• Regulatory	• Report to regulator requiring a major project for corrective action
	• Health, Safety, Environment	• Limited in-patient care required for Employees or third parties, such as customers or vendors

Score	Impact Criteria	Explanation
	• Employee and Operational	• Some senior managers leave, high turnover of experienced staff, extreme Employee dissatisfaction
3 (Moderate)	• Financial	• Financial loss between $100,000 and $250,000
	• Reputational	• National short-term negative media coverage
	• Regulatory	• Report of breach to regulator with immediate correction to be implemented
	• Health, Safety, Environment	• Out-patient medical treatment required for Employees or third parties, such as customers or vendors
	• Employee and Operational	• Widespread Employee morale problems and high turnover
2 (Minor)	• Financial	• Financial loss between $10,000 and $100,000
	• Reputational	• Local reputational damage
	• Regulatory	• Reportable incident to regulator, no follow-up
	• Health, Safety, Environment	• No or minor injuries to Employees or third parties, such as customers or vendors
	• Employee and Operational	• General Employee morale problems and increased in turnover
1 (Incidental)	• Financial	• Financial loss less than $10,000
	• Reputational	• Local media attention quickly remedied
	• Regulatory	• Not reportable to regulator

Score	Impact Criteria	Explanation
	• Health, Safety, Environment	• No injuries to Employees or third parties, such as customers or vendors
	• Employee and Operational	• Isolated Employee dissatisfaction

(c) **Assess the likelihood** – assess the likelihood of the risk occurring on a scale of 1 to 5 according to the criteria set out below:

Rating	Explanation
5 (Almost certain)	Has occurred at least once in last year or more than 80% likelihood of occurrence in next 5 years
4 (Likely)	Has occurred at least once in last 2 to 3 years or more than 60% but less than 80% likelihood of occurrence in next 5 years
3 (Possible)	Has occurred at least once in last 4 to 5 years or more than 40% but less than 60% likelihood of occurrence in next 5 years
2 (Unlikely)	Has occurred at least once in last 6 to 7 years or more than 20% but less than 40% likelihood of occurrence in next 5 years
1 (Rare)	Has not occurred in the last 7 years or less than 20% likelihood of occurrence in next 5 years

(d) **Rank the Level of Risk** – rank the risk to set priorities for Risk Treatment according to the Risk Priority Number as per the matrix below. A high risk priority number means that the Level of Risk is high and should be given priority in Risk Treatment.

Risk Priority Number

		1	2	3	4	5
High	5	15	19	22	24	25
Impact	4	10	14	18	21	23
	3	6	9	13	17	20
	2	3	5	8	12	16
Low	1	1	2	4	7	11
		1	2	3	4	5

Likelihood

Low High

6. RISK EVALUATION

6.1 Risk evaluation is the third and last subset of Risk Assessment.

6.2 Based on the outcome of the risk analysis, the Residual Risk is evaluated by comparing it with the Risk Criteria, Risk Appetite and Risk Tolerance to decide on an appropriate risk response. Four responses are available, and they are as follows:

(a) **Avoid the risk** – not to accept the risk. It involves exiting the activities giving rise to the risk, declining expansion to a new geographical market, or selling a division.

(b) **Reduce the risk** – action is taken to reduce risk Impact or likelihood, or both. This involves implementing controls to reduce occurrence of the Event in order to achieve the desired objectives.

(c) **Share the risk** – reduce the Impact or likelihood, or both by sharing with another party the burden of loss associated with the risk. Techniques used include the purchasing of insurance policies, outsourcing of an activity, and entering into a joint venture or partnerships.

(d) **Accept the risk** – accept the risk because the Inherent Risk or the Residual Risk is within the Risk Appetite or Risk Tolerance, or no treatment is available, or treatment costs are prohibitive. No action is taken to affect Impact and likelihood.

6.3 Having decided on an appropriate response for each risk, the next step is to set a desired risk priority by numbering the risk. Applying Risk Treatment to reduce the risk or share the risk should move the risk at least one box vertically down or one box horizontally to the left or one box diagonally down to the left. The desired risk priority number is the goal to achieve before the next annual review of the Risk Register.

7. RISK TREATMENT

7.1 This step involves designing a Risk Treatment action plan to get to the desired risk priority number as established above. The treatment plan should detail the controls that will be implemented to reduce the Impact and/or likelihood, person responsible, time frame for implementation, and review process to monitor the progress of the treatment process.

7.2 The controls should prevent, detect, correct and deter occurrence of risk Events.

(a) **Preventive control** – are controls to prevent unwanted Events from occurring. Examples are:

(i) segregation of duties;

(ii) supervision;

(iii) authorization; and

(iv) physical barriers/locks.

(b) **Detective control** – are controls to detect unwanted Events that may have occurred. Examples are:

(i) reviews of exception reports;

(ii) reconciliations;

(iii) rolling stock count; and

(iv) internal and external audits.

(c) **Corrective control** – are restorative actions that can be taken after an unwanted Event has been detected. Examples are:

(i) training; and

(ii) changes to procedures.

(d) **Deterrent control** – are controls to deter and discourage individuals from initiating a risk Event. Examples are:

(i) CCTV systems and alarms;

(ii) warning signs; and

(iii) physical barriers/locks.

8. MONITORING AND REVIEW

8.1 The objective of this step is to monitor the risk, and the control effectiveness and progress of the Risk Treatment action plan. Risk owners should regularly review the risks to determine whether the Risk Profile has changed and whether new risks have emerged. If the risk has increased, further controls will be necessary to mitigate the risk.

8.2 The outputs of the risk management process should be documented in a Risk Register to ensure that the identified risks were analysed, evaluated and treated in accordance with the risk management framework. The Company's Risk Register is appended below.

9. BOARD REVIEW

9.1 This Framework and the effectiveness of the risk management process will be reviewed annually by the Board to satisfy the it that it continues to be sound and the entity is operating with due regard to the Risk Appetite set by the Board.

9.2 The Board has determined that the Audit Committee can deal efficiently and effectively with the evaluation and improvement of the Company's governance, risk management and internal control processes without establishing an internal audit function. The Board will periodically review whether this continues to be appropriate or whether a separate internal audit function is necessary.

10. APPENDIX – WATERCO LIMITED RISK REGISTER

Waterco Limited Risk
Register.xlsx