

Business Continuity Plan Template

Disaster Risk Management Authority | The Bahamas

Derived from the DRM Authority Business Continuity Planning Workbook



What this template helps you do

Bring together the principal decisions and arrangements developed through your Business Continuity Planning process into one practical plan that your business can approve, access, activate, maintain and test.

Use this template when...

- you are developing your first Business Continuity Plan;
- you need to consolidate work completed in the Workbook or Starter Kit tools;
- an existing plan is incomplete, outdated or difficult to use;
- roles, strategies or operating arrangements have changed; or
- you are preparing to exercise, review or approve the plan.

How to use the template

1. Complete Parts 1-4 to establish ownership, scope, review and activation arrangements.
2. Transfer final decisions on critical functions, recovery priorities, dependencies and strategies.
3. Confirm people, communication, supplier, technology, financial and recovery arrangements.
4. Attach detailed registers or tools where more information is needed.
5. Approve the plan, store it securely, test it and update it after change, exercise or disruption.

A useful Business Continuity Plan should be

PRACTICAL	ACCESSIBLE	CLEAR	REALISTIC	CURRENT AND TESTED
Built around arrangements the business can actually use.	Available even if normal premises, systems or people are unavailable.	Easy to understand, with responsibilities and actions stated plainly.	Proportionate to the business and supported by actual resources.	Reviewed, exercised and improved as the business changes.

What the completed plan contains

Parts 1-5	Parts 6-10	Parts 11-15
1. Business and Plan Information 2. Purpose and Scope 3. Ownership, Approval and Review 4. Activation and Deactivation 5. Critical Products, Services and Functions	6. Recovery Priorities 7. Dependencies and Vulnerabilities 8. Continuity Strategies 9. Roles, Authority and Succession 10. Employee Arrangements	11. Communications 12. Suppliers and External Dependencies 13. Technology, Data and Vital Records 14. Financial and Insurance Readiness 15. Testing, Review and Improvement

Important

Adapt this template to the size and complexity of your business. Protect personal, commercial and security-sensitive information. Do not record passwords, PINs or other security credentials in the plan; record only where authorized personnel can access them securely. A completed template does not guarantee continuity and is not a certification or audit.

PART 1 - Business and Plan Information

Business Name		Trading Name (if different)	
Primary Location		Other Locations	
Main Telephone		Website / Primary Digital Channel	
Owner / Senior Leader		BCP Owner	
Alternate BCP Owner		Number of Employees	

Plan control

Version	Date Developed	Date Approved	Last Review	Next Review	Last Exercise / Test	Next Exercise / Test

PART 2 - Purpose and Scope

Suggested purpose statement

The purpose of this Business Continuity Plan is to help [Business Name] maintain or restore its most important business functions when normal operations are disrupted.

Scope

State which locations, products, services, functions, teams and types of disruption are covered by this plan.

Exclusions or limitations

Record anything that is outside the current scope and any assumptions that must be addressed later.

PART 3 - Ownership, Approval and Review

Plan Owner		Approved By	
Approval Date		Secure Location of Master Plan	
Backup Access Method / Location		Person Responsible for Updates	

☐ Review every 6 months

☐ Review annually

☐ Review after a disruption

☐ Review after an exercise

☐ Review after major staff, supplier or system changes

☐ Other: _____

PART 4 - Activation and Deactivation

Not every incident requires full activation. Record who may activate and deactivate the plan, the conditions that may trigger action, and the first steps that should follow.

Activation and deactivation authority

Role	Primary Name / Position	Primary Contact	Alternate Name / Position	Alternate Contact
Authority to activate the plan				
Authority to deactivate the plan				

Scalable activation

Level	Type of Disruption	What It Means	Typical Response
Level 1	Limited Disruption	Handled through normal management or a specific workaround.	Activate only the relevant continuity arrangement.
Level 2	Significant Disruption	One or more critical functions are affected.	Activate selected parts of the BCP and coordinate updates.
Level 3	Major Continuity Event	Several critical functions or locations are affected.	Full BCP activation and sustained management may be required.

Activation triggers and initial actions

Trigger / Threshold / Condition	Initial Action	Activation Level	Authorized By	Next Review / Update Time
Premises unavailable				
Electricity outage				
Communications outage				
Critical system failure				
Supplier failure				
Staff unavailability				
Other: _____				

Deactivation condition

State how the business will decide that continuity arrangements may end and normal or recovery operations may resume.

PART 5 - Critical Products, Services and Functions

List the activities that must continue or be restored within a defined period because interruption would have serious consequences. Prioritize the functions that directly support essential products or services.

Priority	Critical Function	Product / Service Supported	Minimum Staff	Function Lead
1				
2				
3				
4				
5				
6				

PART 6 - Recovery Priorities

MAXIMUM ACCEPTABLE DOWNTIME The latest point at which interruption becomes unacceptable.		TARGET RECOVERY TIME The time by which the business aims to restore the function.		RECOVERY PRIORITY The order in which functions should be restored when resources are limited.
Critical Function	Main Impact if Unavailable	Maximum Acceptable Downtime	Target Recovery Time	Recovery Priority

Reality check

The Target Recovery Time should be earlier than the Maximum Acceptable Downtime and should reflect what the business can realistically achieve with the resources and strategies currently available.

PART 7 - Dependencies and Vulnerabilities

Summarize the people, places, systems, suppliers and services on which each critical function relies. Identify where one failure could stop the function because no suitable alternative exists.

Critical Function	Key Dependency	Main Vulnerability	Single Point of Failure? Y / N	Key Assumption

Dependency categories to check

PEOPLE Key staff, skills, decision-makers and authorized users.		PREMISES / EQUIPMENT Worksites, machinery, vehicles, tools and physical assets.		UTILITIES Electricity, water, Internet, mobile/telephone and payment systems.		TECHNOLOGY / DATA Systems, records, devices, backups and access.	
SUPPLIERS Critical goods, services and confirmed alternatives.		TRANSPORT / SHIPPING Ports, airports, freight, routes and inter-island movement.		FINANCE / BANKING Payments, payroll, banking access and emergency purchasing.		EXTERNAL SERVICES Regulators, landlords, professional services and outsourced providers.	
Detailed Dependency / SPOF Tool attached?		☐ Yes ☐ No ☐ Not required		Location / file reference			
Highest-priority vulnerability				Person responsible for follow-up			

Challenge the backup

A second supplier, location, device or communication channel is not a true alternative if the same disruption could disable both the primary arrangement and the backup.

PART 8 - Continuity Strategies

Record the practical arrangements the business will use to keep a critical activity operating, operate temporarily at a reduced level, restore it within the required timeframe, or provide an alternative until normal operations return.

Function / Vulnerability	Continuity Strategy	Activation Trigger	Resources Required	Owner / Alternate

Alternate operating location or arrangement

Primary Operating Location / Model		Alternate Location / Arrangement	
Trigger for Switching		How Access Will Be Obtained	
Maximum Capacity / Limitations		Person Responsible	

Minimum Viable Operations

Critical Function / Service	Minimum Output or Service Level	Minimum Staff	Essential Systems / Equipment	Maximum Duration at Reduced Level

Strategy test

A strategy is not complete until the business has confirmed that it is practical, timely, independent, accessible, sustainable, resourced, owned and tested.

PART 9 - Roles, Authority and Succession

A plan can still fail if people do not know who is in charge, who may make key decisions or who takes over when the primary person is unavailable.

Leadership succession

Primary Leader		First Alternate	
Second Alternate		Where Delegated Authority Is Recorded	

Alternate readiness

Naming an alternate is not enough. Confirm that each alternate has the authority, access, information, contacts and practical preparation needed to act.

Decision authority summary

Decision	Primary Authority	Alternate	Limits / Conditions	Access or Documentation Required
Activate the BCP				
Close operations				
Reopen				
Relocate / move to remote operations				
Approve emergency spending				
Change supplier				
Change staffing arrangements				
Release public information				

PART 9 - Roles, Authority and Succession (continued)

Continuity roles matrix

Responsibility	Primary	Alternate	Key Access / Information Required
Overall continuity coordination			
Employee accountability			
Critical operations			
Premises			
Technology and data			
Suppliers and logistics			
Finance and insurance			
Employee communication			
Customer / public communication			
Documentation and logs			
Recovery and reopening			

PART 10 - Employee Arrangements

Employee Accountability Lead		Alternate	
Primary Contact Method		Backup Contact Method	
Location of Employee Contact List		Method for Employees to Confirm Status	

Critical roles and backup coverage

Critical Role	Primary Person	Backup / Cross-Trained Person	Required Access / Skill	Current Gap or Action

PART 11 - Communications

Summarize the principal communication arrangements here. Keep the detailed Stakeholder Communications Matrix, message templates, cadence, trusted-source register and Communication Log in the Business Continuity Communications Pack.

Communication authority

Authorized Communicator		Alternate Communicator	
Message Approver		Alternate Approver	
Person Monitoring Questions / Rumours		Location of Communications Pack	

Audience and channel summary

Audience	What They Need to Know	Primary Channel	Backup Channel	Responsible Person
Employees				
Customers				
Suppliers				
Business partners				
Bank / insurer				
Government / regulator				
Public / media				

Official update arrangements

Primary Official Channel		Backup Official Channel	
First Update Target		Standard Update Frequency	
Where Contact Lists Are Stored		Next Scheduled Review of Channels	

Communication standard

Messages should be Accessible, Immediate, Frequent, Specific and Clear. Verify facts, protect sensitive information and state when the next update will be provided.

PART 12 - Suppliers and External Dependencies

Record the suppliers and external services required for critical products, services or functions. Confirm that alternatives are available, accessible and not exposed to the same disruption.

Critical Product / Service	Primary Supplier / Provider	Primary Contact	Alternate Supplier / Provider	Alternate Contact	Shared Dependency / Concern

PART 13 - Technology, Data and Vital Records

Critical System / Record	Primary Location	Backup / Alternative	Who Can Restore / Access?	Target Restoration Time	Last Test Date

Security note

Do not store passwords, PINs, recovery codes or other credentials directly in the BCP. Record where authorized personnel can securely access them, and make sure more than one authorized person can restore or access critical systems where appropriate.

PART 14 - Financial and Insurance Readiness

Record how the business will meet essential financial obligations and access recovery support when normal payment, banking or accounting arrangements are disrupted.

Financial Need	Current Arrangement	Backup / Alternative	Authorized Person	Access / Documentation Required
Payroll				
Supplier payments				
Emergency purchases				
Banking access				
Insurance claims				
Cash / liquidity				
Insurer		Policy Number / Reference		
Claims Contact		Secure Location of Policy Information		

PART 15 - Testing, Review and Improvement

☐ Employee notification	☐ Backup power	☐ Data restoration
☐ Remote work	☐ Alternate supplier	☐ Alternate location
☐ Tabletop exercise	☐ Payment / banking continuity	☐ Other: _____
Next Test / Exercise		Responsible Person
Planned Date		Date Plan Will Be Reviewed

Improvement actions

Lesson or Gap Identified	Corrective Action	Owner	Due Date	Status / Evidence

Keep the plan current

Review the plan after an exercise, disruption or major change in staff, suppliers, premises, systems or operating arrangements. Record version changes and confirm that all authorized users can still access the current plan.

APPENDIX A - Initial Activation Checklist

Use this checklist when the Business Continuity Plan or selected continuity arrangements are activated. Adapt the sequence to the disruption and record the person responsible, completion time and any required follow-up.

Business		Date / Time Activated		
Activated By		Activation Level	☐ Level 1 ☐ Level 2 ☐ Level 3	
Disruption		Next Review / Update Time		

Done	Activation Step	Responsible Person	Time Completed	Notes / Follow-Up
☐	Address immediate life-safety issues.			
☐	Assess which critical functions are affected.			
☐	Notify primary and alternate decision-makers.			
☐	Account for employees and issue initial instructions.			
☐	Activate the relevant continuity strategies.			
☐	Contact critical suppliers and external service providers.			
☐	Communicate with employees, customers and other priority audiences.			
☐	Notify insurer, bank or regulator where appropriate.			
☐	Begin decision, expenditure, event and communication logs.			
☐	Confirm Minimum Viable Operations and current service limitations.			
☐	Set and communicate the next review or update time.			

Record the event

Use the Continuity Event Log and Communication Log to document what happened, the decisions taken, who authorized them, messages issued and any follow-up required.

APPENDIX B - Business Continuity Quick Reference

Keep this page accessible to authorized personnel. It provides the most important information at a glance; it does not replace the full Business Continuity Plan.

Business		Plan Owner	
Authorized to Activate		First Alternate	
Employee Accountability Lead		Authorized Communicator	
Top Three Critical Functions	Top Three Vulnerabilities	Top Three Continuity Strategies	
1.	1.	1.	
2.	2.	2.	
3.	3.	3.	

Communication and operating arrangements

Primary Employee Communication Channel		Backup Employee Channel	
Primary Customer Communication Channel		Backup Customer Channel	
Alternate Operating Arrangement		Minimum Viable Operations	
Primary Critical Supplier Contact		Insurer / Claims Contact	
Secure Location of Full BCP		Next Review / Test Date	

Store the plan where you can reach it

Do not create a Business Continuity Plan that can only be accessed from the office that may be inaccessible, from the computer that may be damaged, through the Internet connection that may have failed, or by the person who may be unavailable.

Use and Reproduction Notice

Version 1.0 | September 2026

This tool has been developed by the Disaster Risk Management Authority (DRM Authority) of The Bahamas as part of its Business Resilience Programme and is provided to support practical business continuity and resilience planning.

Businesses and organizations may reproduce and adapt this tool for their own internal business continuity and resilience planning, provided that attribution to the DRM Authority and any applicable third-party acknowledgements are retained.

This tool, its templates, or any substantial portion of them may not be sold, rebranded, republished, incorporated into a commercial product, or used to deliver paid training, facilitation, consultancy or other commercial services without the prior written permission of the DRM Authority.

Use of this material does not imply endorsement, accreditation or certification by the DRM Authority. Third-party material, where identified, remains subject to the rights and terms of its respective owner.

Internal adaptation is permitted. Commercial reuse requires prior written permission.