Shire of Broome

Risk Management Plan – Enterprise Risks

Version 1.0
November 2022

Table of Contents

List of Figures

List of Tables

Introduction

General

1. The Shire of Broome (SoB) recognises that risk management is fundamental to the organisation achieving its strategic and operational objectives, and that it plays an integral role in day-to-day management and decision making at all levels in the organisation.

2. To enable the Executive (and to a lesser extent Council) to decide on the nature and extent of the risks it is prepared to take to meet its strategic objectives, the organisation must have an appropriate risk management program to identify and manage risk on an ongoing basis. This policy sets out the organisation's approach to risk management, including its approach to identifying and managing risk, the responsibilities of the Council, management and staff within the organisation in relation to risk management, and the resources and processes dedicated to risk management. Everyone has a role to play in the management of risk within SoB, whether as a Risk Owner, a Control Owner, right down to the need for every employee to follow procedures and processes without deviation.

3. The application of effective enterprise-wide risk management practice as a part of the strategic planning and monitoring systems of an organisation ensures that investment decisions are founded on evidence-based decision making and are linked to the strategic directions of the organisation. Good risk management discipline and practice, stress tests the objectives and goals of SoB, and are to be embedded throughout the organisation.

4. Risk management is viewed as central to SoB's management process, having relevance and linkage to the Integrated Planning and Reporting Framework (Strategic Community Plan, Corporate Business Plan, Annual Budget and associated informing strategies) performance, quality and safety.

5. Effective risk management requires Executive Management and all SoB staff to understand the business risks in their area as part of their day-to-day activities. All staff have a role in managing risk and therefore it is important that all employees of the SoB are familiar with the SoB Risk Management Program.

6. Council is committed to the effective management of risks and ensuring that sufficient resources are available to manage risks within the organisation. Those allocated responsibility for managing risks or being accountable for critical controls must ensure appropriate monitoring and reporting occurs through Council's existing management reporting and governance framework.

7. The effective management of risks plays an important role in shaping Council's strategic direction as outlined in the Council's Strategic Community Plan and thereby contributes to evidence-based decision-making and the successful delivery of Council's objectives.

Purpose

8. The purpose of this Risk Management Plan – Enterprise Risk is to describe SoB's approach to the management of its operational risks.

9. This plan informed by AS/NZS ISO 31000 2018 as well as industry best-practice.

Definitions

Risk

10. In developing this plan, SoB has adopted the following definition of risk:

*A possible event or incident that, **if it occurs**, will have an impact on SoB's objectives.*

11. Whilst this definition is a deviation from that detailed in ISO 31000, it is felt that this definition is much easier to communicate to SoB staff and stakeholders.

Risk Management

12. SoB has adopted the following definition of risk management:

*A systematic process that enables SoB to make **informed decisions** as to the actions to be taken in relation to the possible events or incidents that, if they occur will impact on our objectives*

13. This definition also deviates from that detailed in ISO 31000, once again, due to the fact that it is a lot easier to communicate.

14. Additional definitions applicable to this Plan are detailed in the Glossary at **Attachment 1**.

Enterprise (Operational Risks)

15. Enterprise (Operational) Risks are those risks that, if they occur, will impact the achievement of the current strategic objectives. These are the "day-to-day" risks relevant to SoB operations, some of which, if they were to materialise as incidents/events, could have significant impacts and erode community and state government confidence in SoB.

16. All Operational Risks are Enterprise Risks as not all controls will be located in the one functional area, particularly controls residing within the Corporate Services area. What this means is that there is no possibility that an operational risk within SoB will have all of the controls controlling the risk in one functional area. By definition, therefore, this means all operational risks are Enterprise Risks.

17. To that end, SoB's Enterprise Risks will be managed centrally in one database.

Plan Owner, Approver and Review Requirements

18. The Plan owner is the Manager Governance, Strategy and Risk and it is to be reviewed every two years or when there is any significant change to SoB's operational environment. The CEO is the approver for the Plan.

Roles and Responsibilities

19. Roles and responsibilities for the management of risk within SoB are shown in the table below:

Entity	Roles and responsibilities
Council	• Approve SoB's Risk Management Policy • Define SoB's risk appetite • Manage strategic risks and ensure strategies to reduce vulnerability are included in the strategic plan
Audit and Risk Committee	• Review whether a current and comprehensive risk management framework is in place including associated procedures for effective identification and management of SoB's enterprise risks • Monitor implementation of SoB's additional risk treatments • Determine whether a sound and effective approach has been followed in establishing SoB's business continuity planning arrangements, including whether business continuity and disaster recovery plans have been periodically updated and tested
Chief Executive Officer	• Approve SoB's Enterprise Risk Management Plan and oversee its implementation • Consider risks as part of business planning processes • Regularly monitor risks as part of a standing item on the consideration of governance issues at the Executive Management Group (EMG) • Promote a risk management culture within SoB
Manager Governance, Strategy and Risk	• Coordinate the Risk Management Program within SoB • Maintain the Enterprise Risk Register • Develop reports for the Audit and Risk Committee • Maintain the governance framework for the Risk Management Program
Manager People & Culture	• Maintain the SoB Incident Database • Provide notification of incidents to those requiring it within appropriate timeframes
Directors	• Ensure implementation of controls within their division/unit/branch and/or areas of policy responsibility • Promote a positive risk management culture within the directorate
Risk Owners	The Risk Owner is the person assigned the responsibility for the day-to-day management of a risk. Risk Owners are responsible for the following: • Overall coordination of the management of the risk including: • Assurance that controls are effective • Treatments are completed • Monitoring of the environment to identify if there are any indicators the risk might eventuate • Reporting
Control Owners	• Control Owners are assigned the responsibility for the day-to-day management of a control. Control Owners are responsible for maintaining oversight of the effectiveness of the control and for reporting any changes to effectiveness to the Risk Owner

Entity	Roles and responsibilities
Treatment Owners	Treatment owners are responsible for the following: • Implement the treatment as directed • Providing ongoing status of the risk treatment • Reporting any issues that may impact completion within timeframes • Reporting when complete
All staff, including contractors and outsourced service providers	• Ensure the principles of risk management are applied and integrated into the planning and administration of major activities, functions and processes • Recognise, communicate and respond to expected, emerging or changing risks • Report incidents as they occur

Table 1 – SoB Risk Management Roles and Responsibilities

Risk Ownership

20. Whilst incidents will primarily occur within the functional areas, that does not mean the risks are owned within the functional areas. The majority of the controls that are controlling the risk will be policies, procedures etc. that are owned at the Executive/Corporate level. It is not possible for functional managers to be allocated ownership of risks if they do not have ownership/ visibility of the effectiveness of all the controls that are controlling the risk.

21. Risk Owners **must** have the authority in relation to the management of the risk, including decisions as to its acceptability. To that end, risk ownership within SoB will be assigned (where possible) to an Executive who is one level above the highest level of control ownership.

Risk Governance

22. For a Risk Management Program to be effective there needs to be a well-defined risk governance structure.

23. The SoB governance arrangements for the management of risk are detailed in the diagram below:

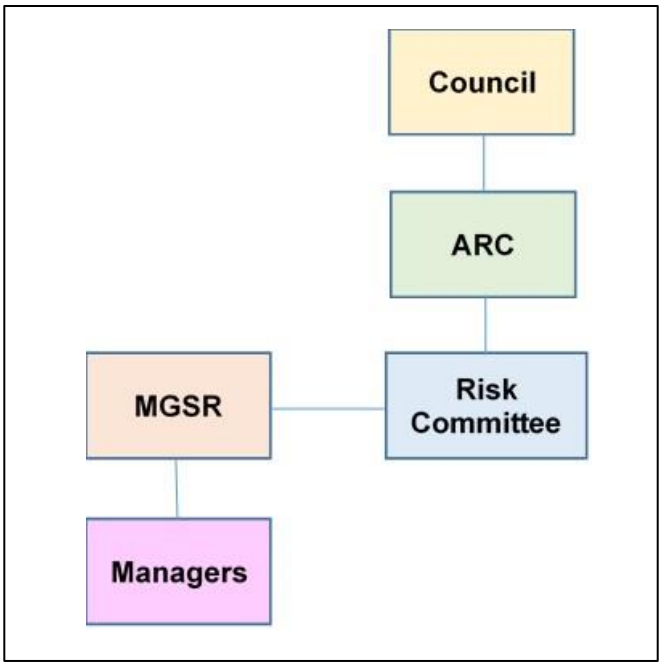

Figure 1 – SoB Risk Governance Arrangements

24. Terms of Reference for each of the Committees provide further detail in relation to roles, responsibilities, and scope of the Committee's activities.

SoB Risk Management Goal, Sub-Goals and Objectives

Goal and sub-goals

25. For the Plan to be effective, there needs to be clear and measurable goals and objectives. As the risk program develops, these objectives can be updated and refined to reflect the more mature risk management culture that exists within SoB.

26. The following is the goal for the SoB risk management framework:

To ensure that the risks facing the organisation are appropriately managed in order to: protect the interests of the organisation and its many stakeholders; assist in the decision-making process; and minimise disruption to critical business functions.

27. This goal is further divided to sub-goals as detailed below:

a. *To maintain a working environment for all employees, contractors and visitors that minimises the risks to their health and safety.*

b. *To ensure that all services provided to the community are safe for use, fit for purpose, and comply with all Legislative and Regulatory requirements.*

c. *To prevent fraud where possible, detect fraud as early as practicable and when discovered, demonstrate a zero tolerance to fraudulent behaviour through appropriate response.*

d. To protect the information, systems and assets that support the operations of SoB.

e. *To ensure organisational resilience through the maintenance of critical business functions during and after disruption related events.*

f. *To ensure that all information provided to critical stakeholders is accurate, complete and provided in a timely manner.*

g. *To ensure all Programs/Projects delivered by SoB are safe and fit for their intended purpose.*

h. *To ensure that SoB's operations do not adversely impact the environment.*

28. The objectives for the program are detailed at **Attachment 4**.

Risk Criteria[1]

Assessing Likelihood of SoB's Enterprise Risks

29. Whether a risk eventuates or not is **not** based on time or frequency – **it is based on the strength of the control environment.** As an example, the likelihood of an unauthorised release of SoB corporate data today, cannot be assessed using statistics and probability, nor can be assessed based on the number of times in the the past. This risk will only materialise today if the controls preventing access to the data are ineffective or non-existent.

30. The only way to determine the likelihood is to determine:

a. Whether controls have been implemented and are being followed; and

b. Whether they are having the desired impact in terms of reducing the risk.

31. To that end, SoB will utilise a likelihood matrix that focusses on the effectiveness of controls. This matrix is at **Attachment 2**.

Assessing the Consequence of SoB's Enterprise Risks

32. The consequence criteria for SoB operational risks are provided at **Attachment 3**. The level of consequence will be assessed against **all** impact categories for each risk and will be recorded in the risk register.

How SoB Determines the Level of Risk

33. SoB will use the following risk matrix when determining the level of an identified risk after assessing the likelihood and consequence:

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

Table 2 – SoB Risk Matrix – Enterprise Risks

How SoB Determines if the Risk is at an Acceptable Level

34. Once a risk has been analysed, decisions need to be taken as to what action, if any, is required. To do this, it is necessary to define the criteria that highlight the actions to be taken.

35. Not all risks that have been assessed at the same level within SoB will have the same level of acceptability. SoB's tolerance for residual risks where the predominant consequence is safety, for example, will not be the same as for residual risks where the highest consequence is financial.

36. A graphical depiction of our willingness to accept risk in the pursuit of our objectives is presented below:

	What is our target level of risk against each impact category?			
Impact Category	Low	Medium	High	Extreme
Reputation		♦		
Financial		♦		
Regulatory Compliance		♦		
Health and Safety	♦			

Table 3 - SoB Risk Target Levels – Enterprise Risks

37. It should be noted that it would not be possible, nor practical, for SoB 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.

38. The table below identifies those with the authority for the acceptance of risks that have exceeded the target level:

	Authority for Acceptance of Residual Risk if it Exceeds the Target Level of Risk			
Impact Category	**Low**	**Medium**	**High**	**Extreme**
Reputation			1 level above Risk Owner	2 levels above Risk Owner
Financial			1 level above Risk Owner	2 levels above Risk Owner
Regulatory Compliance			1 level above Risk Owner	2 levels above Risk Owner
Health and Safety		Risk Owner	1 level above Risk Owner	2 levels above Risk Owner

Table 4 – Authority for Acceptance above Risk Targets

Risk Reporting

39. The Enterprise Risk Report is to be presented to the and Audit and Risk Committee at each meeting and to Council annually. The format for the Enterprise Risk Report is provided at **Attachment 4**.

40. It should be noted that only risks with Severe or Major consequences will be reported to the Audit and Risk Committee and Council.

41. Each report will highlight risks of concern and risks of interest which are defined as follows:

a. **Risks of Concern**. Risks of concern are those risks with Severe or Major consequences where, as a result of the control environment not being to the required level of effectiveness, the Risk Level **exceeds** the specified target level.

b. **Risks of Interest**. Risks can be classified as risks of interest for two reasons:

i. The risk has Severe or Major consequences, however, the level of effectiveness of the control environment has yet to be determined. These risks will be assigned a Likelihood rating of **Possible (TBC)**.

ii. The risk has Severe or Major consequences, however, the level of effectiveness of the control environment is such that the risk is **at or below** the specified target level.

Application of the Risk Management Process within SoB

General

42. The Risk Management process to be followed within SoB is shown in Figure 1 below and is in accordance with the AS/NZS ISO 31000 *Risk Management – Principles and Plan* 2018.

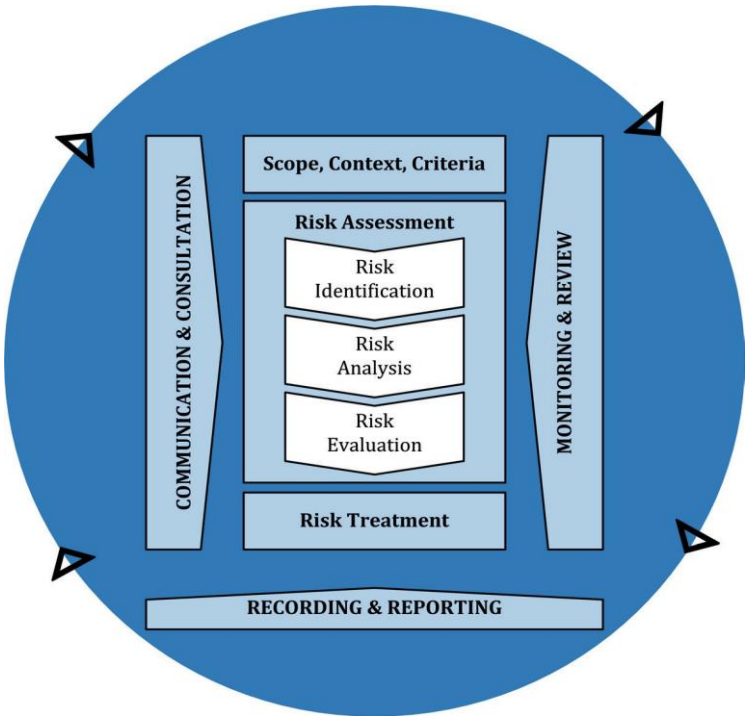

Figure 2 - Risk Management Process

43. SoB's approach to the management of risk will not require multiple risk registers. Instead, SoB will maintain a single central register for enterprise risks.

44. **Our focus in SoB is to gain assurance that the controls aligned to SoB's enterprise risks are effective and, in doing so, the Executive can feel confident that there will be few surprises**.

Shire of Broome Risk Management Focus Areas

Safety

45. Safety has, and always will be, the number one priority for SoB and adherence to these policy statements is one element of the strategy required to reduce workplace incidents within SoB and incidents that may impact the safety of the community.

46. It is critical, therefore, that safety is not only considered during each activity, but that conformance to procedures and processes are being adhered to is part of Council's assurance program.

Fraud

47. As a Council, we will make every effort to implement systems, procedures, and processes that prevent fraudulent and/or corrupt behaviour to the extent possible. Noting, however, that not all fraud and/or corruption can be prevented, SoB will place a significant emphasis on detecting any instances of fraudulent/corrupt behaviour. If/when fraud is identified/suspected, Council will thoroughly investigate and, if it is determined that fraudulent and/or corrupt behaviour has occurred, Council will take the appropriate actions to highlight SOB's zero tolerance for such behaviours.

Environment

48. The Shire of Broome LGA contains some of the most pristine environment in Australia. It is not only critical that SoB ensures that the environment is protected from the actions of 3rd parties, but also that SoB operations do not damage the environmental, cultural, heritage and/or Indigenous values within the Shire.

Information and Physical Security

49. The security of the Shire's information and physical assets is critical. Any unauthorised use of and/or loss of SoB's information resources could have a significant impact on the Shire's reputation. Any loss and/or theft of Council's physical assets could have a significant financial impact and may impact operations.

Compliance

50. Like all organisations, SoB is required to comply with a significant number of Federal and State legislation, codes of practice, regulations, and policies. Any non-compliance with these requirements can have a significant impact on SoB and may lead to fines against the Shire and/or prosecutions against individuals. It is critical, therefore, that SoB maintains a significant focus on maintaining compliance.

Disruption Related Risks (Business Continuity)

51. There are a number of critical business functions within SoB that, if they were to be disrupted, would have a significant impact on the reputation of the Shire and, in some cases, may impact on the health and safety of the community. It is critical, therefore, that advanced plans of action are developed to restore any service disruption as soon as possible.

52. The Business Impact Analysis for SoB is provided at **Attachment 5**.

Risk Identification

53. SoB has identified its enterprise risks which are provided at **Attachment 6**. Further detail is captured in the risk register.

54. It should be noted that new risks will only be added to the risk register once endorsed by the Risk Management Committee and approved by the CEO.

Risk Analysis

55. The risk level for SoB's risks is determined by combining the assessments of likelihood and consequence.

56. Consequences for each risk are to be assessed against **all** impact categories. It is not practical to give the risk multiple consequence ratings, therefore, the highest consequence rating against the impact categories is to be used.

57. The likelihood will be determined by the Risk Owner taking into consideration the level of effectiveness of the controls linked to the risk causes. Emphasis will be placed on the effectiveness of the critical controls.

58. Changes to the level of any risk within SoB can only be authorised by the CEO on the recommendation of the Risk Management Committee.

59. Any changes to risk level for risks with Major or Severe consequences are to be communicated to the Audit and Risk Committee "out of session".

Controls

General

60. Controls are those policies, processes and systems that have been designed and implemented over time to reduce the likelihood and/or consequence of risk. None of the identified risks are new or unique and there are already controls in place to manage them.

61. Up until this point, there has been a level of assumption that the controls are working appropriately to manage the associated risks, however, the focus of the risk management program moving forward is to gain **assurance** that they are effective, particularly those controls identified as critical.

62. At SoB, we want to avoid being in a position of identifying a control was not effective, either through implementation or design, **after** an incident has occurred. Our focus is to identify those control gaps as part of the risk management process, not during a post-event analysis.

Control Ownership

63. Each control is to have a control owner. Ownership of the control is to be reflected in the corresponding position description.

Control Categorisation

64. Not all controls within SoB require the same level of assurance or oversight. To that end, controls are to be categorised based on two considerations:

a. Consequence of the risk; and

b. Criticality of the control in relation to that risk.

65. Through categorisation, SoB will be able to apply proportionality to the implementation and assurance of the control environment.

66. The controls that are linked to the highest consequence risks will be identified in the first instance. This provides us with an initial list of key controls that then need to be assessed for criticality.

67. It needs to be recognised, however, that not all of the controls associated with risks with the highest consequence will have the same impact in terms of reducing/maintaining the level of the risk. If we treat all of the controls associated with high consequence risks the same, we may commit more resources than are necessary to the assurance function. To that end, assigning criticality to each of the controls will assist in prioritising our audit/assurance program.

68. To do this, each control is to be rated for criticality against the table below:

Criticality	Descriptor
5	The control is absolutely critical to the management and reduction of the risk. If this control is ineffective or partially effective, the likelihood and/or consequence of the risk will increase significantly (i.e. increases likelihood or consequnece by 3 or more levels)
4	The control is very important to the management and reduction of the risk. If this control is ineffective or partially effective, the likelihood and/or consequence of the risk will increase (i.e. increases likelihood or consequnece by 2 levels)
3	The control is important to the management and reduction of the risk. If this control is ineffective or partially effective, the likelihood and/or consequence of the risk will increase (i.e. increases likelihood or consequnece by 1 level)
2	The control has some impact on the management and reduction of the risk. Depending on the criticality of the other controls, an analysis should be undertaken to determine the necessity of this control.
1	The control has little to no impact on the management and reduction of the risk. It is unlikely this control is required.

Table 5 – Control Criticality Ratings

69. It should be noted that the criticality of the control is assessed individually against each risk the control is linked to. To that end, the same control may be rated Criticality 5 against one risk and Criticality 3 against another.

70. Once these activities have been completed, the following matrix is used to determine the category of each control:

	Criticality				
Consequence	**1**	**2**	**3**	**4**	**5**
Severe	**Category 3**	**Category 3**	**Category 2**	**Category 1**	**Category 1**
Major	**Category 3**	**Category 3**	**Category 2**	**Category 2**	**Category 1**
Moderate	**Category 4**	**Category 4**	**Category 3**	**Category 3**	**Category 2**
Minor	**Category 4**	**Category 4**	**Category 4**	**Category 3**	**Category 3**
Insignificant	**Category 4**	**Category 4**	**Category 4**	**Category 4**	**Category 4**

Table 6 – Control Categorisation Matrix

71. The category of the control will determine the level of assurance required, however, in general terms **Category 1** and **Category 2** controls will be subject to internal audit/assurance with **Category 1** controls also being subject to external audit/assurance where appropriate.

72. **Category 3** and **Category 4** controls, for the most part, will only require control self-assessment by the control owner.

Measuring Control Effectiveness

73. Once categorised, controls will be measured for effectiveness. The following table details the effectiveness ratings for existing controls:

Effective	No control gaps. The control is influencing the risk level and only continued monitoring is needed
Mostly Effective	Few control gaps. The control is influencing the risk level, however, improvement is needed
Partially Effective	Some control gaps that result in the control having limited influence on risk level
Not Effective	Significant control gaps that result in the control not influencing risk level

Table 7 – Effectiveness of Control Measures

74. To rate the effectiveness of the control, performance measures will be developed for each control. The controls will be tested against these performance measures with **evidence** gathered. This will provide the Executive with a level of confidence that a control that has been assessed as effective is effective.

75. In addition, indicators will be developed that provide specific guidance as to what is considered effective, mostly effective. etc. A simple example is shown below for Fraud Awareness Training:

Control	Performance Measure
Fraud Awareness Training	% of SoB staff that have completed mandatory fraud awareness training within specified timeframes

Effectiveness	Performance
Effective	100% % of SoB staff have completed mandatory fraud awareness training within specified timeframes
Mostly Effective	80-99% of SoB staff have completed mandatory fraud awareness training within specified timeframes
Partially Effective	50-79% of SoB staff have completed mandatory fraud awareness training within specified timeframes
Not Effective	<50% of SoB staff have completed mandatory fraud awareness training within specified timeframes

Table 8 – Control Performance Measures and Effectiveness Rating System

Risk Evaluation

76. The purpose of Risk Evaluation is to determine whether a risk requires further treatment. To do this, the risk level is compared with the Target Level of Risk Matrix previously highlighted.

77. 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, or a conscious decision is taken to accept the risk above the target level. These circumstances are detailed in the risk treatment section below.

Risk Treatment

General

78. Once the effectiveness of the existing control environment is known, it is likely that very few risks will require additional. The purpose of risk treatment, therefore, is to improve and/or enhance the control environment. Treatments will fall into two categories:

a. Short term treatment actions to improve a current control that has been found to be deficient in either its design and/or implementation.

b. Development and implementation of new controls.

79. Where it is determined that additional treatment is required, there are a range of treatment strategies to be considered. These are detailed below.

Treatment Options

Avoid

80. 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 SoB where this treatment strategy will be an option.

Mitigate

81. The purpose of mitigation is to improve and/or add to the current controls aligned to the causes and/or consequences of the risk.

82. 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. This requires that all treatments are to be reflected not only in the risk register, but also as a line item in the SoB Corporate Plan.

83. In addition, to ensure accountability within SoB, all risk treatments are to have an owner assigned.

84. Upon completion of the risk treatments, the Risk Register is to be updated to reflect completion of the treatment and the risk level is to be reassessed as to whether these actions have been successful in reducing the likelihood and/or consequence.

Share

85. Risk sharing 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 risk sharing include contracting and insurance.

86. The overarching tenet in relation to risk sharing is that if SoB owns the function it still owns the risk. **Accountability cannot be transferred to another party**.

Accept/Retain

87. Risks are accepted or retained for a number of reasons:

a. There are no treatment options available (i.e. the risk event is outside SoB's sphere of influence);

b. The level of the risk meets the stated target for that type of risk;

c. The level of the risk is above the target level, however, an informed decision is taken to accept the risk at that level; or

d. Risk treatment would cost more than the consequences of the risk (but not just in dollar terms).

88. Where a decision is taken to accept a risk that is above the target level, the reasons behind that decision are to be recorded in the risk register.

Monitor and Review

General

89. 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**.

90. There are four categories of control monitoring within SoB as described below.

Manage intensively

91. As the name suggests, these are the controls that require the greatest scrutiny and ongoing surveillance. If these risks were to materialise the consequences to the organisation would be significant (and in some cases devastating). These are the **Category 1** controls.

Manage Closely

92. This is the next highest category of control monitoring. Whilst the consequences, if the risks that these controls are linked to were to materialise are not as devastating of those in the previous category, they will still be of a level where senior management will be aware that the event has occurred. These are the **Category 2** controls.

Watch and Act

93. These controls are linked to risks with lesser consequences and/or have a lower level of criticality and, therefore, require less scrutiny. These are the **Category 3** controls.

Acknowledge

94. These are the **Category 4** controls within the organisation and require little to no monitoring.

Monitor Frequency

95. The table below provides guidance as to the frequency of monitoring for each category. Understanding that some may require higher levels of frequency:

Control Category	Control Self-Assessment	Assurance by Internal Audit	External Audit of Control
Category 1	Monthly	Quarterly	Annually
Category 2	Quarterly	Every 6 months	
Category 3	Annually		
Category 4	Annually		

Table 9 – Frequency of Control Monitoring

Review

96. The review process includes reviews of the risk management program (maturity assessment) as well as review (deep dives) of selected risks.

97. A maturity assessment of the risk management program is to be performed at least every three years by an independent 3rd party provider.

98. Deep dives on all Severe Consequence risks are to occur annually and are to be conducted by the Risk Committee and reported to the Audit and Risk Committee.

99. Third party audits of controls will be planned as a transparent part of the risk management assurance system.

List of Attachments

1. Glossary of Terms
2. SOB Likelihood Matrix
3. SoB Consequence Matrix
4. Format of Enterprise Risk Report
5. SoB Business Impact Analysis
6. SoB Operational Risks

ATTACHMENT 1

GLOSSARY OF TERMS

Consequences	Outcome of an event affecting objectives (AS/NZS ISO 31000 - 2018).
Control	Measure that is modifying risk (AS/NZS ISO 31000 - 2018).
Likelihood	Chance of something happening (AS/NZS ISO 31000 - 2018)
Residual Risk	Risk remaining after risk treatment (AS/NZS ISO 31000 - 2018)
Risk	A possible event/incident/issue that, **if it occurs**, will have an impact on objectives
Issue/Incident	An event that has occurred that has taken SoB outside its tolerances/risk appetite
Risk Acceptance	An informed decision to accept the consequences and the likelihood of a particular risk.
Risk Analysis	A process to comprehend the nature of risk and to determine the level of risk (AS/NZS ISO 31000 - 2018).
Risk Avoidance	An informed decision to withdraw from, or to not become involved in, a risk situation.
Risk Identification	Process of finding, recognising and describing risks (AS/NZS ISO 31000 - 2018)
Risk Register	A Risk Register provides a repository for recording each risk and its attributes, evaluation and treatments.
Risk Source	Element which alone or in combination has the intrinsic potential to give rise to risk (AS/NZS ISO 31000 - 2018).
Risk Management	A systematic process that enables organisations to make informed decisions as to the actions to be taken in relation to the possible events/issues/incidents that, if they occur will impact on their objectives
Risk Owner	Person or entity with the accountability and authority to manage a risk (AS/NZS ISO 31000 - 2018).
Risk Sharing	Sharing with another party, the burden of loss or benefit of gain, for a risk. (AS/NZS 4360:2004)
Risk Treatment	Process to modify risk (AS/NZS ISO 31000 - 2018).
Stakeholder	Person or organisation that can affect, be affected by, or perceive themselves to be affected by, a decision or activity. (AS/NZS ISO 31000 - 2018)

ATTACHMENT 2

SoB LIKELIHOOD CRITERIA – ENTERPRISE RISKS

Ratings	Descriptors
Almost Certain	**For Risks with Category 1 and 2 Controls** Less than 30% of the **Category 1** and **Category 2** controls associated with the risk are rated as **Effective** or **Mostly Effective**. Without control improvement, there is almost no doubt the risk will materialise and become an incident. **For Risks without Category 1 or 2 Controls** Less than 10% of the controls associated with the risk are rated as **Effective** or **Mostly Effective**. Without control improvement, there is almost no doubt the risk will materialise and become an incident.
Likely	**For Risks with Category 1 and 2 Controls** Only 30%-50% of the **Category 1** and **Category 2** controls associated with the risk are rated as **Effective** or **Mostly Effective**. Without control improvement, it is more likely than not that the risk will materialise and become an incident. **For Risks without Category 1 or 2 Controls** 10%-30% of the controls associated with the risk are rated as **Effective** or **Mostly Effective**. Without control improvement, it is more likely than not that the risk will materialise and become an incident.
Possible	**For Risks with Category 1 and 2 Controls** 50%-70% of the **Category 1** and **Category 2** controls associated with the risk are rated as **Effective** or **Mostly Effective**. Without control improvement, the risk may materialise and become an incident. **For Risks without Category 1 or 2 Controls** 30%-60% of the controls associated with the risk are rated as **Effective** or **Mostly Effective**. Without control improvement, the risk may materialise and become an incident.
Unlikely	**For Risks with Category 1 and 2 Controls** 70%-90% of the **Category 1** and **Category 2** controls associated with the risk are rated as **Effective** or **Mostly Effective**. The strength of this control environment is such that, if this risk was to materialise and become an incident, it is more likely due to external factors (known or unknown to the organisation) than through the ineffectiveness of the control environment. **For Risks without Category 1 or 2 Controls** 60%-80% of the controls associated with the risk are rated as **Effective** or **Mostly Effective**. Without control improvement, it is more likely than not that the risk will materialise and become an incident.
Rare	**For Risks with Category 1 and 2 Controls** Greater than 90% of the **Category 1** and **Category 2** controls associated with the risk are rated as **Effective** or **Mostly Effective**. The strength of this control environment is such that, if this risk was to materialise and become an incident, it is more likely due to external factors (known or unknown to the organisation) than through the ineffectiveness of the control environment. **For Risks without Category 1 or 2 Controls** Greater than 80% of the controls associated with the risk are rated as **Effective** or **Mostly Effective**. The strength of this control environment is such that, if this risk was to materialise and become an incident, it is more likely due to external factors (known or unknown to the organisation) than through the ineffectiveness of the control environment.

ATTACHMENT 3

SOB CONSEQUENCE MATRIX

Rating	Reputation	Financial	Compliance	Health and Safety
Severe	**If this risk was to eventuate (i.e. become an event/incident) it could result in:** • Greater than **50%** of media stories are negative for a period of **30** days or more; and/or • Exit surveys show a dissatisfaction rate within the organisation of >**50%**	**If this risk was to eventuate (i.e. become an event/incident) it could result in:** • A financial impact to SoB exceeding **$4,000,000**	**If this risk was to eventuate (i.e. become an event/incident) it could result in:** • An officer of SoB facing criminal prosecution or the maximum level of fines able to be imposed by a Regulator on an individual; and/or • SoB receiving a judgement where the fine imposed is the maximum that can be issued by the Regulator and/or • SoB receives an enforceable undertaking from the regulator	**If this risk was to eventuate (i.e. become an event/incident) it could result in:** • Multiple deaths or permanent disability of personnel under the control of SoB where SoB is found to be primarily responsible and/or • Multiple deaths or permanent disability of a member of the public as a result of an incident where SoB is found to be at fault, or to have contributed
Major	**If this risk was to eventuate (i.e. become an event/incident) it could result in:** • Greater than **50%** of media stories are negative for a period of up to **30** days. • Exit surveys show a **30-50%** dissatisfaction rate within the organisation	**If this risk was to eventuate (i.e. become an event/incident) it could result in:** • A financial impact to SoB of **$2,000,001 - $4,000,000**	**If this risk was to eventuate (i.e. become an event/incident) it could result in:** • An officer of SoB receiving a fine that is 50% or more of the maximum that can be issued by a regulator • SoB receiving a judgement where the fine imposed is 50% or more that can be issued by the Regulator	**If this risk was to eventuate (i.e. become an event/incident) it could result in:** • One death and/or multiple permanent disability of personnel under the control of SoB where SoB is found to be primarily responsible • One death and/or multiple permanent disability of a member of the public as a result of an incident where SoB is found to be at fault, or to have contributed.
Moderate	**If this risk was to eventuate (i.e. become an event/incident) it could result in:** • **20-50%** of media stories are negative for a period of up to 7 days • Exit surveys show a **15-30%** dissatisfaction rate within the organisation	**If this risk was to eventuate (i.e. become an event/incident) it could result in:** • A financial impact to SoB of **$250,001 - $2,000,000**	**If this risk was to eventuate (i.e. become an event/incident) it could result in:** • An officer of SoB receiving a fine that is 10-50% of the maximum that can be issued by a regulator • SoB receiving a judgement where the fine imposed is 10-50% of that which can be issued by the Regulator	**If this risk was to eventuate (i.e. become an event/incident) it could result in:** • One permanent disability of personnel under the control of SoB where SoB is found to be primarily responsible: and or • Hospitalisation of multiple personnel under the control of SoB where their injuries will impact them for a period of six months or more where SoB is found to be primarily responsible; and/or • One permanent disability of a member of the public as a result of an incident where SoB is found to be at fault, or to have contributed; and/or • Hospitalisation of multiple members of the public as a result of an incident where SoB is found to be at fault, or to have contributed
Minor	**If this risk was to eventuate (i.e. become an event/incident) it could result in:** • **10-20%** of media stories are negative for a period of up to 7 days • Community satisfaction with SoB Exit surveys show a **5-15%** dissatisfaction rate within the organisation	**If this risk was to eventuate (i.e. become an event/incident) it could result in:** • A financial impact to SoB of **$10,001 - $250,000**	**If this risk was to eventuate (i.e. become an event/incident) it could result in:** • SoB receiving a judgement where the fine imposed is less than 10% of that which can be issued by the Regulator	**If this risk was to eventuate (i.e. become an event/incident) it could result in:** • Injuries or illness to personnel under the control of SoB requiring medical attention with no long-term effects • Injuries or illness to members of the public requiring medical attention with no long-term effects as a result of an incident where SoB is found to be at fault, or to have contributed
Insignificant	**If this risk was to eventuate (i.e. become an event/incident) it could result in:** • Less than **10%** of media stories are negative for a period of up to 7 days • Exit surveys show a dissatisfaction rate within the organisation of **<5%**	**If this risk was to eventuate (i.e. become an event/incident) it could result in:** • A financial impact to SoB less than **$10,000**	**If this risk was to eventuate (i.e. become an event/incident) it could result in:** • SoB receives a judgement where the total cost of legal action, fines and remediation of the issue is less than $10k	**If this risk was to eventuate (i.e. become an event/incident) it could result in:** • Injuries or illness to personnel under the control of SoB requiring no more than treatment at the scene • Injuries or illness to member/s of the public requiring no more than treatment at the scene as a result of an incident where SoB is found to be at fault, or to have contributed

ATTACHMENT 4

ENTERPRISE RISK REPORT FORMAT

SoB RISK REPORT

Recommendations

- It is recommended that you:

  (a) ***note*** the current level of SoB Enterprise Risks;

  (b) ***note*** the escalation of risk CR X-Y to a risk of concern and **endorse** the actions that are being taken to address the risk;

  (c) ***endorse*** the downgrading of risk CR I-J and CR K-L to risks of interest; and

  (d) ***note*** the status of the remaining SoB risks of interest.

Introduction

1. The following is the Enterprise Risk Report for the period xxx to xxx.

2. The following risks have been **added** as Risks of Concern since the last reporting period:

   a. X

   b. X

3. The reasons for the escalation of these risks are detailed within the report.

4. The following risks have been **downgraded** as Risks of Concern to Risks of Interest since the last reporting period:

   a. X

   b. X

5. The reasons for the downgrading of these risks are detailed within the report.

Summary

6. The following is a summary of the Enterprise Risks for SoB:

		Likelihood Level	Consequence Level	Risk Level
PR 1	**Unauthorised release of, amendment to, use of, and/or loss of access to corporate/confidential information**			
PR 2	**Incorrect, incomplete, or untimely information provided to a stakeholder**			

		Likelihood Level	Consequence Level	Risk Level
PR 3	**Disruption to critical business function for a period in excess of specified Maximum Acceptable Outage (MAO)**			
PR 4	**Fraudulent/corrupt behaviour by a member of staff and/or 3rd party**			
PR 5	**Incident occurs that threatens the health, safety and/or wellbeing of staff**			
PR 6	**Incident occurs that threatens the health, safety and/or welfare of the public**			
PR 7	**At fault/avoidable/contributory Incident occurs that threatens the environment**			
PR8	**Shire of Broome delivers a project/program (including investment decisions) that is not fit for purpose or of poor quality**			
PR9	**At fault/avoidable/contributory incident occurs at Shire of Broome operated leisure facility (including jetty)**			
PR10	**Incident occurs at Shire of Broome cemetery**			

7. A summary of the Parent Risks the risk levels for the underlying Child Risks is provided at **Attachment 1** to this report.

Risks Escalated to Risks of Concern

1. **CR X-Y** has been escalated to a risk of concern due to the fact that.

2. **Actions**. The following actions are being taken to reduce the risk to an acceptable level:

   a. xxxxxx

   b. xxxxx

3. **The Audit and Risk Committee will be informed of progress**.

Risks Downgraded to Risks of Interest

4. **CR I-J** has been downgraded to a risk of interest due to the fact that……..

5. **CR K-L** has been downgraded to a risk of interest due to the fact that……..

Additional Risks of Interest

6. The following is the current status of all other SoB risks of interest:

   a. **CR A-B**:

   b. **CR C-D**:

   c. **CR E-F**:

   d. **CR G-H**:

Update on previous actions

Meeting Date	Action	Accountable	Progress + Comment
XXXX	XXXXX	XXXX	Completed. To be removed from next report

List of ineffective Cat 1 and Cat 2 controls

The following is the list of Cat 1 and Cat 2 controls that have been assessed as ineffective:

Control #	Control	Level of Effectiveness	Actions to be taken	Due Date

Report Prepared by:

Report Authorised by:

ATTACHMENT 4

STATUS OF SOB CHILD RISKS

Parent Risks		Risk Level Child Risks																														
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
PR1	Unauthorised release of, amendment to, use of, loss of, and/or loss of access to corporate/confidential information			■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
PR2	Incorrect, incomplete or untimely information provided to a critical stakeholder								■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
PR3	Disruption to critical business function for a period in excess of specified Maximum Acceptable Outage (MAO)			■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
PR4	Fraudulent/corrupt behaviour by a member of staff and/or 3rd party													■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
PR5	Incident occurs that threatens the health, safety and/or wellbeing of staff																																
PR6	Incident occurs that threatens the health, safety and/or welfare of the public																		■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
PR7	At fault/avoidable/contributory Incident occurs that threatens the environment									■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
PR8	SoB delivers a project/program (including investment decisions) that is not fit for purpose or of poor quality						■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
PR9	At fault/avoidable/contributory incident occurs at Shire of Broome operated leisure facility (including jetty)						■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
PR10	Incident occurs at Shire of Broome cemetery					■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■

ATTACHMENT 5

SHIRE OF BROOME BUSINESS IMPACT ANALYSIS

To be Developed

ATTACHMENT 9

SOB ENTERPRISE RISKS

PR1	**Unauthorised release of, amendment to, use of, loss of, and/or loss of access to corporate/confidential information**
CR1.1	Unauthorised release of, amendment to, use of, loss of, and/or loss of access to corporate/confidential information stored electronically
CR1.2	Unauthorised release of, amendment to, use of, loss of, and/or loss of access to corporate/confidential information stored in hard copy
PR2	**Incorrect, incomplete or untimely information provided to a stakeholder**
CR2.1	Reportable WHS incident not reported or reported outside of specified timeframes
CR2.2	Incorrect/incomplete/false information provided to external bodies (accreditation/auditing/funding etc.)
CR2.3	Discovery of systemic/historical issuing of incorrect rates notices to residents
CR2.4	Shire of Broome makes an "incorrect" determination in relation to an application
CR2.5	Staff member makes statements and/or posts on-line information that is in error, incomplete and/or prejudicial
CR2.6	Elected member makes statements and/or posts on-line information that is in error, incomplete and/or prejudicial
CR2.7	Inaccurate, incomplete, untimely or conflicting information provided to stakeholders/community during an emergency situation
PR3	**Disruption to critical business function for a period in excess of specified Maximum Acceptable Outage (MAO)**
CR3.1	Disruption to collection and disposal of putrescible waste for a period in excess of 72 hours
CR3.2	Disruption to response to Municipal Emergency Management incidents for a period in excess of 24 hours
PR4	**Fraudulent/corrupt behaviour by a member of staff and/or 3rd party**
CR4.1	Fraudulent/corrupt behaviour by a member of staff involved in procurement activities (up until the point of contract)
CR4.2	Fraudulent/corrupt behaviour by a member of staff involved in management of contracts/service agreements (e.g. not declaring the hiring of family/friends - conflict of interest)
CR4.3	Fraudulent/corrupt behaviour by a member of staff involved in accounts payable. receivable and/or payroll
CR4.4	Theft or inappropriate disposal of Shire of Broome assets by staff member
CR4.5	Member of staff receives benefits to which they are not entitled (e.g. leave, inappropriate use of credit card. etc)

CR4.6	Contractor/SLA supplier/3rd party (including phishing attack) paid for services not delivered or of poor quality
CR4.7	Theft of and/or wilful damage to Shire of Broome equipment/supplies/infrastructure by 3rd party/s
CR4.8	Unauthorised expenditure from cash reserve accounts
CR4.9	Member of Shire of Broome staff accept benefits for approvals
CR4.10	Fraudulent/corrupt behaviour by elected official (e.g. accepting benefits for approvals, inappropriate/illegal use of Shire of Broome resources, undue influence on staff)
CR4.11	Unauthorised personal use of Shire of Broome equipment/vehicles/assets by a member of staff
CR4.13	Fraudulent/corrupt behaviour by a member of staff involved in allocation of grant funding
CR4.14	Grant recipient utilises grant funding for purposes outside of the scope of the grant agreement
PR5	**Incident occurs that threatens the health, safety and/or wellbeing of staff**
CR5.1	Assault of a member of staff by a member of the public whilst conducting operations
CR5.2	Worker falls from height
CR5.3	Worker contacts or is contacted by live electrical source
CR5.4	Rollover of plant during operations
CR5.5	Worker contacted by and/or becomes entangled in plant/equipment whilst operating (includes debris generated by the moving plant/equipment)
CR5.6	Member of staff struck by moving vehicle/missile thrown from vehicle whilst conducting roadside operations
CR5.7	Unplanned/unintended fall into body of water whilst conducting operations
CR5.8	Trench/confined space collapse during operations
CR5.9	Worker exposed to, and/or contacted by, toxic/hazardous substance whilst conducting operations
CR5.10	Worker exposed to particulate matter (including unbonded/friable asbestos, silica dust, dust) whilst conducting operations
CR5.11	Worker bitten and/or stung whilst conducting operations
CR5.12	Worker exposed to the elements for an inappropriate length of time whilst conducting operations
CR5.13	Worker involved in a vehicle accident whilst conducting operations

CR5.14	Worker lifts weight or undertakes manual activity that exceeds the limit of their biomechanical capacity
CR5.15	At fault worker slip, trip or fall in the workplace or Shire of Broome property or facility
CR5.16	Worker exposed to short or long-term noise, above legislated/recommended levels during operations
CR5.17	Worker suffers bullying, harassment, discrimination (BHD), and/or assault by another staff member, and/or stressful working conditions within Shire of Broome
CR5.18	Loss of containment of energy under pressure whilst conducting operations (includes tire exploding whilst being inflated, burst of hydraulic line, penetration of gas line, puncture of container at waste facility. Etc.)
CR5.19	At fault/avoidable contact with underground services whilst conducting operations
CR5.20	Worker struck by falling object or strikes object (falling, stationary or moving) other than plant/vehicles/machinery
CR5.21	Worker contacts or is contacted by sharp object whilst conducting operations (includes syringes, broken bottles, sharp surfaces. Etc.)
CR5.22	Shire of Broome fails to identify/respond appropriately and/or provide suitable assistance to worker/s exposed to short term or long-term psychologically harmful events/environment/s
CR5.23	Systemic incorrect payment of wages/entitlements to staff discovered within Shire of Broome
CR5.24	Inappropriate response by Shire of Broome to an identified incident/issue (e.g. BHD, discovery of fraud, assault, whistleblower complaint, safety related issue. Etc.)
CR5.25	Worker exposed to infectious disease/pathogen (e.g. COVID-19) whilst conducting operations
CR5.26	Worker falls from vehicle whilst in motion
CR5.27	Incident occurs whilst worker working alone remotely
CR5.28	Worker or body part of worker becomes lodged/caught between two solid surfaces whilst conducting operations
CR5.29	Inappropriate response to an emergency situation within Shire of Broome facility/ies (e.g. fire, active shooter, bomb-threat)
CR5.30	Preventable fire in Shire facilities
CR5.31	Worker contacts, or is contacted by hot surfaces, materials and/or liquids whilst conducting operations
CR5.32	Worker struck by lightning whilst conducting Shire operations

PR6	**Incident occurs that threatens the health, safety and/or welfare of the public**
CR6.1	At fault trip, slip or fall by a member of the public at/in/on Shire of Broome owned and operated facilities
CR6.2	Council contributes through act and/or omission to an incident at/on Broome owned infrastructure/facilities used by the public (e.g. roads, footpaths, jetty, boat ramp. etc).

CR6.3	Contaminated food consumed at a Shire of Broome run facility or an event run by the Shire of Broome
CR6.4	At fault/avoidable/contributory incident occurs at Shire of Broome run/sponsored community event
CR6.5	Member of the public exposed to infectious disease/pathogen (e.g. COVID-19/Legionnaires) within Shire of Broome facility
CR6.6	At fault/avoidable/contributory incident at a Shire of Broome approved 3rd party run event
CR6.7	At fault accident involving Shire of Broome vehicle/plant (including items falling from Shire of Broome operated vehicles as well as "missiles" from plant/equipment)
CR6.8	Member of the public exposed to particulate matter (including unbonded/friable asbestos, silica dust, dust) whilst in Shire of Broome facilities
CR6.9	Member of the public contacts or is contacted by a live electrical source at a Shire of Broome owned/operated facility
CR6.10	Inappropriate/culturally insensitive behaviour by a Shire of Broome staff member/volunteer at a Shire of Broome operated facility and/or event or within a program provided by Shire of Broome
CR6.11	At fault/avoidable/contributory collapse/structural failure of Shire of Broome approved installations - permanent or temporary (e.g. art pieces/signage)
CR6.12	At fault/avoidable/contributory collapse/structural failure of Shire of Broome facilities/amenities used by the public (e.g. civic centre, library, BRAC, jetty. etc)
CR6.13	At fault/avoidable/contributory collapse/structural failure of Shire of Broome facilities leased to 3rd parties
CR6.14	Object belonging to, or for which Shire of Broome is responsible (e.g. tree branch) falls from height as a result of Shire of Broome operations, activities, and/or failure to act upon reported hazards
CR6.15	Member/s of the public exposed to toxic/hazardous substance as a result of Council operations
CR6.16	Inappropriate/culturally insensitive behaviour by an elected member at a Shire of Broome event
CR6.17	Shire contributes to member of the public being struck by lightning whilst using a Shire facility (e.g. pool not closing during storm event)
PR7	**At fault/avoidable/contributory Incident occurs that threatens the environment**
CR7.1	Loss of containment of a bushfire during, or as a result of, Shire of Broome operations
CR7.2	At fault/preventable overflow of storm water
CR7.3	Loss of containment of toxic/hazardous substance from stored location or whilst being transported
CR7.4	At fault ignition of flammable/explosive material being stored or transported
CR7.5	Items of environmental/cultural/Indigenous significance impacted/destroyed during, or as a result of, Shire of Broome operations
CR7.6	Shire of Broome introduces, releases, or fails to prevent the spread of exotic/noxious flora, fauna or disease

CR7.7	Shire of Broome operations further exacerbate existing contamination
CR7.8	At fault/contributory fire at waste management facility
PR8	**Shire of Broome delivers a project/program (including investment decisions) that is not fit for purpose or of poor quality**
CR8.1	Shire of Broome delivers a construction that is not fit for purpose or of poor quality
CR8.2	Shire of Broome delivers an IT project that is not fit for purpose or of poor quality
CR8.3	Shire of Broome delivers new equipment and/or equipment replacement project that is unsafe or not fit for purpose
CR8.4	Shire of Broome delivers a community project/program that is not fit for purpose or of poor quality
CR8.5	Shire of Broome reserves invested outside of policy guidelines
PR9	**At fault/avoidable/contributory incident occurs at Shire of Broome operated leisure facility (including jetty)**
CR9.1	Inappropriate response/delayed response to a member of the public who gets into difficulty in the pool
CR9.2	Members of the public exposed to water borne infection/disease at a Shire run facility
CR9.3	Inappropriate behaviour by a Shire of Broome staff member (incl causals) and/or volunteer at a Shire facility or event
CR9.4	Inappropriate or untimely response by Shire of Broome staff to inappropriate behaviour towards a patron by 3rd party (including other patrons) at a Shire facility
CR9.5	At fault/contributory incident involving member of the public getting into difficulty at Shire of Broome owned jetty
PR10	**Incident occurs at Shire of Broome cemetery**
CR10.1	At fault/contributory damage to cemetery infrastructure (e.g. headstones)
CR10.2	Casket buried in incorrect plot
CR10.3	At fault/contributory incident occurs during digging of gravesites by members of the public
CR10.4	Loss of and/or loss of access to historic cemetery records