Business Continuity Toolkit

Risk Assessment
Methodology & Guide

March 2021

HALIFAX PARTNERSHIP

Welcome to the Business Continuity Toolkit

- The COVID-19 pandemic has shone a spotlight on how quickly things can change for a business.
- You never really expect the unexpected, so it's useful to plan ahead for change and crises.
- The Halifax Partnership has developed a Business Continuity Toolkit to help small- and medium-sized business plan for changes and crises, whether it is a pandemic or another type of disruption.

The Why, What and How of the toolkit

Why – The Halifax Partnership has prepared this guide to help small- and medium-sized business facing challenges in a time of crisis.

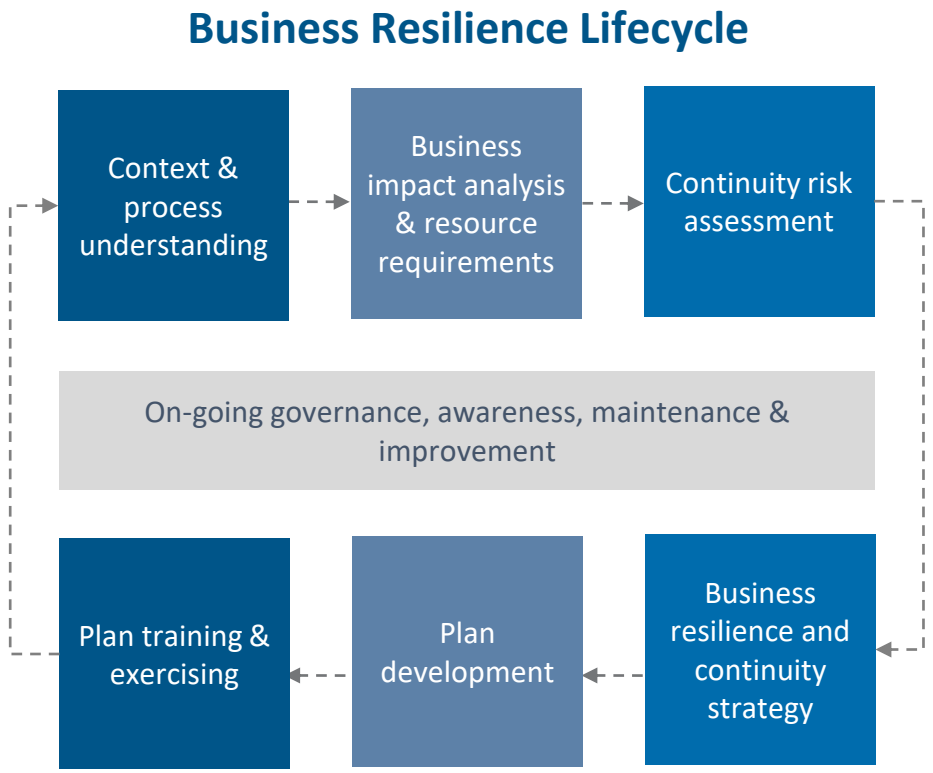
What – The toolkit is set of guides, templates, webinars and additional resources which will help businesses with planning and building resilience to prepare and respond to crises, whether it's a pandemic or any other critical challenge.

How – The toolkit has been designed for busy people who are juggling many challenges. It can be used to create a resilience plan to prepare for major disruptions and crises.

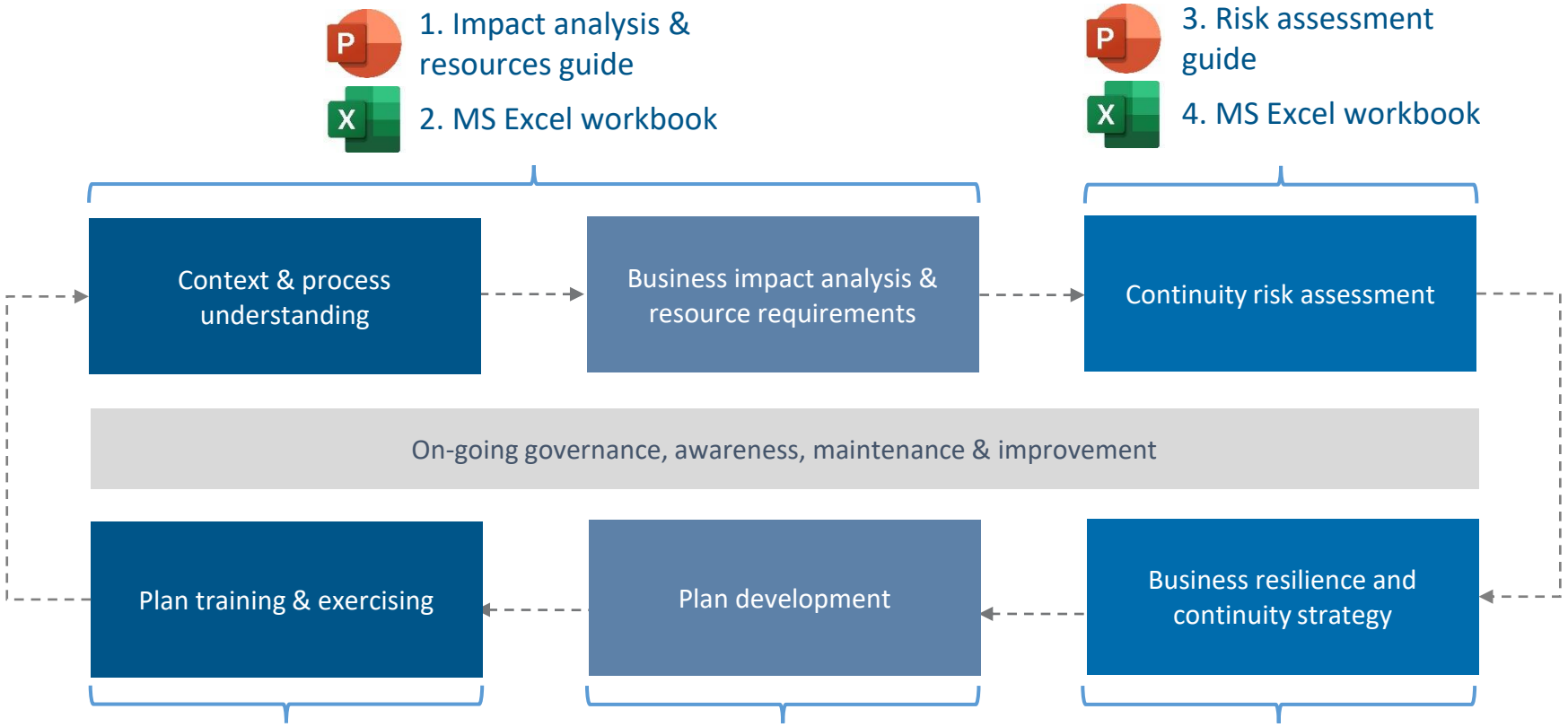
Business resilience overview

A business resilience program helps you to:

- Understand your business systems, supply chains, human resources and other types of critical resources
- Examine how each is affected by a disruption
- Develop responses to mitigate risks
- Communicate challenges and train teams
- Develop response plans
- Develop resilience and continuity plans and continue to revise and adapt them.



Toolkit components



14. Resources: examples of exercise scenarios and injects

8. Continuity plan development guide

9-12. MS Word plan templates

13. Resources: return-to-work checklist

5. Gap analysis & strategy guide

6. MS Excel workbook

7. Resources: examples of recovery alternatives

Webinar #1 – Business Resilience Basics

Webinar #2 – Business Resilience Lessons from the Pandemic

Webinar #3 – BCM Toolkit Walkthrough

Methodology

Business Continuity Risk Assessment

HALIFAX PARTNERSHIP

Risk Assessment Objective & Approach

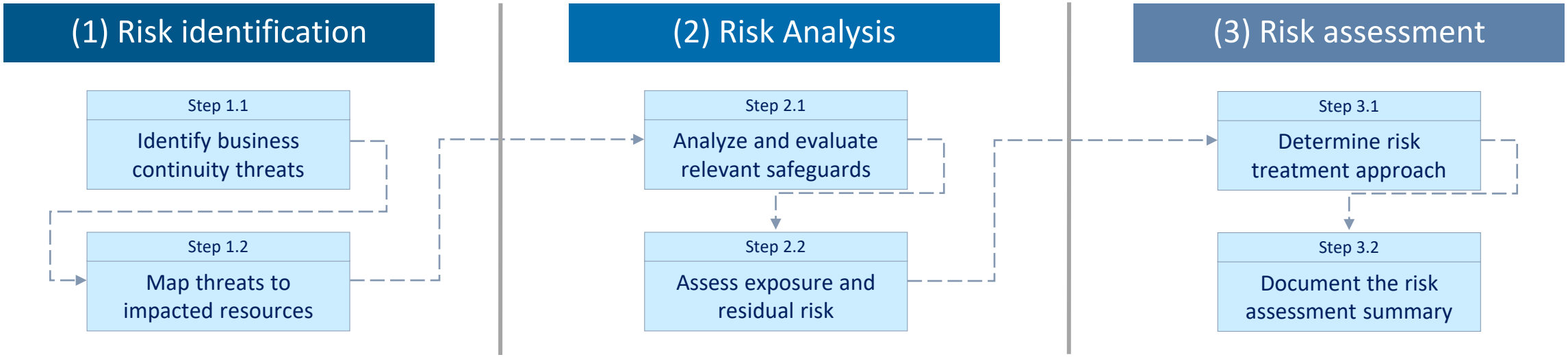
Objective

The Business Continuity Risk Assessment aims to identify, analyze and evaluate the risks of disruption to a business. This means analyzing threats and existing safeguards to determine the residual level of risk to your business.

Approach

The Business Continuity Risk Assessment focuses on the risks to critical processes that could result in a major disruption to your business. It considers safeguards currently in place to mitigate each risk.

The following process is followed:



Risk Assessment Approach

The Business Continuity Risk Assessment focuses on the risks to critical processes that could result in a disruption. It also considers safeguards currently in place to mitigate each risk.

The following steps are conducted:

(1) Risk identification

This step identifies events that may disrupt your critical business processes and highlights the impacted resources.

The business continuity threats are identified by the business head and managers. Members of this group have knowledge of every aspect of the business and the wider context of the market and industry.

(2) Risk Analysis

This step analyzes and evaluates safeguards currently in place to mitigate the impact or likelihood of threats. It also shows the residual exposure to each risks after existing safeguards are considered.

These insights are discovered in discussion-based workshops with the business head and managers.

(3) Risk assessment

This step determines the best response to each potential risk. These could include “avoiding”, “accepting”, “mitigating” or “transferring” the risk.

Risks that exceed the risk tolerance of the business must be mitigated or transferred.

The risk treatment is a key input for the overall continuity strategy, which focuses on selecting remediation and recovery solutions.

Step 1: Risk Identification

Threats that create business risk can be categorized as the following: deliberate, accidental and natural hazards.

The first step in the risk assessment is to identify threats to your business and determine which aspects of the business they may disrupt.

The business continuity threats are identified by the business head and managers who have overall knowledge of the business and industry context. A sample of these threats are presented below.

Deliberate threats	Accidental threats	Natural hazards
• Cyber-attack (sabotage such as ransomware) • Labor strike/protest • Physical vandalism/attack • Theft of critical assets	• Fire/explosion • Equipment/hardware malfunction • Power failure • Chemical/hazmat spill • Software malfunction • Supplier failure/bankruptcy • Industrial accidents	• Epidemic/pandemic • Snowstorm • Earthquake • Hurricane • Flooding/tidal wave • Extreme cold temperatures

Step 2: Risk Analysis

In this step, workshops are held with the business managers to analyze the disruption risks and threats identified in Step 1. Risks could affect key resources such as people, suppliers and facilities. The threats are mapped out to show which aspect of the business they impact.

Threats are analyzed based on two factors: “likelihood” of occurrence and “impact” on the business. Four factors are used to determine the impact and two factors are used to determine the likelihood.

“Likelihood and “Impact” of risks depend on existing safeguards which reduce the probability of a risk occurring or the impact if it does occur. These two factors are used to calculate the ‘residual risk’ level once existing safeguards are identified.

Residual risk levels are needed for the next step where they are used to select of risk treatment strategies.

Risk likelihood

The probability of a threat materializing and disrupting critical resources and processes (after considering existing safeguards)

X

Risk impact

The magnitude of damage or disruption that may be caused after a risk materializes (after considering existing safeguards)

=

Residual risk

The remaining potential exposure after existing safeguards and controls are taken into consideration

Risk Measurement Scale

Threats are analyzed based on probability and impact on resources and critical processes of the business. Impact is determined four factors: business impact, geographic extension, damage and recovery capability. The table below shows the factors which determine probability and impact of threats.

Rating	Impact				Probability	
	Business impact	Geographic extension	Damage	Recovery capability	Likelihood	Vulnerability
1	**Insignificant**	**Individual**	**Very Superficial**	**Very easy**	**Very Low**	**Very Low**
	No impact or affects only processes with recovery targets of > 1 month	Affects a portion of one site	No impact on equipment / workers / systems or <$10K in damages	Duration < 8 h	Extremely unlikely to occur but may do so in at least 5 years	Efficient controls implemented and monitored
2	**Low**	**Site**	**Superficial**	**Easy**	**Low**	**Low**
	Affects processes with recovery targets of < 1 week	Affects a single building	Affects few equipment / workers / systems or $10-$25K in damages	Duration 8-48 h	Likely to occur and may do so within the next 3-4 years	Efficient controls implemented, with some monitoring
3	**Moderate**	**Local**	**Moderate**	**Moderate**	**Moderate**	**Moderate**
	Affects processes with recovery targets of < 72 hours	Affects a site (e.g. adjacent buildings)	Affects a moderate amount of equipment / workers / systems or $25-100K in damages	Duration 48 h - 1 week	Likely to occur within the next 2 years	Some efficient controls implemented, but lack monitoring
4	**High**	**City**	**Structural**	**Hard**	**High**	**High**
	Affects processes with recovery targets of < 24 hours	Affects a city (e.g. Halifax)	Partial destruction of a building, major effect on workers and systems or $100-500K in damages	Duration 1 week - 1 month	Likely to occur within the next 6-12 months	Ad-hoc controls implemented
5	**High**	**Regional**	**Total destruction**	**Very difficult**	**High**	**High**
	Affects processes with recovery targets of < 4 hours	Affects the whole province	Total destruction of a building, catastrophic effect on workers and systems or >$500K in damages	Duration > 1 month	Very likely to occur within the next 1-3 months or is occurring at present	No controls implemented

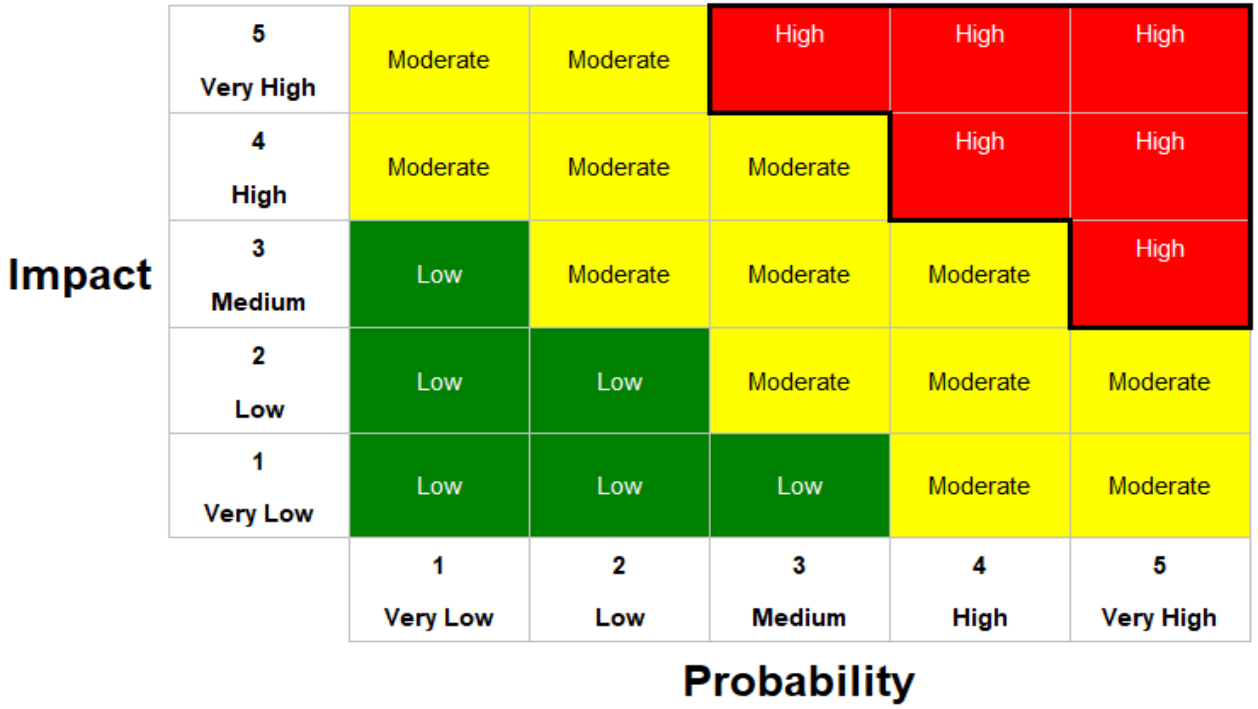
Risk Scoring

Residual risk scores are based on the product of the highest impact rating and highest probability rating for each threat, which are assigned after relevant safeguards are considered.

Risk scores are classified as follows:

- Risk scores of 1-4 without any ‘4-high' ratings are considered “Low”
- Risk scores of 5-14 are considered “Moderate"
- Risk scores of 15-25 are considered “High”

The diagram to the right illustrates the risk scoring matrix:



Step 3: Risk Assessment

Once the risk analysis is conducted and the residual risk levels are determined, businesses must select their response for all risks. These include:

- Avoid business activity: if the risk cannot be addressed or accepted due to exposure level, you may choose to avoid the high-risk business activity altogether.
- Accept the risk: if the risk is within your risk tolerance threshold, the risk can be accepted and treated at a later stage through risk reduction efforts. Risk acceptance must be formally documented by the person responsible for protecting the impacted resources.
- Mitigate the risk: risks that exceed your risk tolerance threshold must be mitigated or transferred. Risk mitigation includes implementing additional safeguards to reduce the likelihood and impact of a risk. The safeguards are analyzed and selected in the business continuity strategy.
- Transfer the risk: you may choose to transfer risks that would otherwise be uneconomical to mitigate internally. This may be achieved through approaches such as obtaining insurance or engaging third party outsourcers to carry part of the risk.

The risk treatment approach for risks to be mitigated or transferred serves as a key input into the business continuity strategy, which focuses on selecting remediation (pre-disruption) and recovery (post-disruption) solutions.

Guide

Business Continuity Risk Assessment

HALIFAX PARTNERSHIP

Risk Assessment Guide

You will find the following table in the first tab of the risk assessment workbook:

Identify credible threats to your resources & determine which resource types they may disrupt.

Identify the resources (people, facilities/workplaces, technologies, third parties, specialized equipment and inventory) that might be impacted by each threat.

For each identified threat, analyze and document controls and safeguards currently in place.

Assess if the controls and safeguards are working effectively. This aims to reduce the probability of a risk occurring and/or reduce the implications (impact) if the risk does materialize.

Threat #	Threat category & name		Impacted resource types	Existing controls & safeguards	Effectiveness of controls & safeguards
1	Deliberate threats	Cyber-attack (sabotage such as ransomware)	Technology systems	Antivirus, email & web filtering, internal network monitoring, firewalls and network security devices, user security awareness training	Adequate
2		Labor strike/protest			
3		Physical vandalism/attack			
4		Theft of critical assets			
5		<Other>			
6		<Other>			
7	Accidental threats	Fire / explosion			
8		Equipment/hardware malfunction			
9		Power failure			
10		Chemical/hazmat spill			
11		Software malfunction			
12		Supplier failure/bankruptcy			
13		Industrial accidents			
14		<Other>			
15		<Other>			
16	Natural hazards	Epidemic/pandemic			
17		Snow storm			
18		Earthquake			
19		Hurricane			
20		Flooding / tidal wave			
21		Extreme cold temperatures			
22		<Other>			
23		<Other>			

Risk Assessment Guide

You will find the following table in the first tab of the risk assessment workbook (continued from the previous section):

Rate the risk impact level by specifying a number from 1- 5 for each category (business impact, geographic extension, damage and recovery capability). This residual risk should be rated after current safeguards have been applied.

Rate the probability of each threat occurring from 1-5 through the likelihood of it occurring in the next time periods and your vulnerability based on the current safeguards.

This section includes formulas which will automatically calculate the residual risk rating by multiplying maximum impact and maximum likelihood for each risk.

Residual risk impact				Residual risk likelihood		Risk impact (numeric)	Risk likelihood (numeric)	Residual risk rating	Risk level
Business impact	Geographic extension	Damage	Recovery capability	Likelihood	Vulnerability				
2	1	2	2	2	2	2	2	4	Moderate Risk

The residual risk level is automatically classified as Low, Moderate or High based on the calculated risk score. Risks with a score of 1-4 are considered “Low”, a score of 5-14 with are considered “Moderate“, and a score of 15-25 are considered “High”.

Next steps

Once the risk assessment is complete, the following next steps should be taken to determine the risk treatment approaches:

1. Review the results with the management team to ensure alignment of the identified risks.

2. Obtain sign-off on the results from supervisors/management.

3. Proceed to the next step: business continuity gap analysis and strategy.

Halifax Partnership Resources:

halifaxpartnership.com/how-we-help/grow-your-business/

Minder Singh

msingh@halifaxpartnership.com

Hector Fraser

hfraser@halifaxpartnership.com

Jason Guidry

jguidry@halifaxpartnership.com

HALIFAX PARTNERSHIP

Thank you.

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

HALIFAX PARTNERSHIP