ADDITIONAL BUSINESS RESILIENCE RESOURCE

Business Risk & Physical Protection Pack

Disaster Risk Management Authority | The Bahamas

Developed as part of the DRM Authority's Business Resilience Programme

What this pack helps you do

Identify and prioritize the hazards and disruptions most likely to affect your business, review the physical measures already in place, and convert the most important weaknesses into assigned risk-reduction actions. This pack contains the Risk and Hazard Assessment Template and the Physical Risk Reduction and Preparedness Checklist used by the Business Resilience Self-Assessment.

Use this pack when...

• you are completing the Business Resilience Self-Assessment or reviewing your preparedness;
• your premises, operations, equipment, stock or records may be exposed to physical hazards;
• your business has changed location, activities, equipment or operating arrangements; or
• you need to decide which practical risk-reduction actions should be completed first.

How to use the pack

1. Describe the business context and identify what is especially exposed.
2. Screen the hazards and disruptions that could affect operations.
3. Assess likelihood and consequence, then identify priority risks.
4. Complete the physical protection and preparedness checklists.
5. Assign actions, owners, dates and evidence of completion.
6. Transfer unresolved continuity gaps to the BCP, Strategy Planner or 30/60/90-Day Action Plan.

Key concepts

Hazard	Exposure	Existing control	Residual risk
An event or condition that could cause harm, damage or business interruption.	The people, premises, equipment, stock, systems or operations that could be affected.	A measure already in place to prevent, reduce or manage the effect of a hazard.	The risk that remains after existing controls are considered.

Important scope boundary

This pack is a planning aid. It does not replace structural, engineering, electrical, fire-safety, environmental, occupational health and safety, security, building-code or other professional assessment. Do not enter or work in an unsafe area. Follow instructions from emergency services, public authorities and qualified professionals.

For internal business continuity and resilience planning. Commercial use requires prior written permission.

1. Business Context & Exposure Snapshot

Document the operating context that shapes your risk. A hazard becomes more serious when the business is highly exposed, depends on one location or resource, or has limited time to recover.

Business information	Record
Business name	
Assessment owner / position	
Date completed / next review	
Main operating location(s)	
Critical products / services	
Top three critical functions	
Peak periods or deadlines	
Key external dependencies	

Exposure snapshot

Exposure area	Questions to consider	Business notes
Premises / location	What location features increase exposure? Consider coastal or low-lying areas, drainage, building condition, shared premises, access routes and nearby hazards.	
People	Which employees, customers, contractors or visitors could be affected, and what assistance or communication may be needed?	
Equipment / stock	Which equipment, stock, materials or records are difficult, costly or slow to replace?	
Utilities / services	Which operations depend heavily on electricity, water, fuel, Internet, telecommunications, transport or payments?	
Time / season	Which seasons, deadlines, events or operating periods make disruption more damaging?	

For internal business continuity and resilience planning. Commercial use requires prior written permission.

2. Hazard & Disruption Screening

Mark the events that could affect the business. Do not select everything automatically. Focus on credible exposures, past experience, near misses, location, operating model and the dependencies that matter most.

Weather & environmental hazards

☐ Hurricane, tropical storm or severe wind
☐ Heavy rainfall, flooding or water intrusion
☐ Storm surge or coastal inundation
☐ Lightning, extreme heat or drought / water shortage
☐ Wildfire, earthquake or other location-specific hazard

Premises, safety & security

☐ Fire, smoke or hazardous-material incident
☐ Roof, window, door or structural failure
☐ Restricted access, nearby incident or unsafe surroundings
☐ Theft, vandalism, burglary or deliberate damage
☐ Failure of refrigeration, ventilation or critical building systems

Utilities, technology & transport

☐ Electricity, water or fuel interruption
☐ Internet, mobile or telecommunications outage
☐ Banking, payment or point-of-sale disruption
☐ Road, port, airport, freight or inter-island disruption
☐ Technology, data or critical equipment failure

People, suppliers & external disruption

☐ Key employee or decision-maker unavailable
☐ Widespread staff shortage or public-health event
☐ Supplier, contractor or outsourced service failure
☐ Regulatory, inspection or public-service disruption
☐ Customer, community or market disruption affecting operations

Other business-specific hazards or disruptions

Hazard / disruption	Why it could affect this business	Include in detailed assessment?
		☐ Yes ☐ No
		☐ Yes ☐ No
		☐ Yes ☐ No
		☐ Yes ☐ No

Next step
Choose the hazards and disruptions that could create the most serious consequences or expose the most important functions. Carry those items into the Risk Prioritization Matrix and Priority Risk Register.

For internal business continuity and resilience planning. Commercial use requires prior written permission.

3. Risk Prioritization Method

Use the simple 1–4 scales below to compare risks consistently. This is a practical planning method, not a technical risk model. Adjust the discussion to the size, complexity and operating context of the business.

Likelihood

1 — Unlikely: Not expected in normal planning, but still possible.
2 — Possible: Could occur; limited history or credible exposure exists.
3 — Likely: Has occurred before or conditions make recurrence reasonably likely.
4 — Very likely: Expected, frequent, seasonal or already showing warning signs.

Consequence

1 — Limited: Minor interruption; manageable through normal procedures.
2 — Moderate: Noticeable operational or financial effect; short recovery effort required.
3 — Serious: Critical function affected, major loss, safety concern or prolonged recovery.
4 — Severe: Threat to life, major damage, extended closure or inability to meet critical obligations.

Risk score and planning priority

Multiply Likelihood × Consequence. Use the result as a discussion aid, then apply professional judgement. A safety or compliance concern may require immediate action even where the numeric score is lower.

Likelihood ↓ / Consequence →	1 Limited	2 Moderate	3 Serious	4 Severe
4 — Very likely	4 Planned action	8 High priority	12 Immediate priority	16 Immediate priority
3 — Likely	3 Monitor	6 Planned action	9 High priority	12 Immediate priority
2 — Possible	2 Monitor	4 Planned action	6 Planned action	8 High priority
1 — Unlikely	1 Monitor	2 Monitor	3 Monitor	4 Planned action

Priority rule
Do not rely on the score alone. Elevate any risk that could cause serious harm, stop a critical function before its recovery target, breach a legal or regulatory obligation, or disable both the primary arrangement and its backup.

For internal business continuity and resilience planning. Commercial use requires prior written permission.

4. Priority Risk Register

Assess the selected hazards in more detail. Record the controls already in place and the additional action needed to reduce the likelihood, consequence or exposure.

Ref.	Hazard / disruption	What could be affected?	Existing controls	L	C	Score	Priority	Additional action / owner / date
1								
2								
3								
4								
5								
6								

Carry forward the remaining risk

Risk reduction may not remove the hazard. Where important exposure remains, use the Continuity Strategy Planner to define the backup or alternative, the activation trigger, who decides and what must be arranged in advance.

For internal business continuity and resilience planning. Commercial use requires prior written permission.

5. Physical Risk Reduction & Preparedness Checklist — Premises and Site

Review the physical conditions that could increase damage, injury or interruption. Enter Y, P, N or N/A in the status column and record the action, owner and target date for any gap.

Status key: Y = Yes / in place P = Partly N = No / not in place N/A = Not applicable

No.	Preparedness check	Status	Action / owner / target date
1	Roof, doors, windows, shutters and other protective features are inspected, maintained and suitable for the principal hazards.		
2	Outdoor furniture, signs, waste containers, loose materials, trees and other potential projectiles are secured or can be moved safely.		
3	Drains, gutters, pumps, barriers and other water-control measures are maintained, and likely water-entry points are known.		
4	Critical stock, equipment and records are positioned or protected to reduce flood, leak, heat, smoke or impact damage.		
5	Emergency exits, access routes, assembly points and routes used by emergency services are clear and identifiable.		
6	Fire detection, warning and suppression arrangements are present, accessible, maintained and inspected as required.		
7	Electrical panels, wiring, outlets, surge protection and isolation arrangements are reviewed and maintained by qualified persons where required.		
8	Hazardous or flammable materials are identified, stored, labelled and handled in accordance with applicable requirements.		
9	Exterior and interior lighting, signage, handrails, floors and access areas are maintained to reduce injury and support safe movement.		
10	Access restrictions, security arrangements and landlord or shared-premises responsibilities are documented, current and understood.		

For internal business continuity and resilience planning. Commercial use requires prior written permission.

6. Physical Risk Reduction & Preparedness Checklist — Critical Operations and Resources

Check the practical measures that protect the resources needed to continue or restart operations. Use the dedicated continuity tools where a backup, alternate source or detailed operating arrangement is required.

Status key: Y = Yes / in place P = Partly N = No / not in place N/A = Not applicable

No.	Preparedness check	Status	Action / owner / target date
1	Backup power, generators, batteries or alternative arrangements are appropriate to critical loads and are maintained and tested by qualified persons.		
2	Fuel, water and other essential supplies are stored and managed safely, with replenishment and access arrangements documented.		
3	Critical equipment, spare parts, tools and vehicles are identified, protected and supported by repair or replacement options.		
4	Minimum stock levels, substitutes, storage conditions and reorder triggers are established for critical inventory and materials.		
5	Refrigeration, temperature control or other environmental requirements for stock and equipment are protected and monitored.		
6	Essential paper records, licences, contracts and contact information are protected and can be accessed if normal premises are unavailable.		
7	Communication devices, chargers, power banks, radios, emergency supplies and protective equipment needed during disruption are accessible and checked.		
8	Critical suppliers, transport routes and service providers have been reviewed for common points of failure and practical alternatives.		
9	Employees know immediate safety actions and information channels; inspection, maintenance and testing responsibilities are assigned; and defects, near misses and Lessons Identified are used to update arrangements.		

For internal business continuity and resilience planning. Commercial use requires prior written permission.

7. Inspection, Maintenance & Readiness Record

Use this record to show when protective measures were checked, what was found and whether corrective work was completed. Attach or reference supporting photographs, certificates, invoices or service records where appropriate.

Date	Item / area checked	Check performed by	Condition / finding	Action required	Owner / target date	Completion evidence / next check

Readiness review

Review question	Response / action
Which protective measure is most likely to fail when needed?	
Which gap could most seriously affect a critical function?	
Which action can be completed immediately at low cost?	
Which action requires specialist assessment, procurement or management approval?	
What will be checked again before the next high-risk period?	

For internal business continuity and resilience planning. Commercial use requires prior written permission.

8. Priority Risk-Reduction Action Plan

Convert the highest-priority findings into specific, assigned and verifiable actions. Do not record “monitor” or “fix” without stating what will be done, who owns it and how completion will be confirmed.

No.	Risk / gap addressed	Action	Priority	Owner	Target date	Status	Evidence of completion / review
1							
2							
3							
4							
5							
6							
7							
8							

Top three commitments

Commitment	Action	Owner	Target date	How we will verify
Within 30 days				
Within 60 days				
Within 90 days				

For internal business continuity and resilience planning. Commercial use requires prior written permission.

Review and approval

Prepared by	Reviewed by	Approved by	Next review / trigger

Review triggers
Review this pack after a disruption or near miss; when the business changes premises, equipment, suppliers or operations; before a high-risk season; when maintenance identifies a serious defect; or when new information changes the risk picture.

Use and Reproduction Notice

This business risk & physical protection pack 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 resource 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 resource, 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.