Queensland Government

GOLD COAST WATERWAYS AUTHORITY

Risk Management Framework

MAY 2020

Risk Management Framework
Table of Contents

1.0 About this framework 3

1.1 Definition of Risk 3

1.2 GCWAs Risk Management Framework 4

1.3 Management of Risk 5

1.4 Purpose of risk management 6

2.0 Framework for Management of Risk 7

2.1 Risk Management Process 7

2.2 Summary 15

3.0 Review 15

. **Revision History**

Version	Status	Completed by	Date	Reviewed by	Date	Comments
V.01	Approved	W Turner	22.04.2014	MGT Audit Committee Board	22.04.2014	Endorsed
V.02	Revised	J Bourner	14.11.2016	C Turner	21.11.2016	Final Draft ARC Approval
V.03	Revised	J Bourner	06.12.2016	C Turner	19.12.2016	Risk Appetite included Board Approved
V.04	Revised	J Bourner	28.05.2020	C Turner	29.05.2020	Updated to align to ISO 31000:2018 Board Approved 22.06.2020

1.0 About this framework

The Gold Coast Waterways Authority (GCWA) was created as a statutory authority on 1 December 2012 under the Gold Coast Waterways Authority 2012. The Authority is governed by a Board.

GCWA faces unique risks in its operating environment which are both opportunities and threats to the achievement of the strategic objectives of the GCWA and the Queensland Government. The management of risk is part of the GCWAs governance and leadership structure and is fundamental to management of activities within the organisation at all levels. The Risk Management Framework should drive continual improvements in the organisation through regular review, inclusiveness, and leadership.

The Board has recognised that strategy and risk are interrelated and that appetite for certain risk drives strategic goals and outcomes. It is therefore appropriate for the Board to develop a Risk Management Framework which is consistent with its strategic objectives and accountabilities.

1.1 Definition of Risk

The definition of risk adopted by the Authority is **"The effect of uncertainty on the achievement of the Authority's objectives".**

1.2 Principles of Risk Management

The AS/NZS ISO 31000:2018 is the international Risk Management Standard adopted by GCWA to manage the risk to the organisation and the Gold Coast Waterways. The AS/NZS ISO 31000:2018 principles (Figure 1) have be used to guide the GCWAs eight (8) principles of risk management listed below;

1. Risk management activities are integrated within the GCWA
2. Risk management follows a structured and comprehensive framework
3. Risk management is adapted to GCWA operational and strategic imperatives
4. The GCWA Risk Management framework includes operational and strategic activities from across the organisation.
5. The GCWA understands that Risk management required a dynamic framework that is fit for purpose
6. The GCWA Risk management framework, plans and registers are maintained with current data
7. Risk management within the GCWA considers social, cultural, economic and environmental values
8. The GCWA Risk management framework is regularly reviewed and revised to ensure continual improvement

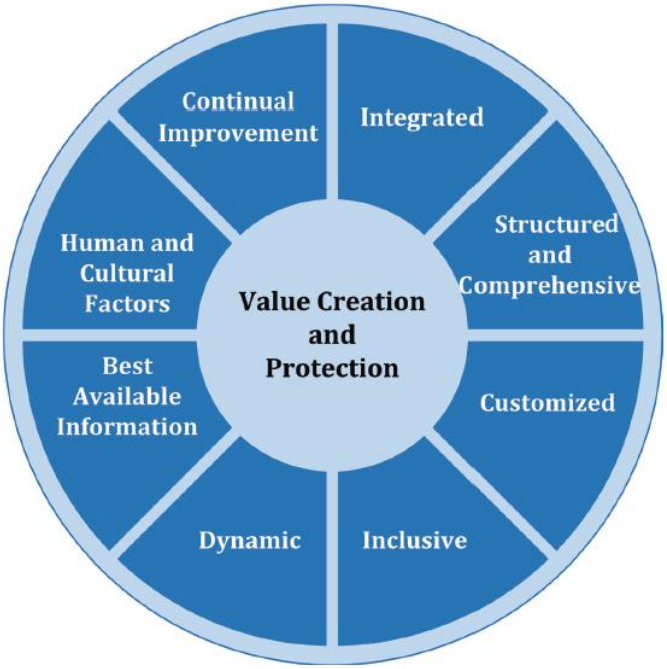

Figure 1 Risk Management Principles (AS/NZS ISO 31000:)

1.3 GCWAs Risk Management Framework

The Gold Coast Waterways Authority Risk Management Framework comprises several elements:

- Risk Management Policy;
- Risk Appetite Statement;
- Risk Assessment and Treatment;
- Risk Register; and
- Risk Management Plan.

1.3.1 Risk Management Policy

The Gold Coast Waterways Authority has developed a Risk Management Policy to foster a risk-aware culture in all decision-making and demonstrate proactive and effective management of risk.

Outcomes of the activities under the policy and Risk Management Plans will be regularly reported to the Board.

1.3.2 Risk Appetite Statement

The Gold Coast Waterways Authority has developed a Risk Appetite Statement to outline the amount and type of risk that the Authority is willing to take in order to meet its strategic objectives.

The Risk Appetite Statement covers a number of critical risk categories as identified in the GCWA Risk Management Framework, Risk Policy and Risk Register which are regularly reported to the Board.

1.4 Management of Risk

Management of risk represents the coordinated activities which direct and control an organisation with regard to risk, that is, it is the culture, processes, systems and structures that are directed towards realising potential opportunities available to an organisation whilst mitigating and managing adverse effects.

AS/NZS ISO 31000:2018 is the international Risk Management Standard which has been adopted as the Australian National Standard and which will be used to guide the Board and senior management of the Authority in managing risk. The following chart sets out the principles, framework, process and attributes of risk management as set out in that Standard.

The Table 1 sets out other definitions associated with risk which is used in relation to the current Standard:

Table 1 AS/NZS ISO 31000:2018 Terms & Definitions

Term	Terms & Definitions
risk	effect of uncertainty on objectives
risk management	coordinated activities to direct and control an organisation with regard to risk
risk management framework	set of components that provide the foundations and organizational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organisation
Risk appetite statement	outlines the amount and type of risk that the Authority is willing to take in order to meet its strategic objectives.
risk management policy	statement of the overall intentions and direction of an organisation related to risk management
risk management plan	scheme within the risk management framework specifying the approach, the management components and resources to be applied to the management of risk
Stakeholder	Person or organisation that can affect, be affected or perceive themselves to be affected by a decision or activity
Risk source	Element which alone or in combination has the potential to give rise to risk
Event	Occurrence or change of a particular set of circumstances
Consequence	Outcome of an event affecting objectives
Likelihood	chance of something happening
Control	Measure that maintain and/or modifies risk

1.5 Purpose of risk management

Managing risk within GCWA is based on the principles, framework and process outlined in the AS/NZS ISO 31000:2018 standard (Figure 2).

Risk management is not a tool to stop or impede an organisation's activities. Instead it is focussed on enabling the GCWA to seize and act upon business opportunities, with a clear view of the risks and the action plans necessary to manage associated risks. Risk management enables the GCWA to achieve the following:

- The Board and senior management are in a position to confidently make informed business decisions based on risk assessments and be assured that compliance obligations are met;
- Risks are able to be identified, prioritised (in terms of likelihood, consequence and frequency) and managed in a proactive and coordinated manner;
- The safety and wellbeing of GCWA staff and users of the waterways and surrounding areas are protected;
- Unexpected adverse and costly outcomes are avoided;
- Costs are reduced through more targeted and effective controls;
- There is better identification and exploitation of opportunities; and
- GCWA compliance with relevant legislation.

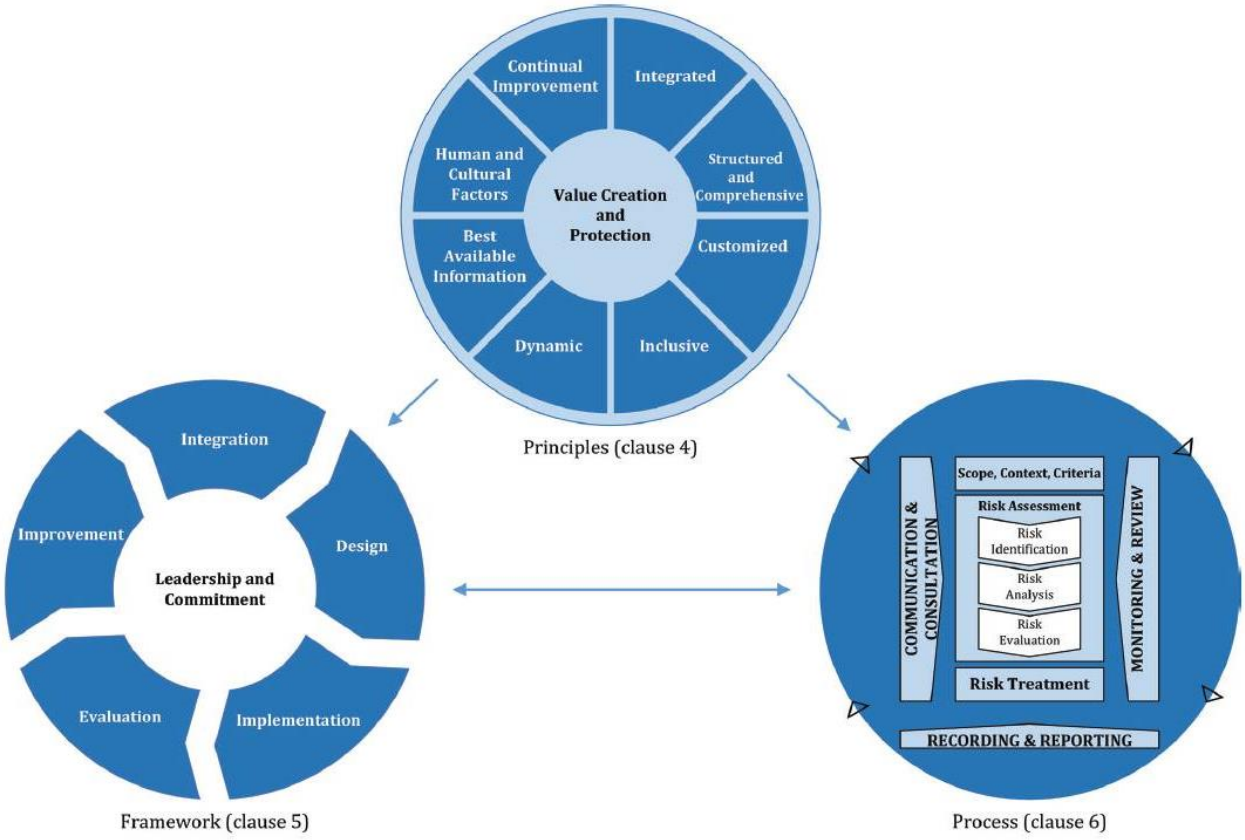

Figure 2 AS/NZS ISO 31000:2018 Relationships between the risk management principles, framework and process

2.0 Framework for Management of Risk

A Risk Management Framework comprises a number of elements:

- Risk Management Policy;
- Risk Appetite Statement;
- Risk Assessment and Treatment;
- Risk Register; and
- Risk Management Plan.

The underlying objective of the GCWA Risk Management Framework is to ensure that risk management is:

- Embedded in the key organisational functions across the Authority;
- Integrated within all work flows, both operational and strategic,
- Consistently applied across the Authority; and is
- Evaluated and reviewed to ensure continual improvement.

Figure 3 Risk Management Framework (AS/NZS ISO 31000:)

2.1 Risk Management Process

It is vital that all potential risks to which the Authority is exposed are identified. Without recognition of the various risks and opportunities, it is not possible to assess their likelihood, consequence and velocity of occurrence. The process can be outlined through a number of steps.

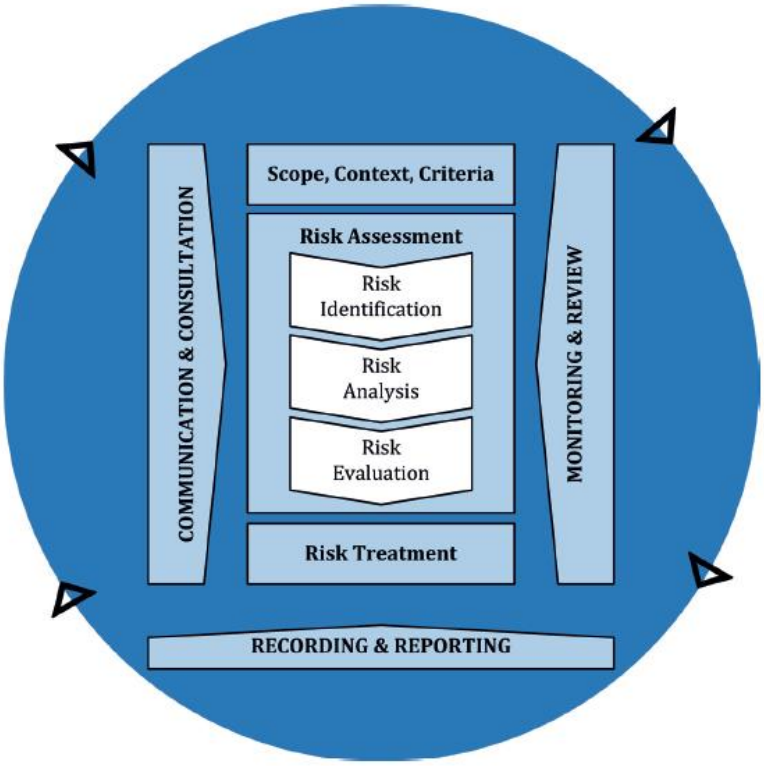

Figure 4 Risk Management Process (AS/NZS ISO 31000:)

2.1.1 Step 1

2.1.1.1 Establish Context (environment)

The first step is focused on establishing the context or the business environment in which the GCWA operates.

2.1.2 Step 2

2.1.2.1 Risk Identification

The identification of the risks which arise from all aspects of the Authority's environment and operations is undertaken with the aim of developing a list of the risks that could impair the achievement of business objectives. It must be emphasised that risk identification is probably the most critical step in risk assessment and should therefore involve the Board and all key management team members/stakeholders. Identification using a well-structured systematic process is critical so as not to miss key risks. This included:

- A workshop involving the Board and senior management;
- Risk scenarios being developed and risks identified;
- Options for treatment of risks being evaluated;
- Development of a risk register which indicates the level of risk faced by the Authority both before and after treatment;
- Continual self-assessment and monitoring of the risk environment;

- Review of reports and external environments;
- Advice from external sources proficient in risk identification in the GCWA strategic or operating environment.

The GCWA has adopted the following primary categories of risk outlines in Table 2 :

Table 2 GCWA Primary Risk Categories

GCWA Primary Risk Categories	
1	Strategic
2	Strategic Planning
3	Regulatory, Legal and Compliance
4	Program and Project Management
5	Operational Performance and Capability
6	Workplace Health and Safety
7	Financial
8	Business Management

Having identified risks to which the Authority is exposed, it is necessary to then assess those risks in terms of likelihood, consequence and velocity. The tables following show likelihood and consequence measures for the identified risks and is designed to assist assessment.

Each risk can be assigned likelihood and consequence with the consequent rating ranging from rare with insignificant impact to almost certain with critical and/or immediate impact.

This will allow the Board and senior management to initially focus on extreme or very high risks (prior to treatment).

It is important to recognise that the initial assessment is undertaken before action is taken to avoid, share, eliminate or mitigate the risk. There will therefore be a need to consider the actions deemed necessary with a view to assessing their effectiveness and their resulting outcomes in terms of changes to the rating of the risk. Adjustments can be made for velocity where appropriate to the type of risk.

2.1.3 Step 3

2.1.3.1 Risk Analysis and Evaluation

Risk analysis and evaluation is about developing an understanding of the risks. It provides input to decisions on whether the risks need to be treated and the most appropriate and cost effective risk treatment strategies. Risk analysis and evaluation requires consideration of the causes and sources of risk, their positive and negative consequences and the likelihood of occurrence (and for some risks the likely velocity of occurrence).

The initial assessment of the level of risk is undertaken on the basis of the risk being “untreated”, that is, without activity on the part of the Board or senior management to avoid, eliminate, share, mitigate or manage the risk. The analysis of risk may be undertaken either quantitatively or qualitatively:

2.1.3.2 Quantitative Analysis

Wherever possible, risks should be quantified as outlines in Table 3 below:

Table 3 GCWA Quantitative Capital and Operational cost categories

Level	Description	Capital Cost	Operational Cost
1	Minor	$0.01M to $0.05M	$0.1M to $0.05M
2	Moderate	$0.05M to $0.1M	$0.05M to $0.1M
3	Major	$0.1M to $3M	$0.1M to $0.25M
4	Critical	>$3M	>$0.25M

Risk Exposure = Consequence x Likelihood where consequence is expressed in monetary terms with reference to the GCWA budgeted capital or operating cost (refer to table above) and likelihood expressed as a probability (in percentage terms) of occurrence.

2.1.3.3 Qualitative Analysis

Where the consequence is intangible or difficult to quantify such as environmental or safety effects, qualitative analysis can be used. It may also be used where the level of risk does not justify the time and resources needed to do a quantitative analysis. Qualitative analysis uses words to describe the magnitude of potential consequence and the likelihood that those impacts will occur. Rating scales are used to provide common understanding of the qualitative analysis. (See table below for guidance in relation to rating of risk consequence).

Table 4 GCWA Qualitative Definition (Risk consequence)

Level	Description	Qualitative Definition
4	Critical	Most objectives cannot be achieved
3	Major	Some important objectives cannot be achieved
2	Moderate	Some objectives affected
1	Minor	No material impact. Effects are easily remedied

Table 5 below sets out the rating given to each risk in terms of likelihood:

Table 5 GCWA qualitative and quantitative likelihood definitions

Level	Descriptor	Qualitative Definition	Quantitative Definition (Probability)
1	Almost certain	This event occurs frequently within GCWA even with current controls you expect an occurrence.	>90%
2	Likely	This event may have occurred in GCWA or 'like' organisations on a regular basis. With current controls or circumstances you can expect occurrence within the financial year.	60%-90%

3	Possible	This event may have occurred occasionally in GCWA or 'like' organisations. Current controls or circumstances suggest there is a distinct possibility of occurrence.	30%-60%
4	Unlikely	The event has occurred infrequently in GCWA or 'like' organisations. Current controls and circumstances suggest the occurrence would be considered highly unusual.	5%-30%

2.1.3.4 Overall rating of risks

Together the ratings attaching to each risk will provide an overall risk rating ranging from Low to Extreme.

Where a risk involves consideration of the velocity of risk and that risk may impact immediately and extensively, it may be appropriate to shift the overall assessment to the right one or more categories depending on the nature and consequence of the risk.

The level of management attention and the time of response required depend on the overall untreated risk rating however the following guidelines are proposed:

Extreme risks

- Immediate action required to implement controls to eliminate, reduce or share risk in a timeframe commensurate with the severity of the impact, and with resolution no later than 1 month. Regular reporting to the CEO and the Board is required, or more frequently, where determined by the CEO;
- Immediate notification to the CEO and to the Board via the CEO in case of a new extreme risk;
- Direct accountability of the position nominated as the Risk Owner; and
- Ongoing monitoring by the Audit and Risk Committee.

High risks

- Attention needed to implement control to eliminate or reduce risk within a maximum of 3 months;
- Management accountability identified; and
- Reviewed monthly by senior management and regularly by the Board.

Medium risks

- Manage by specific monitoring or response procedures; and
- Monitored regularly by senior management.

Low risks

- Manage by routine procedures.

2.1.4 Step 4

2.1.4.1 Risk Treatment

Risk treatment involves identifying the range of options for treating risks, assessing these options and the preparation and implementation of treatment plans. The cost of any risk treatment option must be considered relative to the loss, damage or injury (in the widest sense and not just $) that could be incurred if that risk eventuated. Typical risk treatment options are as follows:

- **Avoid:** avoiding the risk by deciding not to commence or process with the activity that gives rise to the risk, for example, by not providing particular services or not investing in particular asset classes;
- **Accept/Exploit:** talking or increasing the risk in order to pursue an opportunity or outcome; Steps taken to leverage opportunities, for example, reorganise and restructure, renegotiate contracts, etc.; or
- **Share:** Sharing the responsibility or burden of loss through such means as insurance, and outsourcing contracts. This may usually involve a cost or risk premium such as an insurance premium or the premium which a service provider may build into a contract for assuming the risk;
- **Reduce:** Eliminating or reducing the source of risk or reducing the consequence and/or likelihood of its occurrences, for example, quality assurance procedures, preventative and corrective maintenance, day to day procedural and management controls or minimising the consequence of risk, for example, contingency planning, crisis management, contract terms and conditions;
- **Retain:** Through informed decision making accepting the burden of loss, or benefit of gain, from a particular risk. Risk retention also includes the acceptance of risks that have not been identified.

Every decision made on how to treat risks can result in the emergence of new risks. It is therefore important to note that risk treatment can be a combination of two or more risk treatment options and that risk treatment does not stop once a particular risk treatment option has been determined.

After risk treatment decisions have been made, the risk assessment process will be undertaken again to determine the residual risk level. If a residual risk level is deemed too high, the assessment and treatment process will be repeated.

If the Board or management decides to tolerate residual risks, that is, no further treatments are considered cost effective; no further mitigation action will be taken however careful monitoring and regular reviews should be undertaken.

In summary it is the ongoing significant residual risks to which the Authority is exposed which should be the focus of management, monitoring and reporting. Any extreme or very high risks (after treatment) should be reported to the Audit and Risk Committee each quarter and then to the Board.

2.1.4.2 Risk Register

The Risk Management Register was developed to identify risks and opportunities to which the Authority is exposed. It shows untreated and treated scores for identified risks.

2.1.4.3 Risk Management Plan

To effectively manage overall risk, it is necessary to select appropriate treatments, controls or countermeasures to manage or mitigate each individual risk. Risk mitigation needs to be approved by the appropriate level, that is, the Board or a level of management. For example, a risk concerning the image of the Authority should be considered by the Board whereas the CEO would have the authority to decide on a workplace, health and safety risk.

The Risk Management Plan should therefore propose applicable and effective actions for managing the risks. For example, an observed high risk of equipment failure could be mitigated by having access to back up resources perhaps through a standby piece of equipment or access to private resources via a lease. The Risk Management Plan will therefore include on the risk register details of control implementation and the responsible persons for those actions.

As part of the development of a Risk Management Plan, the stage immediately after completion of the risk assessment phase consists of preparing a Risk Treatment Plan, which should document the decisions about how each of the identified risks should be handled. Mitigation of risks often means selection of actions, the reasons for which should be clearly documented.

Once decisions have been made, it is important that accountability for action is assigned to the party most likely to be able to manage the risk and who will be accountable for monitoring and reporting on the risk.

Table 6 indicates the party accountable for risk management within the Authority:

Table 6 GCWA Risk Accountability Legend

GCWA Risk Accountability Legend	
Board	GCWA Board
ARC	Audit and Risk Committee
CEO	Chief Executive Officer
M (P & I)	Manager (Planning and Innovation)
M (PD)	Manager (Program Delivery)
PPM (SMI)	Principal Project Manager (Spit Masterplan Implementation)
M (W)	Manager (Waterways)
M (BS)	Manager (Business Services)
A & FM	Assets and Facilities Manager

Review and evaluation of the Plan

Initial Risk Management Plans are unlikely to be perfect. Practice, experience, and actual results will necessitate changes in the Plan and contribute information to allow possible different decisions to be made in dealing with the risks being faced.

Risk analysis results and Risk Management Plans will be updated periodically. There are two primary reasons for this:

- to evaluate whether the previously selected actions are still applicable and effective; and
- to evaluate the possible risk level changes in the business environment. For example, information risks are a good example of rapidly changing business environment.

2.1.5 Step 5

2.1.5.1 Monitoring and Review

The objective of monitoring and reviewing the risk management process is to ensure that appropriate information is being prepared and provided to the Board, senior management and other stakeholders. In addition, monitoring and review provides an assessment of the performance of the risk management system and framework to ensure that:

- Controls identified are appropriately designed and are operating effectively;
- Appropriate information is being gathered which assists management with improving risk assessments;
- Events are being analysed for lessons to be learnt that can assist/improve the risk management process;
- Changes in the internal and external context are being detected;

- Any emerging risks are being pro-actively identified; and
- That risk profiles anticipate and reflect changing circumstances and new exposures.

Each responsible party must ensure that the monitoring and review requirements are met.

2.1.5.2 Frequency of Actions Required for Monitoring and Review

Annual - Full Risk Review

As part of its annual review of performance against its Strategic Plan, the Board will review the risk profile, and effectiveness of associated controls;

- Senior management will undertake a review of the WH & S risk profile, concurrent with its review of performance against the Strategic Plan; and
- Each area will perform a full review of its risk profile on an annual basis based on the risks for which they are accountable.

Quarterly – Risk Register

- The Audit and Risk Committee will review the risk register at each of its quarterly meetings, followed by Board review.

Periodic - Board Report

- The Board will review all Extreme Risks; and
- Relevant senior management leaders will ensure that all significant risks and risk management actions are discussed and minuted. This will include escalation of any risks to the Board.

Periodic - Urgent escalation of risks

Occasionally, there may be cases where major risk issues requiring Board or management attention are identified by an operating unit. In this instance, the operating unit is required to escalate the major risk issues to its respective Manager as and when they arise. The Manager will be accountable for escalating further as appropriate. The risk will be recorded on the Risk Management Register as per this framework.

2.1.6 Independent Internal Review of Risk Management Framework and Processes

Compliance with the Risk Management Framework and Risk Register will be periodically reviewed as part of the GCWA's rolling internal audit plan. In addition, a scan of the Risk Register will be undertaken as part of the preparation of the Annual Internal Audit Plan to identify controls for testing and will provide observations and feedback to the CEO and risk owners as part of relevant audits.

2.1.7 Communicate and Consult

Communication and consultation with internal and external stakeholders as appropriate are important considerations at each step of the risk management process. They should involve a dialogue with stakeholders with efforts focused on consultation rather than a one-way flow of information from the decision maker to other stakeholders.

Effective internal and external communication is important to ensure that those responsible for implementing risk management, and those with an interest in the issue, understand the basis on which decisions are made and why particular actions are required.

3.0 Summary

The management of risk is part of the all activities associated with GCWA operations and strategic directions and includes interactions with stakeholders to manage and mitigate risks.

The management of risk includes the Risk Management Framework , assessment processes and guiding principles to ensure effective and efficient identification and management of risks.

The development of a Risk Management Framework is to ensure that there is a systematic, structured, dynamic and responsive process in place to enable the GCWA to manage the “effect of uncertainty on objectives”, and indicates that the GCWA has incorporated the processes as outlined in the Risk Management Framework to assist in evaluating the efficacy of the GCWA’s risk management program.

3.1 Review

The Risk Management Framework will be reviewed every five (5) years, or more frequently as appropriate.