Town of
Port Hedland

ATTACHMENTS

Under Separate Cover

Audit, Risk and Compliance Committee Meeting
Tuesday, 6 December 2022

Table of Contents

11.3 Internal Audit Report - Business Continuity and Disaster Recovery Management

Attachment 1 2022/23 Financial Year Internal Audit Report of Business Continuity and Disaster Recovery 4

William Buck
ACCOUNTANTS & ADVISORS

Town of Port Hedland

Business Continuity & Disaster Recovery Review
October 2022

williambuck.com

William Buck
ACCOUNTANTS & ADVISORS

CONTENTS

EXECUTIVE SUMMARY 2
DETAILED FINDINGS 6
STAFF INVOLVEMENT 12
INHERENT LIMITATIONS 12
APPENDIX A – RECORD OF WORK DONE AND OUTCOMES 13

William Buck
ACCOUNTANTS & ADVISORS

EXECUTIVE SUMMARY

Introduction

In accordance with the approved Strategic Internal Audit Plan, the Audit and Risk Committee of the Town of Port Hedland ("the Town") requested William Buck Consulting (WA) Pty Ltd to conduct an internal audit of the Town's Business Continuity and Disaster Recovery processes.

Background

The Town recently adopted a Business Continuity and Disaster Recovery Plan to ensure its business functions and services can still be delivered to its customers and the community in the event of a disaster.

Business Continuity Planning (BCP) is a management process that provides a framework for building resilience to business and service interruption risks; responding in a timely and effective manner to ensure continuity of critical business activities and ensuring the long-term viability of the City following a disruptive event.

The following diagram illustrates the business continuity process:

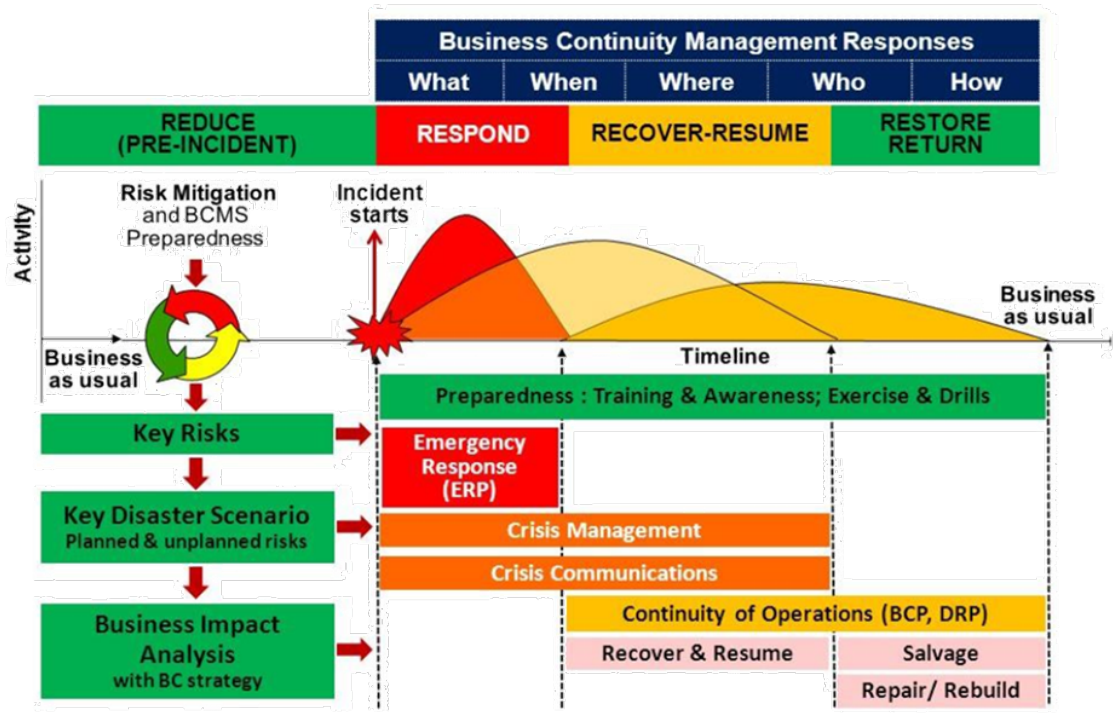


Figure 1: - BCP Process

As can be seen, the business Impact Analysis (BIA) is an integral part of the BCP and is designed to be flexible to accommodate a range of situations that are sudden, unforeseen or occur with varying levels of warning to prepare for, respond to, and recover from disruptive incidents when they arise. A BIA should focus on identifying the impact on core and critical business activities to which an occurrence of disruption may cause threats to business continuity.

William Buck
ACCOUNTANTS & ADVISORS

Proper risk assessment is important for effective Business Continuity Planning. Risk assessment includes identification, analysis, mitigation, and treatment of risks and their consequences, which may have adverse impacts on the business. In the context of Business Continuity Planning, it is crucial that organisations isolate the risks that may have an impact on the organisation's ability to continue as a going concern. An organisation needs to have proper contingency plans in place that will enable it to minimise the impact of critical business continuity risks to an acceptable level that will help drive the organisation with minimal risks of failure.

Objective

The overall objective of this engagement was to determine whether adequate and effective business continuity and disaster recovery measures were in place for ensuring continuity of business during and/or after incidents.

Scope

The scope of this engagement included consideration of the following:

- Roles and responsibilities for co-ordinating Business Continuity Plan ("BCP") development, maintenance and testing are clearly defined;
- A formal risk assessment has been completed to define potential events or incidents that could cause a disruption to the Town's business services;
- A formal plan has been developed to define the Town's response to business continuity risks and is regularly reviewed and approved;
- BCP clearly defines contingencies to manage various stages of the BCP life-cycle including emergency, backup and recovery phases;
- BCP establishes a "chain of command" in the event of a crisis which defines who is responsible for decision making and how decisions should be made; and
- BCP's are regularly tested, results of testing are documented, and outcomes of testing are used to refresh and improve plans.

Risks

Relevant risks identified in the Town's risk register in relation to the objectives of this review were:

#	Risk Description	Risk Level	Controls	Residual Risk
9	Business and Community Disruption	High	Adequate	Moderate

William Buck
ACCOUNTANTS & ADVISORS

Approach

The approach adopted for this review was as follows:

- Consideration of relevant processes and procedures, and discussion with the Town's management and staff responsible for the relevant scope areas;
- Identification of control weaknesses through analysis of the adequacy and effectiveness of controls;
- Identification of any discrepancies or deviations from processes and procedures.
- Discussion of control weaknesses, deviations from process and procedure with relevant stakeholders and the Town's management; and
- Development of this report identifying any weaknesses or issues, making relevant recommendations on the areas under the scope of the engagement.

Refer to Appendix A for the details of work done on this review.

Overall Comments & Findings

The Town has established a detailed BCP that is rich in information. Overtime this document should be refined through testing, reviews, and ongoing monitoring of risks.

The internal audit has identified improvement opportunities to enhance the business impact analysis by the inclusion of the recovery time objective and references to the maximum acceptable outage timeframes for business activities.

Whilst the business impact analysis is extensive (in Appendix 1 of the BCP), it is saturated with many business activities and priority ranking that seem to be disconnected to the critical business functions identified in the relevant part (section 3) of the BCP. Accordingly, it is uncertain whether all key dependencies have been identified and addressed.

The number of findings and their rating are summarised in the table below. Details of findings and recommendations are contained in the next section of the report.

Observation	Extreme	High	Medium	Low	PI	Total
Maximum Acceptable Outage & Recovery Time Objectives		1				1
Critical Business Activities		1				1
Testing of the BCP			1			1
Total		**2**	**1**			**3**

William Buck
ACCOUNTANTS & ADVISORS

The following risk and control matrix was used to evaluate and rate the findings.

RISK		CONTROL EFFECTIVENESS
Extreme	Extreme Risk	Extreme residual risk – Urgent attention required.
High	High Risk	High residual risk – Attention required
Medium	Medium Risk	Medium residual risk – Monitor
Low	Low Risk	Low residual risk – Acceptable
PI	Process Improvement	Low residual risk – administrative improvement required, or no issues noted.

William Buck
ACCOUNTANTS & ADVISORS

DETAILED FINDINGS

1. Maximum Acceptable Outage & Recovery Time Objectives

High | Medium | Low | PI

Section 8.2.2 (d) and (e) of *ISO 22301:2019: Security and resilience – Business continuity management systems – Requirements* respectively stipulate that the organisation shall:

> *(d) "Identify the time frame within which the impacts of not resuming activities would become unacceptable to the organisation.*
>
> *NOTE 1: This time frame can be referred to as the "maximum tolerable period of disruption [MTPD]""*
>
> *(e) "Set prioritised time frames within the time identified in (d) for resuming disrupted activities at a specified minimum acceptable capacity.*
>
> *NOTE 2: This time frame can be referred to as the "recovery time objective (RTO)""*

Although the Town's BCP includes a tier list with maximum acceptable outage timeframes, these timeframes were not incorporated into the Business Impact Analysis. Furthermore, we identified that the BCP and the BIA lack the Recovery Time Objectives that describe the timeframes for the resumption of business activities at a minimum specified acceptable capacity after a disruption.

Without Recovery Time Objectives, the Town may face difficulties in prioritising recovery actions which could lead to risks of prolonged business disruptions.

The recovery time objectives should be realistic and ideally be shorter than the maximum allowable outage period, meaning that the affected business operations should be resumed within the maximum allowable outage period.

When set correctly, the recovery time objectives will help the Town minimise the consequences arising from disruptions by way of forward planning in scheduling and allocating resources to bring the affected critical business function back to normal.

Recommendation

We recommend that the Town:

1.1. Assess and assign realistic recovery time objectives within the BIA.

1.2. Incorporate the maximum acceptable outage timeframe into the BIA.

William Buck
ACCOUNTANTS & ADVISORS

Recommendation 1.1

Management Response	
Agree/Disagree:	Agree.
Action to be taken:	Management will add a column to the BIA to capture realistic Recovery Time Objectives. Management will update the BCP on the intranet by 31 December 2022. The BCP and any updates made since its adoption in mid-2022 will be put up to Council for formal approval prior to 30 June 2023.
Completion Date:	31 December 2022 – Update BCP on the intranet 30 June 2023 – Formal approval by Council.
Responsible Officer:	Director Regulatory Services.

Recommendation 1.2

Management Response	
Agree/Disagree:	Agree.
Action to be taken:	Management agree to change the name of the column in the BIA column 'Period before business loss occurs/noticed by public' to 'Maximum acceptable outage'. Management will update the BCP on the intranet by 31 December 2022. The BCP and any updates made since its adoption in mid-2022 will be put up to Council for formal approval prior to 30 June 2023.
Completion Date:	31 December 2022 – Update BCP on the intranet 30 June 2023 – Formal approval by Council.
Responsible Officer:	Director Regulatory Services.

William Buck
ACCOUNTANTS & ADVISORS

2. Critical Business Activities

High | Medium | Low | PI

A business impact analysis identifies the activities in a business that are key to its survival, also known as critical business activities. It also helps the business to identify:

- The resources needed to support each activity
- The impact of ceasing to perform these activities
- How long the business could cope without these activities.

We reviewed the Business Impact Analysis in the BCP and identified that the BIA contains an extensive list of critical and high priority business activities some of which do not appear to be essential to such extent that it imposes a business continuity threat to the Town.

Listed below are some selected examples of business activities at different levels of priority within the BIA and our comments thereto:

Business activity	Priority	William Buck's Comment
Answering main line phone calls	Critical	Whilst the disruption would be noticeable by the public and may threaten the efficiency and effectiveness of service, however, it would seem unlikely to escalate to an existential threat.
Facilities Closed	High	The loss of "revenue" or financial impact would not be at a level, in the short to medium term, represents a going concern risk for the Town.
Cleaners unable to provide services to perform contract on public ablutions.	Medium	Whilst this would cause an inconvenience to the public due to closure of public toilet facilities, however, the consequences are relatively minor and unlikely to cause major damage, disruption to the Town's operations.
Failure of Pool Heating	Low-Medium	Failure to heat the pools is unlikely to pose a business continuity risk in an environment of warm climate for most parts of the year.

Generally, we found that most of the activities rated "Low-Medium" and "Low" priority do not really pose a threat to the Town's business continuity. These activities represent risks to the Town's normal operations, which should be attended in the ordinary course of business.

In terms of business continuity, it is important to identify and prioritise critical business functions to ensure resources and management actions are focused on the activities that are required to enable the Town providing a minimum level of services. To that regard, we also observed, the "key dependencies", i.e., the activities which a business process dependent upon, have not been clearly identified in the BCP. For example, what are the system, processes and human resources which fortnightly payroll requires?

By identifying the dependencies, the Recovery Time Objectives can be defined for each business activity and appropriate strategies can be developed.

Additionally, the relationship between the outcomes of the BIA in Appendix 1 and the key business functions in *section 3 Business Impact Analysis – Critical Activities*, is not clear because the terminologies used in the BIA to describe the priority are not aligned to the tier MAO table. For example, the highest priority in the tier MAO table of section 3 is "*Immediate*" whereas the BIA uses the concept "*Critical*"; similarly, it is unclear what is the equivalent of "*High*" priority in the BIA to the priority of the tier MAO table.

William Buck
ACCOUNTANTS & ADVISORS

Recommendation

We recommend that the Town:

2.1. Consider the priority ratings and business activities identified in the BIA and how they link to the critical business functions defined for "priorities for continuation" in section 3 of the BCP;

2.2. Align the priority concepts in the BCP and the BIA to ensure consistency; and

2.3. Identify and document the key dependencies for critical business functions and consider whether the current responses are sufficient.

Recommendation 2.1

Management Response	
Agree/Disagree:	Agree.
Action to be taken:	Management will review the priority ratings for the business activities identified in the BIA. Only business activities with a priority of high or critical will be retained in the table. This will be updated in the BCP informally by 31 December 2022 and updated on the intranet. This update will go to Council for formal approval before 30 June 2023.
Completion Date:	31 December 2022 – Update BCP on intranet 30 June 2023 – Council approval.
Responsible Officer:	Director Regulatory Services.

Recommendation 2.2

Management Response	
Agree/Disagree:	Agree.
Action to be taken:	The wording within the BCP and BIA will be aligned and include both a time priority and business priority.
Completion Date:	31 December 2022 – Update BCP on intranet 30 June 2023 – Council approval.
Responsible Officer:	Director Regulatory Services.

Recommendation 2.3

Management Response	
Agree/Disagree:	Agree - in part.
Action to be taken:	Some of the key dependencies are already listed in the BIA, however, will include another column to reflect this. Further, workarounds may be identified at the time of the incident/emergency where the ordinary system or process is not able to be applied.
Completion Date:	31 December 2022 – Update BCP on intranet 30 June 2023 – Council approval.
Responsible Officer:	Director Regulatory Services.

WilliamBuck
ACCOUNTANTS & ADVISORS

3. Testing of the BCP

High	Medium	Low	PI

Section 8.5 of *ISO 22301:2019: Security and resilience – Business continuity management systems – Requirements* stipulate that:

> *"The organisation shall implement and maintain a programme of exercising and testing to validate over time the effectiveness of its business continuity strategies and solutions.*
>
> *The organisation shall conduct exercises and tests that:*
>
> *a) are consistent with its business continuity objectives;*
> *b) are based on appropriate scenarios that are well planned with clearly defined aims and objectives;*
> *c) develop teamwork, competence, confidence and knowledge for those who have roles to perform in relation to disruptions;*
> *d) taken together over time, validate its business continuity strategies and solutions;*
> *e) produce formalized post-exercise reports that contain outcomes, recommendations and actions to implement improvements;*
> *f) are reviewed within the context of promoting continual improvement;*
> *g) are performed at planned intervals and when there are significant changes within the organization*
>
> *The organization shall act on the results of its exercising and testing to implement changes and improvements"*

The Town's BCP includes a training and testing schedule. We identified that the schedule is incomplete as it only includes training/testing of Work-From-Home arrangements. We identified through enquiries that the IT components of the BCP are planned to be undertaken in September 2022, which was not included in the schedule.

We acknowledge that the BCP was recently adopted, on 25 May 2022, and the Town's comments that there is no formal testing since the adoption of the BCP.

Nevertheless, it is important that the Town identify and plan in advance the testing requirements in order to test the effectiveness of the BCP and to ensure they are fit for purpose. Section 8.5 of *ISO 22313:2020 – Business continuity management systems* states that *business continuity procedures and arrangements cannot be considered reliable until exercised and unless their currency is maintained.*

Testing of the BCP will also give the Town more confidence in the procedures and arrangements in cases where risks materialise and cause disruptions.

Recommendation

We recommend that the Town:

3.1 Identify testing requirements;

3.2 Plan and perform testing of BCP; and

3.3 Reflect on the testing outcomes and revise the BCP as required.

William Buck
ACCOUNTANTS & ADVISORS

Recommendation 3.1

Management Response	
Agree/Disagree:	Agree.
Action to be taken:	Management have identified testing requirements for the period before the BCP is due to be reviewed (May 2023). The identified testing requirements include: 1. A SMS test for cyclone alerts 2. An ICT systems 'crash'. Further tests will be identified and included within the current version of the BCP.
Completion Date:	31 December 2022 – Update BCP on intranet 30 June 2023 – Council approval.
Responsible Officer:	Director Regulatory Services.

Recommendation 3.2

Management Response	
Agree/Disagree:	Agree.
Action to be taken:	As part of annual BCP reviews moving forward, documented testing programs will be prepared and included within the following years amended/updated BCP. BCP testing will be included within the table at the start of the financial year, and adopted by Council. Learnings and any modifications will be incorporated into the document after each test, with the document being reviewed and adoption by Council at the end of financial year.
Completion Date:	30 June 2023.
Responsible Officer:	Director Regulatory Services.

Recommendation 3.3

Management Response	
Agree/Disagree:	Agree.
Action to be taken:	Testing outcomes and lessons learned will inform amendments to the BCP after each test event. These will be included within the document for review and adoption by Council at the end of financial year review.
Completion Date:	30 June 2023.
Responsible Officer:	Director Regulatory Services.

William Buck
ACCOUNTANTS & ADVISORS

STAFF INVOLVEMENT

Staff involved with this engagement were:

Interviewed employees	Stephanie Sikaloski (A/Senior Risk and Audit Advisor) Craig Watts (Director Regulatory Services)
William Buck Process Lead	Conley Manifis (Quality Assurance Director) Duy Vo (Engagement Director) Shifaz Moosa (Internal Auditor)

INHERENT LIMITATIONS

The nature of our review is influenced by factors such as the use of professional judgement, selective testing, the inherent limitations of internal controls, and the availability of persuasive, rather than conclusive, evidence.

William Buck ensures that reasonable care and competence are displayed during our engagements. As such, we conduct examinations and verifications to a reasonable extent, but we cannot give absolute assurance that noncompliance or irregularities do not exist.

Our review is focused on "Key Controls" as identified and assessed. Inherent audit limitations exist in any internal control structure, and it is possible that errors or irregularities may occur and not be detected.

Our findings expressed in this report have been based on the evaluation of existing processes in the organisation and sample testing performed on the existing controls as designed and implemented by management.

For these reasons, we can only provide reasonable, but not absolute assurance on the status of the internal control environment.

WilliamBuck

APPENDIX A – RECORD OF WORK DONE AND OUTCOMES

Test #	Test Procedures	Information / Document Reviewed	William Buck Analysis	Outcomes	Finding #
Scope Item 1 – Roles and responsibilities for co-ordinating Business Continuity Plan ("BCP") development, maintenance and testing are clearly defined.					
01-1	1 Through discussions with management and review of the BCP, identify that roles and responsibilities are clearly defined in an event of a crisis. 2 Identify that the BCP and other related plans have relevant contact numbers of responsible staff. 3 Identify that the BCP is appropriately communicated and available on the Town's intranet as well as off-site in an event of a disaster/crisis. 4 Identify that BCP testing requirements are defined.	1 Business Continuity Plan 2 Recovery Plan	1 Reviewed the BCP along with the Recovery Plan to determine whether: 1.1 Business continuity roles and responsibilities were clearly defined; 1.2 Contact details of key staff were provided; and; 1.3 BCP testing requirements were included 2 Enquired with the Town to demonstrate whether the BCP was appropriately communicated and made available for all staff.	1 The roles and responsibilities were defined in Section 4 of the BCP under the heading "Business Continuity Team – Roles and responsibilities" as well as in Section 8 of the Recovery Plan. 2 Contact details of key staff were included in Section 4 of the BCP under the heading "Key Contacts". 3 BCP testing requirements, including testing frequency, was included in Section 6 of the BCP under the heading "Testing and Training schedule". 4 The CEO and Executives provide a briefing to all staff members after Ordinary Council Meetings. This was communicated with all staff members through email and the minutes of the meeting where the BCP was endorsed, were made	No findings.

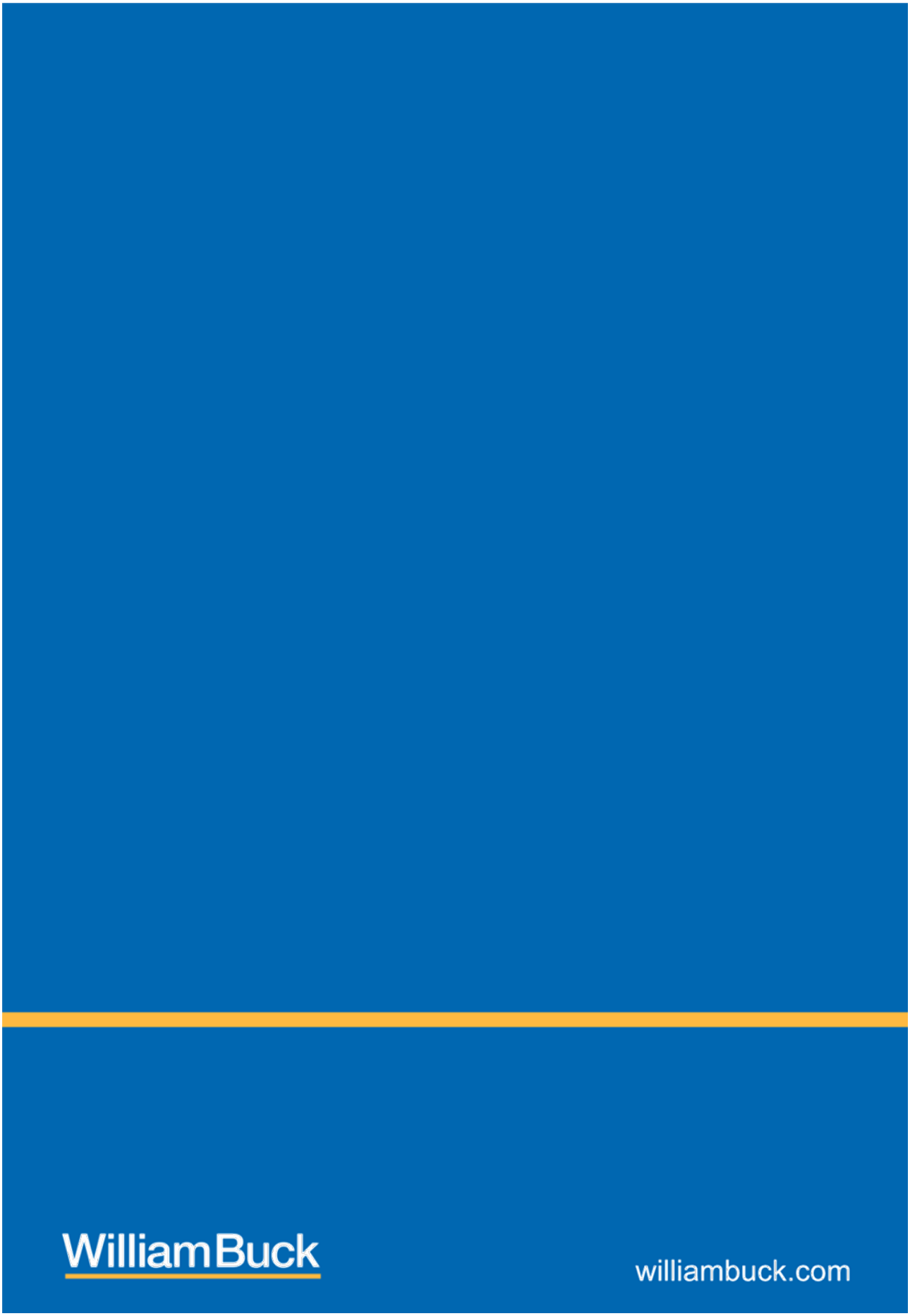
Test #	Test Procedures	Information / Document Reviewed	William Buck Analysis	Outcomes	Finding #
				available. The BCP is also readily available on the Town's intranet.	
Scope Item 2 – A formal risk assessment has been completed to define potential events or incidents that could cause a disruption to the Town's business services.					
02-1	Identify whether a formal risk assessment has been done to define potential events or incidents that could cause a disruption to the Town's business services.	1 Business Continuity Plan 2 Business Impact Analysis	1 Reviewed the BCP to determine if a risk assessment was done. The BCP mentioned that risk assessments need to be done in accordance with AS/NZS ISO 31000:2009 and the Town's Risk Management Policy 2 Appendix A of the BCP includes the Business Impact Analysis (BIA) that was performed. Reviewed the BIA to determine if it captured critical business activities and their impact of an incident.	1 The BIA does not include Recovery Time Objectives (RTO). 2 The priority concepts defined in the BIA is different from the tier MAO table. 3 Key dependencies have not been identified.	Finding 1 Finding 2

Test #	Test Procedures	Information / Document Reviewed	William Buck Analysis	Outcomes	Finding #
Scope Item 3 – A formal plan has been developed to define the Town's response to business continuity risks and is regularly reviewed and approved.					
03-1	1 Identify whether a response plan has been developed that defines the Town's response to business continuity risks 2 Identify that the plan is approved and regularly reviewed.	1 Business Continuity Plan 2 Incident Response Plan (within the BCP)	1 Reviewed the Incident Response Plan (IRP) within the BCP to determine whether: 1.1 The IRP activation details were included; 1.2 Details on communication and maintaining chain-of-command were included; 1.3 Details of responsible staff, including their contact details, were included; and 1.4 Appropriate course of action were included; and 1.5 Identified the BCP adoption date and when it is due for the next review.	1 The IRP (Section 4 of the BCP) includes details on how the Town will respond to business continuity risks. It includes details such as how the plan will be activated and communicated, details of key staff responsible and their contact details, and the proposed course of action during a crisis. 2 The BCP was adopted on 25 May 2022 and is scheduled for review on a 12-month cycle.	No findings.
Scope Item 4 – BCP clearly defines contingencies to manage various stages of the BCP life-cycle including emergency, backup and recovery phases.					
04-1	1 Identify that the BCP clearly defines contingencies to manage various stages of the BCP's lifecycle including: 1.1 Emergency 1.2 Back-up: and	Business Continuity Plan	1 Reviewed the BCP to identify whether adequate contingency planning has been done to manage the various stages of the BCP's lifecycle.	1 Section 1 of the BCP under the heading "Activation" describes that the BCP will be activated by the CEO. In the absence of the CEO, it will be activated by the Executive Management Team.	No findings.

Test #	Test Procedures	Information / Document Reviewed	William Buck Analysis	Outcomes	Finding #
	1.3 Recovery Phases.		2 Assessed whether there is a link between the different phases of the BCP such as: 2.1 When does the emergency response kick in at the onset of a disruptive event; 2.2 How long does it take for the crisis management team to take control of the incident; 2.3 When do business continuity and disaster recovery operations begin; 2.4 How long does it take for recovery actions to begin; 2.5 How long does it take for the restoration of normal business activities. 3 Assessed whether the BCP addresses the key aspects of: 3.1 Denial of access to premises 3.2 Loss of workforce/human resources	2 After activation, the Business Continuity Team (BCT) comes into action. 3 Section 4 of the BCP details the procedures that will be followed by the BCT throughout the disruption. 4 Section 4 of the BCP under the heading "Business Continuity Team – Recovery of Business Operations" includes the steps that will be taken to recover business operations. It also refers to the Town's Recovery Plan which includes further details of recovery. 5 Section 2 Risk Management Planning consider the risk of loss of staff, loss of premises, loss of ICT, and loss of a key supplier.	

Test #	Test Procedures	Information / Document Reviewed	William Buck Analysis	Outcomes	Finding #
			3.3 Prolonged interruptions to ICT		
Scope Item 5 – BCP establishes a "chain of command" in the event of a crisis which defines who is responsible for decision making and how decisions should be made.					
05-1	Determine if the BCP clearly establishes a chain of command in the event of a crisis that defines who is responsible for decision making and how decisions should be made.	Business Continuity Plan	Reviewed the BCP to determine if it includes a chain of command	Section 4 of the BCP under the heading "Business Continuity Team Relocation when required" states that the Tier hierarchy should be considered to maintain the chain of command and essential functions.	No Findings
Scope Item 6 – BCP is regularly tested, results of testing are documented, and outcomes of testing are used to refresh and improve plans.					
06-1	Identify the BCP testing process and determine if the BCP is regularly tested, and the outcomes documented.	Business Continuity Plan	Enquiries were made to identify the BCP testing process. A testing/training schedule is included in Section 6 of the BCP under the heading "Testing and Training Schedule"	1 Section 6 of the BCP under the heading "Testing and Training Schedule" describes the testing process; minor components of the plan are to be tested quarterly and larger components annually. 2 We identified the following: 1.1 There was no definition of what is considered minor and major. 1.2 The testing schedule looks incomplete as it only includes the testing of Work-From-Home arrangements	Finding 3

Test #	Test Procedures	Information / Document Reviewed	William Buck Analysis	Outcomes	Finding #
06-2	Identify whether the outcomes of the testing are reflected in the response plans to refresh and improve the plans.		Enquiries were made to identify whether any testing of the BCP has been performed.	The BCP was recently adopted on 25 May 2022, the Town had not yet performed any testing of the BCP. Planned testing on IT components is to be done in September 2022. The BCP is scheduled for review on a 12-month cycle.	Finding 3


WilliamBuck
williambuck.com