


Business Continuity Management Policy

About this document

Disclaimer	For Department of Conservation (DOC) internal use only.
Document Coordinator	Drew Coleman, Senior Advisor, Risk Management
Document Owner	Graeme Ayres, Director, Business Assurance
Approved for use by	Rachel Bruce, Deputy Director-General, Corporate Services (Acting) Date: 20/02/2020 
Effective date	20/02/2020
Last reviewed	20/02/2020 (please check this document within two years to ensure it is up-to-date)
Classification	IN-CONFIDENCE
docCM ID	doc-1313310

Contents

1.	Background	2
1.1	Purpose	2
1.2	Scope	2
1.3	Audience	2
1.4	Introduction/Context	2
1.5	Objectives	2
1.6	Guiding principles	3
1.7	Mandate	3
1.8	Statement of Governance	3
1.9	Terms and definitions	4
2.	Critical Functions and Critical Services	6
3.	Roles and responsibilities	9
4.	Policy statements for Business Continuity	10
5.	Related documents	12
6.	Document history	13

1. Background

1.1 Purpose

This Policy ensures the Department is clear about Critical Functions and Critical Services required for minimum business operability. This policy defines the way in which the organisation will approach business continuity and how the Business Continuity Management programme will be structured and resourced.

1.2 Scope

This Policy describes the strategic direction from which the business continuity programme is delivered. The business continuity programme is to be rolled out across the Department beginning with governance roles and executive level business continuity plans for Critical Functions and Critical Services.

This Policy sets out the Governance structures and roles and responsibilities required to maintain minimum business operability.

Minimum business operability covers the Critical Functions and Critical Services that the Department of Conservation provides to staff, contractors, key stakeholders, and customers in an emergency or disruption to business. These Critical Functions and Services are owned by Deputy Directors-General who are accountable for the delivery of the Critical Function or Critical Service.

1.3 Audience

This Policy applies to the Senior Leadership Team, and specifically to Deputy Directors-General with accountability for Critical Functions and Critical Services. Directors with responsibility for delivering the function or service through their business group must ensure the Policy is understood by their staff.

1.4 Introduction/Context

Business continuity management is critical to responsible business management practice and is an integral part of DOC's approach to risk management. Effective management of risk in this context will develop a more resilient organisation to threats and business disruption events.

This policy is aligned with the Business Continuity Institute [BCI] 'good practice guidelines', which follows the global standard ISO 22301:2012 Societal Security, Business Continuity Management Systems requirements. It is also supported by protective security best practice.

1.5 Objectives

Implementing this policy will:

- Demonstrate a commitment toward Business Continuity activities as a core assurance function for the Department.
- Document senior leadership commitment towards long-term and comprehensive business continuity planning within DOC.

- Identify governance structures and accountability for the development, implementation, monitoring, review and ongoing maintenance of Business Continuity Management.

1.6 Guiding principles

The business continuity policy provides the intentions and direction of the Department as formally expressed by the Executive.

Business continuity:

- o is an integral element in DOC's risk management and protective securities processes.
- o is embedded into the culture of the organisation through structured and resourced Business Continuity practices.
- o requirements are considered while developing new business initiatives, and where business partners are involved in the delivery of critical functions or critical services.

The 'Team Process' leadership and decision-making methodology underpins the process of Business Continuity planning (see [Team Process guidelines for managers](#) (docdm-1521828) and [Team Process Intranet page](#)).

1.7 Mandate

The mandate for this policy originates from legislation governing the management of business continuity and government protective security requirements.

- The New Zealand government Protective Security Requirements for Governance ([GOVo3 – Prepare for business continuity](#)) require agencies to:
 - o Maintain a business continuity management programme, so that your organisation's critical functions can continue to the fullest extent possible during a disruption. Ensure you plan for continuity of the resources that support your critical functions.
- The [Civil Defence Emergency Management Act 2002](#), Section 58
Every department must:
 - o ensure that it is able to function to the fullest possible extent, even though this may be at a reduced level, during and after an emergency:
 - o make available to the Director in writing, on request, its plan for functioning during and after an emergency.

The State Services Commission, Department of the Prime Minister and Cabinet and Officials Committee for Domestic and External Security Coordination (ODESC) require central government agencies to prepare business continuity activities to support Ministers from an Auckland base during significant disruption to government business.

1.8 Statement of Governance

Policy Accountability

The Deputy Director-General, Corporate Services, accepts Single Point Accountability for implementing this Policy. Accountability includes:

- resourcing and budget for the Business Continuity programme of work.
- monitoring and measuring indicators of implementation of this Policy.

- monitoring progress of Executive Business Continuity Plans associated with the Critical Functions and Critical Services identified in this policy.

Critical Function & Service Accountability

Individual DD-Gs have accepted accountability for Critical Functions and Critical Services within parameters of their role as identified in this Policy.

System Custodian

The Business Assurance Unit is custodian of this Policy and the associated Business Continuity framework.

1.9 Terms and definitions

Term	Definition
Business Continuity	The capability of the organisation to continue delivery of products or services at acceptable pre-defined levels following a disruptive incident.
Business Continuity Management (BCM)	A holistic management process that identifies potential threats to an organisation and the impacts to business operations those threats, if realised, might cause, and which provides a framework for building organisational resilience with the capability of an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities.
Business Continuity Plan (BCP)	Documented procedures that guide organisations to respond, recover, resume, and restore to a pre-defined level of operation following disruption.
Business Continuity Programme	The ongoing management and governance process supported by top management and appropriately resourced to implement and maintain business continuity management.
Business Disruption Event	An event that has an adverse effect on the delivery of the critical functions of an organisation. It may be an acute, creeping or sustained event.
Business Impact Analysis (BIA)	The process of analysing activities and the effect that a business disruption might have upon them.
Critical Function	Processes and activities which, if interrupted, will cause an organisation to lose the capability to deliver on its objectives, and as a result suffer serious financial, legal, reputational, or other damages or penalties.
Critical Services	Beneficial outcomes provided by an organisation to its customers, recipients and interested parties.
Disaster Recovery Plan	A disaster recovery plan documents how information technology (IT) systems would be recovered in the event of a disaster.
Incident	A situation that might be, or could lead to, a disruption, loss, emergency or crisis.

Maximum acceptable outage (MAO)	The time it would take for adverse impacts, which might arise as a result of not providing a product/service or performing an activity, to become unacceptable.
Maximum tolerable period of disruption (MTPD)	The time it would take for adverse impacts, which might arise as a result of not providing a product/service or performing an activity, to become unacceptable.
Minimum Business Continuity Objective (MBCO)	The minimum level of services and/or products that is acceptable to the organisation to achieve its business objectives during a disruption.
Protective Securities Requirements	An all-of-government policy framework that when implemented, provides pathways for successfully protecting people, information and assets.
Resilience	The ability of an organisation to absorb and adapt in a changing environment.
Risk management	Coordinated activities to direct and control an organisation with regards to risk.
Test	An exercise whose aim is to obtain an expected, measurable pass/fail outcome.

2. Critical Functions and Critical Services

Critical Business Functions					
Critical Function	Business Group	Why is it important?	Maximum Acceptable Outage	Maximum Tolerable Period of Disruption	Minimum Business Continuity Objective
ICT	CSG	DOC is reliant on workable ICT solutions for everyday tasks and for maintaining minimum business functions.	1 day	1 week	Ensure all staff can access core business critical communication services external dependency?
Property	CSG	Ensure safety of DOC owned buildings.	1 month	6 months	Alternative accommodation
		Provide alternative work accommodation for staff to resume normal operations.	2 weeks	3 years	Alternative office space
Payroll	People and Engagement	To support our people	1 day	Until the next pay date (1-14 days)	Average fortnightly pay is provided
Accounts Receivable	CSG	Working capital Money due may not be recovered	60 days	90 days	Maintain working capital
Legal Services	CSG	Advice to the DG, Minister, other agencies and Operations on:	1 day	1 week	Ministerial advice is provided that at least meets Minister's minimum expectations.
		Policy or statutory implications of decisions made in response to an event, and on DOC's Critical Functions.	1 day	1 week	Policy & Legal advice is provided to SLT during response & recovery

Comms Hardware	CSG	National DOC radio network	N/A	2 weeks	Wellington and Auckland are focussed on to restore service.
		Cell phones	Dependent on external infrastructure		
		Satellite phones	N/A	3 days	External response and recovery agencies rely on DOC radio network.
Consent processing	Ops	Consideration of emergency authorities or consents from the DG of Conservation or Minister of Conservation that may be needed for a response.	1 day	1 week	Consents required for remediation of roading, buildings etc under the RMA.
H&S	People & Engagement	Ensure H&S of staff impacted by the event, and during response and recovery efforts.	1 day	3 days	Maintain DOC's H&S system
Wellbeing	People & Engagement	Ensure wellbeing of staff impacted by the event.	1 day	3 days	Maintain DOC's Wellbeing system
HR	People & Engagement	Onboarding of temporary staff for response and recovery. Assessment of allowances. Dispute resolution. Relocations due to disruption.	1 week	1 month	Maintain HR system

Critical Business Services					
Critical Service	Business Group	Why is it important?	Maximum Acceptable Outage	Maximum Tolerable Period of Disruption	Minimum Business Continuity Objective
Accounts Payable	CSG	Maintaining obligations to Debtors	90 days	3 periods	

		Maintaining key Contractors critical to the recovery of business systems or activities	60 days	2 periods	Focused on accounts and contractors associated with response and recovery efforts
Media & Comms	People & Engagement	Internal communication to staff	1 day	1 week	DOC website, social media, and the DOC intranet
		External communication	1 week	1 month	DOC website used to indicate safe sites for public access
Engineering assessments	Ops	Provision of engineering assessment services, and asset planners for data relating to inspection	90 days	8 months	Service Standards Minimising risk to public Closure of huts Closure of bridges and structures Closure of tracks

3. Roles and responsibilities

This Policy applies to all DOC staff responsible for, or involved in, the delivery of DOC's critical functions and services.

All staff members: Must be familiar with the [policy subject] principles and apply them to their day-to-day activities as necessary.

Managers and team leaders: In addition to their usual responsibilities, staff members must provide support and guidance to assist staff and contractors to follow the policy.

Directors: If responsible for delivery of a Critical Function or Critical Service must develop a Business Continuity Plan that meets agreed MAO, MTPD, & MBCO as stated in this policy.

Deputy Directors-General [SLT collective]:

- Must agree on the Critical Functions and Critical Services detailed in this Policy;
- Must ensure Delegations of Authority are formalised for their Tier 1 or Tier 2 roles, and maintained at all times;
- Must own the relevant Function or Service as appropriate within their role and span of control; and
- Must agree to champion business continuity activities with the Department.

Deputy Director-General, Corporate Services

- Accountable for the coordination and strategy of Business Continuity within the Department;
- Promotes compliance with Business Continuity policies, SOPs and guidelines; and
- Final approval and policy sign-off.

Business owner – Director, Business Assurance

- Responsible for the implementation of Business Continuity Management System including the supervision of appropriate documentation, training, testing, monitoring and reviewing of the Business Continuity Framework.

Senior Advisor Risk Management:

- Manages, maintains and advises on DOC's Business Continuity Management practices and activities.
- Over-sees the Business Continuity (Senior) Advisor / Coordinator.

Business Continuity (Senior) Advisor/Coordinator [Not funded]:

- Contributes towards improving the process by which business continuity planning is organised and maintained within DOC.
- Ensures that business continuity planning for individual units or sites is consistent and does not contradict or undermine other plans.
- Ensures current practice is aligned with Business Continuity standards and good practice.

4. Policy statements for Business Continuity

Business Continuity Management [BCM] Governance

Governance for business continuity primarily focuses on:

- Ensuring the Policy is approved.
- Supervision; support and resourcing of the business continuity framework.
- Ensuring the Business Continuity framework aligns with the Department's objectives and strategic risks.
- Planning for business disruption events to minimise impacts.

Threat and Risk Assessment

- Critical functions and critical services are assessed with an all-risks approach to business disruption.
- DD-G's assess the specific risks to maintaining their critical functions.

Business Impact Analysis

The Business Impact Analysis (BIA) is critical to DOC's business continuity planning. It identifies the roles, facilities and systems required to support key processes for Critical Functions or Services, including interdependencies between business areas and external providers.

Business Continuity Plans

This Policy requires DOC to have an overarching Business Continuity Plan for Critical Functions and Critical Services. This Policy defines the following for each Critical Function and Critical Service:

- Maximum Tolerable Period of Disruption [MTPD]
- Maximum Allowable Outage [MAO]
- Minimum Business Continuity Objective [MBCO]

Business Continuity planning ensures the continued delivery of Critical Functions or Services identified in the Policy in the event of a disruption or emergency. These plans consider the impact of all risks and identify the options to increase resilience for critical functions and to minimise disruption to the Department.

Business Continuity Management Testing

DOC Business Continuity Management arrangements are tested to ensure that they continue to meet business requirements. The Business Continuity test programme is coordinated and maintained by the Business Assurance Unit.

External Providers

When engaging with external providers, DOC staff always consider both the nature and scale of the service being provided, and the level of assurance required from providers for contingency planning. This must be included in the contract conditions and deliverables when contracting for services regarding continuity of essential services.

Business Continuity Documentation and Records

The following documentation and activities form the essential elements of DOC Business Continuity management:

- Business Continuity Management Policy
- Business Impact Analyses
- Risk Assessments
- Business Continuity Plans
- Exercising and testing plan
- Maintenance and review schedule
- Internal audit and/or external review
- Instrument of Delegation

Documentation Controls

Controls are established over the Business Continuity documentation to ensure:

- documents are approved for use by the appropriate DD-G prior to their issue (this is coordinated by Business Assurance as custodian of the Business Continuity Framework).
- documents are reviewed, updated and re-approved as required by the Business Rules Framework.
- all DOC business continuity documentation is discoverable from a central file within the document management system.

Auditing Business Continuity Management

Periodic internal or external audit of the status of DOC's system of Business Continuity management and associated documentation will be undertaken against Business Continuity standards.

Maintaining this policy

Keeping this policy up to date is the responsibility of the Deputy Director-General, Corporate Services, and a review of this policy is to be undertaken every two years.

5. Related documents

DOC Business Continuity Planning	
Business Continuity Management policy	docDM-1313310
Legislation	
The Civil Defence Emergency Management Act 2002, Section 58	
External Standards	
ISO 22301:2012 Societal Security, Business Continuity Management Systems – requirements	
AS/NZS 5050:2010; Business continuity – Managing disruption-related risk	
Protective Securities Requirements	
Related DOC publications	
Risk Management Policy	doc-2224884
Research and analysis to support DOC Business Continuity planning 2017-18	doc-2968865
Register of Corrective Actions 2017	doc-3089707
Conservation House Critical Emergency Plan	doc-5463211
Hamilton/Kirikiroa Critical Emergency Plan in the event of a large Wellington earthquake	doc-2956380
Risk Leadership Guideline	doc-2901864
Team Process guidelines for managers	docDM-1521828

6. Document history

Date	Details	Document ID and revision number	Amended by
10/02/2014	First draft - unpublished	docDM-1313310 revision 1	Carolyn Ramsay
01/07/2014	Second draft - unpublished	docDM-1242481	Leah Watts
4/08/2017	First version for publication - unpublished	doc-1313310 revision 15	Nicki Stevens
06/09/2019	Updated Policy for approval	doc-1313310 revision 16	Drew Coleman
20/02/2020	Approved Policy	doc-1313310 revision 25	Drew Coleman
12/03/2020	<p>Urgent update in the context of COVID-19 to reflect the need for Delegations of Authority for T1 and T2 roles.</p> <p><u>Additions to:</u></p> <ul style="list-style-type: none"> - Chapter 3 – Roles and Responsibilities. - Chapter 4 – BC Documentation and Records 	Doc-1313310 Revision 28	Drew Coleman