



## **Appendix 7a**

### **16.5 Risk Register**


*CP017 Risk Management*

# **Ordinary Meeting of Council**

Wednesday 23 June 2021 at 7:00pm

Via videoconference (Zoom)

## COUNCIL POLICY

Risk Management	<b>Adopted By Council:</b>	20/02/01	
	<b>Date/s Revised:</b>	27/10/04, 17/06/09, 16/12/09, 18/10/11, 30/01/13; 29/04/15; 13/12/18	
	<b>Next Review Date:</b>	12/2024	
	<b>Document No:</b>	CP017	
	<b>Directorate:</b>	Organisational Performance & Community Services	
	<b>Responsible Officer:</b>	Risk Manager	

### 1. PURPOSE AND SCOPE

The purpose of this document is to outline the policy, process and elements of the Borough of Queenscliffe's risk management policy which enables the Borough of Queenscliffe to manage its risks efficiently and effectively. This policy applies to all areas of the Borough of Queenscliffe's operations, and includes risk of financial loss, injury to employees, damage to equipment and property and loss of reputation.

The Borough of Queenscliffe is committed to the management of risk to protect:

- its ratepayers;
- its quality of service;
- its legislative requirements;
- its image and reputation;
- its employees;
- its other stakeholders; and
- its assets.

### 2. PRELIMINARY MATTERS

#### 2.1 STANDARDS

The Borough of Queenscliffe's Risk Management Policy has been developed in accordance with AS NZS ISO 31000-2009 Risk Management – Principles and Guidelines. The Risk Policy is intrinsically linked to the Borough of Queenscliffe's Council Plan and organisational objectives. The accompanying handbook HB 327:2010 – Communicating and consulting about risk is used as a reference guide.

#### 2.3 RISK APPETITE

Risk appetite, at the organisational level, is the amount of risk exposure, or potential adverse impact from an event, that the organisation is willing to accept/retain. Once the risk appetite threshold has been breached, risk management treatments and business controls are implemented to bring the exposure level back within the accepted range. As the Borough of Queenscliffe is a public organisation, the Borough of Queenscliffe generally has low risk appetite. However, in the context of our work, some conflicts and resultant risks are inevitable. Where practicable, measures will be implemented to mitigate risk exposure.

### **3. GUIDELINES**

#### **3.1 APPLICATION OF RISK MANAGEMENT**

The risk management process will apply to the following areas:

- strategic, operational and business planning processes;
- asset management and resource planning;
- management of ethics, fraud, security and probity issues;
- business interruption and continuity management;
- management of significant change issues and projects;
- occupational health and safety risks; and
- financial management.

#### **3.2 OBJECTIVES**

The objectives of the Borough of Queenscliffe's risk management policy are to:

- formally recognise the uncertainties surrounding the Borough of Queenscliffe's ability to achieve its organisational objectives;
- formalise and enhance existing risk management practices;
- demonstrate compliance with relevant legislation and regulatory requirements;
- raise the profile of risk management at all levels of the Borough of Queenscliffe;
- develop and retain a risk register to facilitate the understanding of the Borough of Queenscliffe's risks;
- protect the safety, security and health of staff;
- demonstrate and promote good corporate governance;
- demonstrate the integrity and transparency of its decisions and processes; and
- achieve a proactive rather than a reactive approach to risk management.

#### **3.3 OVERALL APPROACH**

##### **3.3.1 Roles and responsibilities**

An important component of the risk management policy is the structured and disciplined oversight of the overall operations of the organisation, including at the Council and Executive Management Team (EMT) level.

##### **Council**

In the risk management context Council has specific responsibilities for:

- Overseeing the scope, quality and independence of the external audit arrangements;
- Monitoring the internal audit process;
- Monitoring overall legal and regulatory compliance;
- Monitoring the effectiveness of risk management policies and the adequacy of insurance programs; and
- monitoring to ensure that appropriate processes, controls, and sufficient resources are in place to effectively and efficiently manage risk so that strategic and operational objectives can be met.

Councillors also hold the same individual responsibility the Borough officers hold, as detailed further below.

### **Audit and Risk Committee**

The Audit and Risk Committee will monitor management's implementation of the Policy and its risk management performance. The internal auditor will be asked to report progress to the Committee on a regular basis.

### **Executive Management Team (EMT)**

The primary responsibility for risk management rests with the Chief Executive Officer (CEO) and the EMT. The EMT is responsible for identifying, assessing, monitoring, managing and reporting risks within the organisation. It is the responsibility of the EMT to ensure that policies and procedures are in place and to ensure internal controls, skills and systems enable compliance with the policies.

### **Risk Manager**

The Risk Manager is responsible for ensuring that the Risk Register is established, implemented and maintained. The Risk Manager is also responsible for the assignment of responsibilities in relation to risk management, including the responsibility for training in risk management. The Risk Manager also has the following specific responsibilities:

- Investigating, assisting and monitoring Council's insurance register for third party claims;
- Monitoring agreements, leases and contracts with Third Parties ensuring that they have appropriate indemnity/hold harmless and insurance clauses in place to reduce Council's liability;

### **Compliance Committee**

The Compliance Committee reviews risk status, actions and accountabilities arising from the Individual Risk Assessments every second month. Emerging /changing risks in the organisation are discussed and the progress of mitigation plans is reviewed.

The Compliance Committee includes representatives from all business areas at a range levels from Executive to Officer Level. The Compliance Committee is chaired by the Risk Manager. Official minutes from the Compliance meeting are recorded and forwarded to the EMT.

Specific responsibilities include:

- Providing assistance in the control and treatment of risks, until the residual level of risk becomes acceptable;
- Identifying and recording any problems relating to the management of risks;
- Verifying the implementation of solutions;
- Verifying that investigations of incidents and accidents are undertaken to determine the action necessary to prevent a recurrence; and
- Reporting annually to the EMT with respect to its work in the area of risk management.

## **All Borough of Queenscliffe Personnel**

All Councillors, managers, committee members and staff members are responsible for managing the risks in their activities and in the workplace. Staff are trained on key risks in their business areas.

### **Documenting roles and responsibilities**

Risk Management is included in the position descriptions of all EMT and Program Leaders at the Borough of Queenscliffe. Risk Management is also included in the following documents:

- The Borough of Queenscliffe Code of Conduct; and
- Audit and Risk Committee Terms Of Reference

### **Assurance**

Assurance as to the efficiency and effectiveness of the Borough of Queenscliffe Risk Management Policy, processes and controls is provided through two areas. First, assurance is provided by management through regular Risk Management reporting and management forums, including reporting to Council. Second, assurance also comes from the independent testing, review and reporting undertaken by the external and internal audit functions.

The frequency and scope of audits is assessed and increased if weaknesses and significant issues are discovered or if significant changes have been made to business activities or business processes.

### **3.3.2 People and Culture**

Having the right people and promoting an appropriate risk culture are critical to a successful risk management Policy. Ensuring that an effective structure exists in relation to the competency, training, reward and recognition for all employees is a fundamental component of the risk management process. The Borough of Queenscliffe is committed to fostering a culture of risk.

## **3.4 ELEMENTS OF RISK MANAGEMENT POLICY**

### **3.4.1 Individual Risk Assessments**

Individual Risk Assessments incorporate risk identification, assessment, mitigations and residual risk. They present details on control effectiveness and mitigation plan status and record how the Borough of Queenscliffe assures the controls are effective. The Risk Manager is responsible for ensuring that the Individual Risk Assessments are reviewed and maintained and also for the assignment of responsibilities in relation to the risks. The Individual Risk Assessment is updated or raised immediately a risk event occurs or a potential risk event is identified. Mitigating controls and allocated responsibilities are recorded against each risk.

The 'risk rating' table combines the likelihood of the occurrence and the potential consequences of the risk to establish a 'risk rating' as follows:

- low
- moderate
- high

For each potential risk, the Borough of Queenscliffe notes the actions it currently takes to mitigate the risk. The Borough of Queenscliffe also identifies any additional action required to

deal with the risk, and determines a residual risk rating. These actions are monitored by the Compliance Committee. A sample Individual Risk Assessment is attached as Appendix A.

### **3.4.2 The Risk Register**

The Risk Register is the accumulated Individual Risk Assessments.

### **3.4.3 Policies and Procedures**

Borough of Queenscliffe has in place accounting policies that define and establish criteria for the recording of assets, liabilities, revenue and expenses. Borough of Queenscliffe also has policies that document and provide guidance in relation to particular business activities, legal requirements and risk matters.

Relevant policies are communicated and made available to all staff. Where new policies are introduced or changes are made to existing policies, information or training sessions are held to communicate and educate employees.

### **3.4.4 Internal Controls**

As part of its Risk Management Policy the Borough of Queenscliffe has documented the controls in place within each major business process and financial information flow. This documentation is updated for changes in processes as required. The controls are subject to testing via the internal audit assurance process, however any weakness or breakdown in controls is addressed with management when identified. The outcomes of control testing are reported independently to Council. In addition, the financial software in place has built in controls that ensure rigorous processes and appropriate delegations are applied to financial transactions.

### **3.4.5 Business Continuity Planning**

The nature of the Borough of Queenscliffe business requires the ability to provide rapid recovery of key services in the event of business disruptions. The Borough of Queenscliffe has a documented Business Continuity Plan and has an IT Disaster Recovery Plan in place, including access to a back up recovery site.

Testing of Borough of Queenscliffe's ability to resume critical operations after a major disruption is tested every two years. Procedural aspects of the plan, including what to do in an emergency, are communicated to all staff.

### **3.4.6 Project Governance Framework**

Increasingly the Borough of Queenscliffe is running concurrent projects and initiatives that may have a major impact on the way the business operates. A project methodology is currently being developed to ensure every project follows consistent project guidelines to ensure that key processes, including identification of project risks, are followed and potential issues are addressed. Regular project updates are reviewed by management including risks identified and high level reporting will be provided to Council in regular reports.

## 3.5 REVIEW STRUCTURE

### 3.5.1 Risk Management Policy

The Compliance Committee and Executive Management Team hold a workshop once every two years to review the Risk Management Policy in light of the current Council Plan as well as to formally identify any new risks that have emerged. The new Risk Management Policy is then signed-off by Council.

Unplanned reviews may be triggered by incidents, new technology and legislation/regulation changes. All reviews will take into account hazard and incident reports, complaints about the Borough of Queenscliffe and any other information affecting the risk.

### 3.5.2 Risk Reporting and Review

Risk reporting occurs at three levels

**Level 1 – The Compliance Committee.** The Compliance Committee reviews risk at the Individual Risk Assessment Level. In addition to reviewing recorded risks the Compliance Committee identifies new and potential risks and develops Individual Risk Assessments for these.

**Level 2 – The Borough of Queenscliffe EMT.** The Borough of Queenscliffe Executive Management Team reviews risks at the Risk Register level and signs off on Level 3 reporting.

**Level 3 – Borough of Queenscliffe Council.** Borough of Queenscliffe Council receive summary reports half yearly. The summary reports include an assessment of key risks, a heat map displaying the level of risk, a summary of control effectiveness and the status of mitigation plans. The Audit and Risk Committee reviews the Risk Register annually.

### 3.5.3 Risk Reports

Risk reports incorporate the following:

- A heat map which displays both the current likelihood and consequence of each risk, and the targeted likelihood and risk after mitigation actions are complete;
- A summary of key risks;
- A graph indicating the movement in risks over time;
- Supporting information

### 3.5.4 Performance measures

- Risks assessed as High be reduced to Medium within 6 months
- Risks assessed as Medium be reduced to Low within 6 months
- Risk Calendar (see 3.5.6) fully complied with
- Audit and Risk Committee to recommend the Risk Register to Council for sign off at times required by the Local Government Act/Audit and Risk Committee Charter

### 3.5.5 Training

- All staff to be introduced to the Risk Management Framework at induction
- Staff involved in the Compliance Committee to receive additional hands on training in assessing risks and in the Risk Register more broadly

- New Councillors to receive training on the Risk Management Framework and the Risk Register

### 3.5.6 Risk Calendar

Frequency	Reporting Mechanism / Event
Ongoing	A risk register is maintained by the Risk Manager as the central document in the risk management framework
Ongoing	The risk management framework document and the risk register are accessible on the Borough of Queenscliffe intranet
Two monthly	Compliance Committee review progress and risks on current Borough of Queenscliffe activities – minutes and report forwarded to the Borough of Queenscliffe Executive.
Half Yearly	Borough of Queenscliffe EMT reviews reports and minutes from the Compliance Committee.
Half Yearly	Council and Audit and Risk Committee review summary reports.
Half yearly	The risk register is reviewed by Executive Team in Feb and Aug each year
Annual	The risk register, to Individual Risk Assessment level, is provided to the Audit and Risk Committee to review, along with a report by EMT
Annual	The internal audit program for the forthcoming year is agreed
Annual (various)	Internal auditors perform reviews
Annual (Jul/Aug)	External auditors perform statutory audit
Annual	Conduct testing of the BCP
Biennial	A risk management workshop is held. Results inform Risk Management Framework and Risk Register

Note: Months detailed are approximate and dependent on the Annual Governance Calendar.

## 3.6 ASSOCIATED BOROUGH OF QUEENSCLIFFE POLICIES AND DOCUMENTS

### a. Borough of Queenscliffe Council Plan and Implementation Plan

The Borough of Queenscliffe's Council and Implementation Plans provide a sound basis for the organisation to meet its underlying objective which is to ensure the Borough remains a safe haven for the historic, cultural and environmental values that make it a special place with high levels of community wellbeing. As such, risks identified in the Risk Register are explicitly linked to the Borough of Queenscliffe's Council Plan. The Risk Management Framework is put in place to identify and mitigate uncertainty surrounding the achievement of organisational objectives.



**b. Existing risk related Policies/Procedures**

- Complaints Handling Policy
- Internal Complaints Procedure
- Disaster Recovery Plan
- Councillor Code of Conduct
- Disciplinary Action Procedure
- Equal Employment Opportunity Policy
- Information Technology Policy
- OH & S Policy
- Information Privacy Policy
- Employee Assistance Program
- Asset Management Policy
- Fraud Prevention Policy
- Procurement Policy
- Election Caretaker Period Policy
- Business Continuity Management Policy
- Protected Disclosure Policy
- Child Safety Statement
- Employee Leave
- Municipal Emergency Management Plan
- Business Continuity Plan

**c. Policies Currently in Development or Under Review**

- Working with Children & Policy Checks Procedure
- OH&S Procedures

#### 4. RISK CLASSIFICATION

##### 4.1 RISK ANALYSIS MATRIX

The Borough of Queenscliffe established a list of potential risks and then estimated the level of threat posed by each risk on the basis of the likelihood of occurrence and the anticipated impact if the event occurred.

##### Consequences to Borough of Queenscliffe if event occurs

- 5 - extreme
- 4 - severe
- 3 - major
- 2 - moderate
- 1 - minor

##### Likelihood of event occurring

- 5 – very likely (>90% chance)
- 4 – likely (>60% chance)
- 3 – possible (>30% chance)
- 2 – unlikely (>5% chance)
- 1 – very unlikely (<5% chance)

Likelihood	Consequences				
	1 - minor	2 – moderate	3 - major	4 - severe	5 - extreme
5 – very likely	Moderate	Moderate	High	High	High
4 - likely	Low	Moderate	Moderate	High	High
3 - possible	Low	Moderate	Moderate	High	High
2- unlikely	Low	Low	Moderate	Moderate	High
1- very unlikely	Low	Low	Low	Moderate	Moderate

Risk Level	Description of Risk
High Risk	Consequences are significant, and may threaten the survival of the Borough of Queenscliffe
Moderate Risk	Consequences may affect effectiveness and operations but will not have significant impact
Low Risk	Minor consequences for the Borough of Queenscliffe

## 4.2 RISK RATING CRITERIA

Rating	Business Objectives	Key Financial Metrics	Stakeholder Interests		
			Ratepayers	Government/Regulator	Employees
<b>5. Extreme</b> Requires immediate & extensive senior management attention & effort & Council involvement	Results in failure of one or more key objectives or major initiatives or prevents Council from delivering key services.	More than 5% impact on Revenue (incl. remediation & opportunity costs).	Prolonged loss of service to community. (4+ days)	Breach of compliance obligations with potential costs (including costs to litigate, resolve and/or remediate penalties and claims) likely to exceed \$800K or criminal provisions apply.	Multiple fatalities or permanent disability. Resignation of large number of key executives or Councillors.
<b>4. Severe</b> Requires significant senior management attention	Seriously endangers one or more key objectives or major initiatives.	2.5-5% impact on Revenue (incl. remediation & opportunity costs).	Prolonged loss of service to a significant number of the community. (<4days)	Breach of compliance obligations with potential costs (including costs to litigate, resolve and/or remediate penalties and claims) likely to exceed \$300K.	Single fatality or permanent disability. Resignation of a number of key executives.
<b>3. Major</b> Requires considerable senior management attention	Constitutes some threat to one or more objectives or major initiatives.	0.5-2.5% impact on Revenue (incl. remediation & opportunity costs).	Loss of service to a significant number of the community. (<1 day)	Breach of compliance obligations with potential costs (including costs to litigate, resolve and/or remediate penalties and claims) likely to exceed \$100K.	Multiple serious injuries. Resignation of Key Staff. Significant impact on staff morale and turnover.
<b>2. Moderate</b> Requires limited senior management attention	Limited impact on objectives or major initiatives.	0.1-0.5% impact on Revenue (incl. remediation & opportunity costs).	Service disruption resulting in some community dissatisfaction that is managed as BAU. (<3 hours)	Breach of compliance obligations with potential costs (including costs to litigate, resolve and/or remediate penalties and claims) likely to be under \$100K.	Moderate injury or illness. Some impact on staff morale or turnover.
<b>1. Minor</b> Requires no senior management attention	No or negligible impact on objectives or major initiatives.	Less than 0.1% impact on Revenue (incl. remediation.	Minor service disruptions. (<1 hour)	Minor compliance incident. No penalties or costs to litigate resolve and/or remediate.	Minor injury or illness. No noticeable impact on staff morale and turnover.

## Appendix A - Individual Risk Assessment (example only)

Risk Title	Risk Owner	Risk Description	Overall Risk					
<b>Risk 5: People Risk</b>	CEO	Operational. The risk of the BoQ not having or being able to attract and retain the right staff	Current	<b>M</b>	Planned	<b>M</b>		
Causes	Consequences	Current Controls	Control effectiveness	Current Risk Rating				
				Likelihood	Consequence	Level		
1. Un-competitive conditions	1. Talent goes elsewhere	1. a. Above award conditions b. Above other union conditions	Effective	1	3	L		
2. Low morale	2. Poor performance	2. Genuine efforts to maintain morale	Effective	2	3	M		
3. Lack of diversity	3. Decreases outcome effectiveness	3. Nil	Poor	4	3	M		
4. Inadequate training	4. Poor performance	4. Training plans introduced for Admin staff	Effective	3	3	M		
5. Industrial activity	5. Lost time	5. Nil	Effective	1	3	L		
Planned Control	Planned Control effectiveness	Responsible	Due date	Status	Comment	Planned Risk Rating		
						Likelihood	Consequence	Level
1. Review and formalise staff classification structure	Effective	COO	Q1 2018	Scheduled		1	3	L
2. Formalise staff morale policies	Effective	COO	Q2 2018	Scheduled	Include BBQ, quarterly lunch, flu shots etc	1	3	L
3. New group forming to address female issues and strategies	Adequate	CEO	Q3 2018	Commenced training		2	2	L
4. Formalise induction and exit process	Effective	Danielle	Q4 2018			2	2	L
5. Nil (see 2 above)						1	3	L

Appendix B - Sample risk Report

ID	Risk Description	Last Report ( Aug 12)	This Report ( Nov 12)	Control Effectiveness	Mitigation plan status	Target Risk Level	Comment
1	Asset	High	High	E		Moderate	Implementation on track
2	Reputation	Moderate	High	E		Moderate	Implementation on track
3	Financial	High	High	A		Moderate	Implementation delayed due RADAR
4	IT	High	High	E		Moderate	Some delays to implementation
5	OHS	Moderate	Moderate	A		Moderate	Implementation on track
6	Catastrophic		Low	E		Low	Implementation on track

