



Risk Management Framework

Waterco Limited

Adoption date: 1 July 2020 (Revision 1: 28 August 2026)

TABLE OF CONTENTS

1	Introduction	2
2	Purpose	2
3	Everyone's Responsibilities	3
4	Definitions	3
5	Risk Management	4
6	Control Environment	6
7	Objective Setting	6
8	Event Identification	7
9	Risk Assessment	7
10	Risk Response	10
11	Control Activities to Reduce / Mitigate the Risks	11
12	Monitoring	12
13	Information and Communication	13
14	Roles and Responsibilities	13
15	Approval and Review	14

1 INTRODUCTION

- 1.1 Management recognises that uncertainties exist, but does not know whether the risk will occur, or when, or its impact, should it occur.

1.2 ASX Corporate Governance Principles and Recommendations

ASX Recommendation 7 (4th edition), 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.

1.3 Alignment with Australian Standard and COSO Framework

This document outlines the processes involved in conducting Risk Assessments and risk management in the Waterco Group. This framework is aligned to the Australian Standard AS ISO 31000:2018 Risk Management – Guidelines and The Committee of Sponsoring Organizations of the Treadway Commission (COSO) Enterprise Risk Management – Integrated Framework.

2 PURPOSE

- 2.1 A risk management framework is a structured system that outlines how an entity identifies, assesses, manages, monitors and reports risks. Hence, the purpose is to provide guidelines on managing risk to the achievement of objectives, and to embed in all the staff to think about and manage risk as part of their daily operations and decision making.

- 2.2 The application of the risk management framework will provide the basis for the following:

- (1) a consistent approach by all staff in identifying, assessing and managing risk across the Waterco Group;
- (2) making risk management part of the day-to-day work activities, including planning and decision making;
- (3) identifying potential problems before they occur so that risk management control activities may be planned and carried out to mitigate adverse impacts on achieving Company objectives;
- (4) pro-active rather than re-active management of risks;
- (5) promoting a culture of risk awareness;
- (6) strengthening internal controls to mitigate risk; and
- (7) ensuring the Waterco Group meets its risk management obligations.
- (8) 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 planning and decision making.

3 EVERYONE'S RESPONSIBILITIES

- 3.1 Risk Management is a central part of strategic and operational management. Everyone in Waterco has a responsibility for risk management. The Group Chief Executive Officer is ultimately responsible and should assume responsibility. Other managers support the risk management philosophy, promote compliance and manage risks within their spheres of responsibility. Other personnel are responsible for executing risk management in accordance with the risk management framework. The Audit Committee provides oversight on the effectiveness of risk management.

4 DEFINITIONS

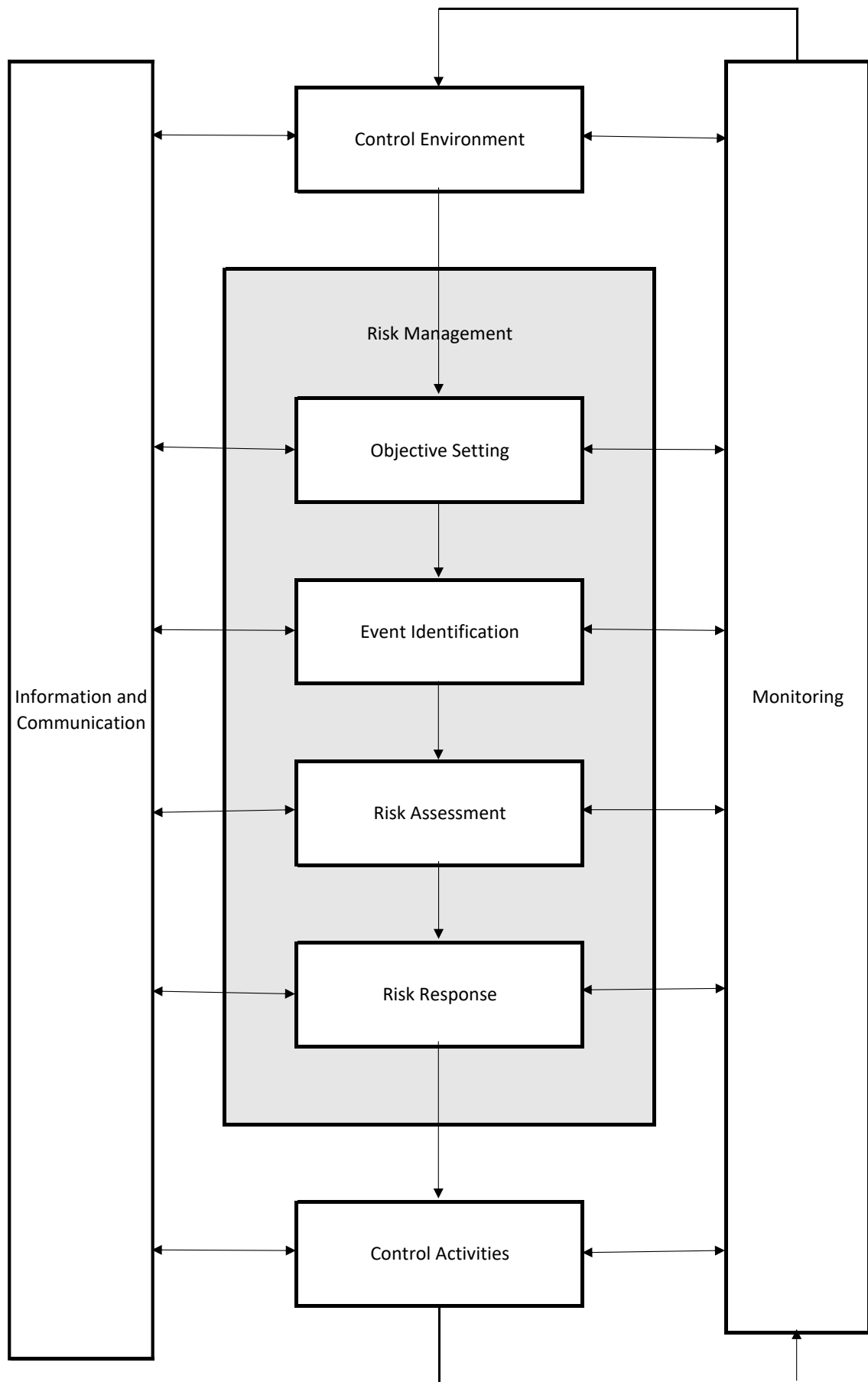
- 4.1 **Board** means the board of directors of Waterco Limited.
- 4.2 **Control Activity** means an action established through policies and procedures that help ensure that management's directives to mitigate risks to acceptable levels and to the achievement of objectives are carried out.
- 4.3 **Event** 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.
- 4.4 **Existing Controls** means the control activities / procedures to mitigate the inherent risks.
- 4.5 **Impact** means the effect of an Event.
- 4.6 **Inherent Risk** means a risk in the absence of any controls management might take to reduce the risk's impact and likelihood.
- 4.7 **Key Risk Indicator (KRI)** means a quantifiable metric to monitor, measure and provide early warning signals of escalating risk levels. It is a forward-looking measure to help management anticipate and mitigate potential threats before the risk escalates to high / extreme.
- 4.8 **Likelihood** means the possibility that a given Event will occur.
- 4.9 **Level of Risk** means the magnitude of a risk and expressed in terms of a Risk Priority Number.
- 4.10 **Management** means the Chief Executive Officer and senior management team
- 4.11 **Opportunity** means the possibility that an event will occur and positively affect the achievement of objectives (or provide a greater likelihood of achieving objectives)
- 4.12 **Residual Risk** means the risk that remains after application of controls i.e., the net risk or risk after putting in place controls to mitigate inherent risk.
- 4.13 **Risk** means any uncertain event, which, should it occur, will have an effect on the achievement of objectives. An effect is a deviation from the expected; it can be positive (opportunity) or negative (risk). Risk is measured in terms of Impact and likelihood of occurrence.
- 4.14 **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.

- 4.15 **Risk Assessment** means the overall process of risk identification, risk analysis and risk evaluation.
- 4.16 **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.
- 4.17 **Risk Owner** means a person that has been given the authority to manage a particular risk and is accountable for doing so.
- 4.18 **Risk Priority Number (RPN)** means a numerical score to measure the severity of the risk and set priorities for Risk Treatment. It is calculated where the impact-axis and likelihood-axis intersect in the Risk Priority Number Matrix on page 9. A high number means that the risk is high and has top priority in Risk Treatment.
- 4.19 **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.
- 4.20 **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.
- 4.21 **Risk Response** means the decision to avoid, reduce, share or accept a risk.
- 4.22 **Risk Tolerance** means the acceptable levels of variation relative to the achievement of objectives. For example, a company targets on-time delivery at 98%, with acceptable variation in the range of 96% to 100% of the time.
- 4.23 **Risk Treatments** means the processes to modify risk.

5 RISK MANAGEMENT

- 5.1 Risk management is a process effected by management across the entity to identify potential events that may affect the entity, and manage risk to be within the risk appetite and to provide reasonable assurance regarding the achievement of entity's objectives. This process, consisting of eight interrelated components (namely, Internal Environment, Objective Setting, Event Identification, Risk Assessment, Risk Response, Control Activities, Information and Communication, and Monitoring), is illustrated in the diagram below.



6 CONTROL ENVIRONMENT

- 6.1 The control environment is the foundational component of the risk management framework. It starts with the Board and Management establishing the tone at the top influencing the risk consciousness of the people providing discipline and structure, with regard to the corporate culture, integrity, ethical values, governance and the importance of internal control, including expected standards of conduct.
- 6.2 The key elements of the control environment are:
- (1) Management demonstrates a commitment to integrity and ethical behaviour in all aspects of the entity's activities;
 - (2) The Board demonstrates independence from management, and must be prepared to question and scrutinise management's activities, present alternative views, and act in the face of wrongdoing;
 - (3) Management establishes the corporate culture, ethical values (i.e., the code of conduct), reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives;
 - (4) Management demonstrates a commitment to attract, develop and retain competent individuals in alignment with objectives; and
 - (5) Management holds individuals accountable for their internal control responsibilities in the pursuit of objectives.

7 OBJECTIVE SETTING

- 7.1 There must first be clearly defined objectives before one can identify and assess risks to the achievement of objectives, and take necessary actions to manage the risks.
- 7.2 Within the context of the entity's vision and mission, Management, at the entity level, sets strategic objectives, formulates strategies that are consistent with its risk appetite and, at the activity level, establishes related operations, compliance, and reporting objectives. Briefly, the 4 categories of risk management objectives are defined as follows:-
- (1) **Strategic Objectives** – High level goals that are aligned with and support the entity's vision, mission and risk appetite. They focus on creating and preserving value for the stakeholders.
 - (2) **Operations Objectives** – Ensuring the efficiency and effectiveness of the entity's operations, including performance and profitability goals and safeguarding assets against loss, whether through theft, waste or inefficiency.
 - (3) **Compliance Objectives** – Adherence to policies and procedures and relevant laws and regulations.

- (4) **Reporting Objectives** – Reliability, timeliness and transparency of both internal and external financial and non-financial reporting. They provide accurate and complete information for making informed decisions, and monitoring the entity's activities and performance.

7.3 Objectives should be **SMART** (Specific, Measurable, Achievable, Relevant, Time-Bound).

8 EVENT IDENTIFICATION

- 8.1 The entity should identify internal and external events that will affect its ability to achieve its objectives. Internal events originate within the entity and under the control of management. External events originate outside the entity and beyond the control of management.
- 8.2 Event identification is to find, recognise and describe the risks or opportunities that might prevent or help the achievement of objectives. The aim is to develop a comprehensive list of risks (threats) and opportunities. It then allows management to prepare for threats before they occur, or to tweak the strategy to capitalise on potential gains.
- 8.3 All events regardless of their perceived significance should be identified because any event not identified will be omitted from risk assessment and treatment.
- 8.4 Events are best identified through the use of focus groups, brainstorming, workshops and interviews with relevant people.
- 8.5 Both past and future events should be identified. Past events include payment defaults, production and delivery delays, stockouts, overstocks, product failures, machinery breakdowns, theft, labour shortage, absenteeism, lost-time accidents. Future events include competitors' actions, changes in consumer behaviour, climate, technological, regulatory and geopolitical, global economy, cyber-attacks, loss of key personnel, pandemic, wars.

9 RISK ASSESSMENT

- 9.1 Each identified event should be assessed individually or by category.
- 9.2 The identified events, with the existing controls to mitigate the risks, are assessed from two perspectives – impact and likelihood.
- 9.3 Once the events (risks) are identified, the next steps are to (1) identify and evaluate the existing controls to mitigate the inherent risks; (2) assess the impact of the risk and likelihood of occurrence; and (3) calculate the Risk Priority Number that ranks the severity of the risk. Controls may include preventive and detective controls, and information technology general and application controls.
- 9.3 Based on the strengths and weaknesses of existing controls to mitigate the inherent risks, assess the impact and likelihood on a scale of 1 to 5, from incidental to extreme, according to the quantitative metrics set out below.

IMPACT or CONSEQUENCES

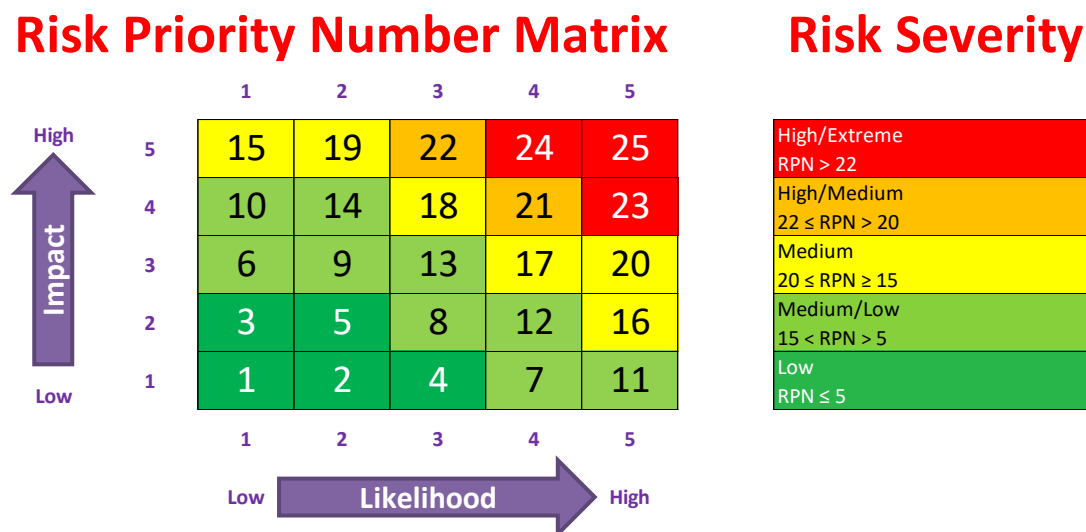
Score	Impact Criteria	Explanation
5 (Extreme)	• Financial • Reputational • Regulatory • Health, Safety, Environment • Employee and Operational	• Financial loss more than AUD500,000 • International long-term negative media coverage; game changing loss of market share • Significant prosecution and fines, litigation including class actions, incarceration of leadership • Significant injuries or fatalities to employees or third parties, such as customers or vendors • Multiple senior leaders leave
4 (Major)	• Financial • Reputational • Regulatory • Health, Safety, Environment • Employee and Operational	• Financial loss between AUD250,000 and AUD500,000 • National long-term negative media coverage; significant loss of market share • Report to regulator requiring major project for corrective action • Limited in-patient care required for employees or third parties, such as customers or vendors • Some senior managers leave, high turnover of experienced staff, not perceived as employer of choice
3 (Moderate)	• Financial • Reputational • Regulatory • Health, Safety, Environment • Employee and Operational	• Financial loss between AUD100,000 and AUD250,000 • National short-term negative media coverage • Report of breach to regulator with immediate correction to be implemented • Out-patient medical treatment required for employees or third parties, such as customers or vendors • Widespread staff morale problems and high turnover
2 (Minor)	• Financial • Reputational • Regulatory • Health, Safety, Environment • Employee and Operational	• Financial loss between AUD10,000 and AUD100,000 • Local reputational damage • Reportable incident to regulator, no follow-up • No or minor injuries to employees or third parties, such as customers or vendors • General staff morale problems and increased in turnover
1 (Incidental)	• Financial • Reputational • Regulatory • Health, Safety, Environment • Employee and Operational	• Financial loss less than AUD10,000 • Local media attention quickly remedied • Not reportable to regulator • No injuries to employees or third parties, such as customers or vendors • Isolated staff dissatisfaction

9.5 Assess the likelihood of the risk occurring on a scale of 1 to 5, from rare to almost certain, according to the quantitative metrics set out below.

LIKELIHOOD OF OCCURRENCE

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

9.6 Calculate the Risk Priority Number (RPN) that ranks the severity of the risk. The RPN is where the impact-axis and likelihood-axis intersect, as depicted in the Risk Priority Number Matrix below.



- 9.7 A high Risk Priority Number means that the severity of the risk is high and should be given priority in risk treatment.
- 9.8 The severity of the risk is classified into 5 levels, as illustrated below.

Risk Severity Levels	Represented by Risk Priority Numbers
High/Extreme	$RPN > 22$
High/Medium	$22 \leq RPN < 20$
Medium	$20 \leq RPN \leq 15$
Medium/Low	$15 < RPN < 5$
Low	$RPN \leq 5$

10 RISK RESPONSE

- 10.1 Having assessed the risk on its impact and likelihood and calculated the Current Risk Priority Number, management analyses the residual risk and selects a response to bring the residual risk within the risk appetite (i.e., the Acceptable Risk Priority Number) or risk tolerance. There are four risk response strategies that management can choose from:
- (1) **Avoid the risk** – not to accept the risk. It involves exiting the activities giving rise to the risk, for instance, declining expansion to a new geographical market, selling a division, or exiting a product line.
 - (2) **Reduce the risk** – action is taken to reduce risk impact, likelihood and risk priority number within the risk appetite or risk tolerance. It involves implementing control activities to reduce occurrence of the Events that affect achievement of objectives.
 - (3) **Share the risk** – reduce the impact or likelihood, or both by sharing the risk with another party. Techniques used include the purchasing of insurance policies, engaging in hedging transactions, outsourcing of an activity, and entering into a joint venture or partnerships.
 - (4) **Accept the risk** – accept the risk because the inherent risk or residual risk is within the risk appetite, or no treatment is available to reduce the risk, or treatment costs outweighs the potential impact (cost versus benefit). No action is taken to alter the severity of the risk.
- 10.2 In conjunction with risk response, management selects an Acceptable Risk Priority Number that not only reduces the Current Risk Priority Number in respect of its impact or likelihood or both but also aligns with the Waterco's Risk Appetite Statement.

11 CONTROL ACTIVITIES TO REDUCE / MITIGATE THE RISK

- 11.1 Having selected a risk response, management designs control activities for staff to implement, directly or through application of technology, needed to reduce the residual risks to within the risk appetite and bring the risk level to Accepted Risk Priority Number.
- 11.2 Prior to designing control activities, management identify what are the key causes and gaps in existing controls that affect achievement of objectives.
- 11.3 With key causes and gaps identified, the right control activities can be designed to eliminate the key causes and close the gaps to reduce the residual risks to within the risk appetite and bring the risk level to Acceptable Risk Priority Number.
- 11.4 The Action Plans to Mitigate Identified Gaps should not only detail the control activities but also the action plan owner, due date, status, key risk indicators, and the review process to monitor the progress of the action plan.
- 11.5 Types of control activities are preventive, detective, and information technology general controls and application controls.
- 11.6 **Preventive Controls** – are proactive procedures designed to prevent unwanted Events from occurring. Examples include:
 - (1) Segregation of duties;
 - (2) Supervision;
 - (3) Authorisations and approvals;
 - (4) Pre-numbered documents;
 - (5) Three-way matching;
 - (6) Physical barriers to block unauthorised access like locks;
 - (7) Policies and procedures.
- 11.7 **Detective Controls** – are reactive controls designed to detect unwanted Events that may have occurred. Examples include:
 - (1) Reconciliations, for example, bank reconciliations, debtors and creditors reconciliations;
 - (2) Variance analysis, i.e., comparison of actual results against budgets, standards, prior period, or previous corresponding periods;
 - (3) Management reviews, i.e., evaluation of actual performance to determine whether they are producing the desired results;
 - (4) Exception reports;
 - (5) Rolling and annual stock counts;

- (6) CCTVs and alarms;
- (7) Internal and external audits.

11.8 **General Controls** – are proactive controls designed to prevent unwanted Events that would compromise the 24/7 availability of the computer system from occurring. Examples include:

- (1) Physical and logical access controls, for example passwords, multi-factor authentication;
- (2) Contingency planning - business continuity plan and disaster recovery plan;
- (3) Data backup and off-site backup
- (4) Antivirus and firewall

11.9 **Application Controls** – are proactive controls designed to prevent unwanted Events that would compromise the integrity, accuracy, completeness and security of the data processing in the computer system from occurring. Examples include:

- (1) Credit limit restrictions;
- (2) Purchase order approval limits;
- (3) Sequence checks;
- (4) Check digits;
- (5) Error reporting, i.e., exception reports.

12 MONITORING

12.1 Each Waterco entity maintains a risk register to record the work done in identifying, assessing, prioritising, mitigating, monitoring and reviewing the risks affecting the achievement of objectives.

12.2 Management conducts ongoing monitoring activities to:

- (1) determine whether the Risk Profile has changed and whether new risks have emerged; and
- (2) assess the presence and functioning of the control activities to mitigate risks, and to gain assurance on the effectiveness of the Action Plans to Mitigate the Identified Gaps.

12.3 Ongoing monitoring is performed on a real-time basis and reacts dynamically to changing conditions.

12.4 Among the many tools to monitor risk and to provide quick identification of deficiencies in control activities and highlight areas in need of improvement, is the Key Risk Indicator (KRI). It is a forward-looking metric giving the risk owners the ability to anticipate risks before they become likely and escalate to high/medium with RPN greater than 20. Examples of KRIs include

- (1) Percentage of debts over 90 days;
 - (2) Inventory turnover period over 90 days;
 - (3) Percentage of products failing within the first 12 months of purchase;
 - (4) Percentage of Purchase Price Variance exceeding the tolerance limit;
 - (5) Backorder rate (Percentage of a part item not shipped on time);
 - (6) Supplier defective rate (Percentage of defective parts received).
- 12.5 Deficiencies in control activities and areas in need of improvement are reported to management and followed up with relevant risk owners on the corrective and preventive actions taken to bring the risk level to Acceptable Risk Priority Number and increase the likelihood of achieving its objectives.

13 INFORMATION AND COMMUNICATION

- 13.1 Information is needed and communicated to appropriate personnel for identification, assessment and mitigation of risks.
- 13.2 Information must be current, reliable, accurate and timely. Otherwise, it can result in poor assessment of risks and bad management decisions.
- 13.3 Information from internal and external sources are identified, captured, processed, analysed and communicated down, across and up the entity to enable management and staff to carry out their risk management responsibilities.

14 ROLES AND RESPONSIBILITIES

- 14.1 The **Board of Directors** have ultimate responsibility for ensuring an effective system of risk management and internal controls. While the Board oversees the entire risk management and internal control frameworks and sets the company's risk appetite, operational and day-to-day execution is delegated down to management.
- 14.2 The **Audit Committee** assist the Board of Directors to fulfil its risk oversight responsibilities and systems of internal controls. The Committee is not responsible for the executive management of these functions. The Committee engages with management and the Group Corporate Assurance and Advisory Department to ensure that management has proactively established, implemented and maintained policies and procedures and control activities to identify, assess and mitigate risks and to safeguard assets and prevent fraud.
- 14.3 The **Group Corporate Assurance and Advisory Department (GCAAD)** acts as the third line of defence. They provide assurance to the Audit Committee and management on the effectiveness of risk management and internal controls. Their role is to evaluate and recommend improvements on the identification, assessment and mitigation of risks, and the presence and effectiveness of

internal controls to safeguard assets, detect errors and prevent fraud. GCAAD does not own or manage risks and internal controls – that is the responsibility of management.

- 14.4 The **Chief Executive Officer** (CEO) is responsible for providing leadership and direction to management for designing and implementing an effective system of risk management and internal controls. The CEO sets the tone at the top and holds senior management accountable for managing risks and implementing internal controls.
- 14.5 **Senior Management** (including the Chief Financial Officer) assist the CEO in designing, implementing and maintaining an effective system of risk management and internal controls. They, being the risk owners and second line of defence, are tasked to identify, assess and mitigate risks and to safeguard assets, detect errors and prevent fraud on a day-to-day basis.
- 14.6 **Staff**, being the first line of defence in risk management and internal control, are responsible to strictly comply, follow and implement the policies and procedures, control activities, relevant laws and regulations to mitigate risks and protect Waterco against financial loss, litigation and reputational damage, including reporting to management instances of internal control breakdown and near misses.

15 APPROVAL AND REVIEW

- 15.1 This Framework is approved and adopted by the Audit Committee and Board of Directors respectively, and will be reviewed regularly to take into account any new changes, and to maintain relevance and effectiveness of the risk management system.