e - VM GLOBAL CONSULTING

2021

MSME – BUSINESS EVALUATION

BUSINESS CONTINUITY PLAN

Victor Nieto
e-VM Global Consulting
8 Wattle Bark Place,
MELTON, VIC 3337
Australia

Copyright

Except for the images contained in this document, this work is © e-VM Global Consulting 2021.

You may download, display, print and reproduce this material in unaltered form only for your personal, non-commercial use or use within your organisation for the purposes of the Micro, Small and Medium Enterprises (MSME).

Apart from any use as permitted under the Copyright Act 1968, all other rights are reserved.

Use of all or part of this material must include the following attribution:

"© e-VM Global Consulting 2021."

This document must be attributed as [MSME – Business Evaluation: Business Continuity Plan].

Any enquiries concerning the use of this material should be directed to info@evmglobalconsulting.com.au or:

e-VM Global Consulting
8 Wattle Bark Place
MELTON, VIC. 3337
Australia

Images

©2021 e-VM Global Consulting

Acknowledgements

The e-VM Global Consulting is an Australian Business that provide business consultancy to Medium, Small, and Medium Enterprises (MSME)

Disclaimer

While the e-VM Global Consulting and its contributors have attempted to ensure the material in this booklet is accurate at the time of release, the booklet contains material on a range of matters that are subject to regular change.

No liability for negligence or otherwise is assumed by the e-VM Global Consulting or its contributors should anyone suffer a loss or damage because of relying on the information provided in this booklet.

BUSINESS CONTINUITY PLAN

"Is the process of creating systems of prevention and recovery to deal with potential threats to a company. In addition to prevention, the goal is to enable ongoing operations before and during execution of disaster recovery.

An organization's resistance to failure is "the ability ... to withstand changes in its environment and still function". Often called resilience, it is a capability that enables organizations to either endure environmental changes without having to permanently adapt, or the organization is forced to adapt a new way of working that better suits the new environmental conditions." [From Wikipedia, the free encyclopedia].

TYPES OF INCIDENTS:

The NHS England Emergency Preparedness, Resilience and Response Unit define the types of incidents as follow:

"The following list provides commonly used classifications of types of incident. This list is not exhaustive and other classifications may be used as appropriate.

The nature and scale of an incident will determine the appropriate Incident Level.

- ➢ *Business continuity/internal incidents – fire, breakdown of utilities, significant equipment failure, hospital acquired infections, violent crime,*
- ➢ *Big bang – a serious transport accident, explosion, or series of smaller incidents,*
- ➢ *Rising tide – a developing infectious disease epidemic, or a capacity/staffing crisis or industrial action,*
- ➢ *Cloud on the horizon – a serious threat such as a significant chemical or nuclear release developing elsewhere and needing preparatory action,*
- ➢ *Headline news – public or media alarm about an impending situation, reputation management issues,*
- ➢ *Chemical, biological, radiological, nuclear and explosives (CBRNE) – CBRNE terrorism is the actual or threatened dispersal of CBRN material (either on their own or in combination with each other or with explosives), with deliberate criminal, malicious or murderous intent,*
- ➢ *Hazardous materials (HAZMAT) – accidental incident involving hazardous materials,*
- ➢ *Cyber Attacks – attacks on systems to cause disruption and reputational and financial damage. Attacks may be on infrastructure or data confidentiality,*
- ➢ *Mass casualty – typically events with casualties in the 100s where the normal major incident response must be augmented with extraordinary measures"*

Source of Information:

https://www.england.nhs.uk/wp-content/uploads/2015/11/eprr-framework.pdf

DEVELOPING A BUSINESS CONTINUITY PLAN – FRAMEWORK

Queensland Government on its "Business Continuity Template" [Publication attribution: Employment, Small Business and Training, Queensland Government, Business Continuity Planning template, licensed under Creative Commons Attribution 4.0 sourced on 26 April 2020] incorporate on their template the PPRR Framework (Prevention, Preparedness, Response and Recovery) providing a clear understanding of the Business Continuity Planning Process.

❖ Prevention - Risk Management planning
  - Incorporates the Prevention element that identifies and manages the likelihood and/or effects of risk associated with an incident.
❖ Preparedness – Business Impact Analysis
  - Incorporates the Preparedness element that identifies and prioritises the key activities of a business that may be adversely affected by any disruptions.
❖ Response – Incident Response planning
  - Incorporates the Response element and outlines immediate actions taken to respond to an incident in terms of containment, control, and minimising impacts.
❖ Recovery - Recovery planning
  - Incorporates the Recovery element that outlines actions taken to recover from an incident to minimise disruption and recovery times.

Source of Information:

https://www.publications.qld.gov.au/dataset/business-continuity-planning-template/resource/63f7d2dc-0f40-4abb-b75f-7e6acfeae8f3

BUSINESS CONTINUITY PLAN

Company Name:

_____

Address:

_____

___

City: _____ Postcode: _____

Phone: _____ Fax: _____

Email: _____ Website: _____

Contact Person:_____ Position: _____

Date: _____

Document Classification: *CONFIDENTIAL*

Electronic Copy Storage:

Document Version Control

Document Name:	Business Continuity Plan
Document Status	Draft
Version Number:	1.01
Date:	
Author:	
Authorized by:	
Distribution:	Limited Distribution List

Change History

Version	Issue Date	Author	Reason for Change
1.01			First draft

<u>CRISIS MANGEMENT TEAM:</u>

List the name of your Business Continuity Plan, to whom they will report and emergency contact details

NAME	LOCATION	REPORT TO	PHONE	EMAIL

RELATED SYSTEMS AND PROCEDURES:

List the related Systems and Procedures, Type of Document and its Electronic/Hard Copy Location

For Example:

- Document Name: Fire Evacuation

- Type of Document: Emergency Document

- Location: Describe where can find the Electronic Copy and or the Hard Copy

DOCUMENT NAME	TYPE OF DOCUMENT	LOCATION

EMERGENCY CONTACT DETAILS:

SUPPLIER	COMPANY	CONTACT	PHONE
Building Owner			
Carpenter/Handyman			
Cleaner			
Electrician			
Gas Supply			
Heating & Aircon			
Insurance Broker			
Internet Service Provider			
ICT Contractor			
Locksmith			
Mail/Courier			
Plummer			
Power Supply			
Security Monitoring			
Telephone Maintenance			
Telephone Company			
Water Supply			
Website Hosting & Support			

CONTINUITY, INTERRUPTIONS, EMERGENCIES OR DISASTERS?

Many organizations have *Disaster Recovery Plans*. We prefer the term *Business Continuity Plan* because it includes not only major disasters (e.g. Total loss of a building) but also routine interruptions to service (eg. The computers are down for half an hour). It puts disaster planning in perspective and makes it more likely that disasters or problems will be handled smoothly.

OBJECTIVES:

The objectives of this plan are:

- To ensure that maximum possible service levels are maintained
- To ensure that we recover from interruptions as quickly as possible
- To minimize the likelihood and impact (risk) of interruptions

PRINCIPLES:

The principles behind this plan are:

- Disaster Recovery is just part of Business Continuity
- Risks are assessed for both probability and business impact
- Business continuity plans must be reasonable, practical and achievable

In other words, we are not planning for *every* possibility. Diminishing returns affect the benefits of planning for extreme cases.

FUNCTIONS VERSUS CAUSES:

We have developed this plan by analysing what is being interrupted, rather than why. For example, the building may be unavailable for many reasons – but in terms of its impact on the operations and services of the [YOUR COMPANY NAME}, it matters not whether the cause is a contaminated aircon unit, a security scare or a major traffic accident (or worse).

Obviously, the Company will manage each differently, depending in some cases on the cause, but for our more specific purposes, the building is simply unavailable.

PRECEDENCE:

The Company's general, security and IT procedures override these instructions if there are any conflicts.

FUTURE CHANGES:

These plans will change in response to new business and client needs and new technology. Please refer all requests for changes to the [PERSON IN CHARGE}

LAYOUT AND USE:

This document is designed to be viewed as a PDF or on paper, and so that it is easy to add new sections and to extract subsets. Where possible, topics are not longer than one page. In the printed version, topics are arranged alphabetically. For each Risk we set out:

- *Likely Scenario* – the most likely reasons for problems to occur
- *Probability* – the likelihood of the risk occurring (high, medium, low)
- *Impact* – will the impact on our business be high, medium or low?
- *Functions Affected* – what document-related functions the problem impacts
- *Action* – what to do when the interruption occurs
- *Responsibilities* – who takes what actions
- *Mitigation* – what is the Company doing to minimize the risk before it happens
- *Constraints* – the practicalities of dealing with the risk
- *Resources* – the implications for costs, staffing, facilities etc.

COMMUNICATION:

Whenever we say *contact* or *advise staff*, this will usually be done by email, phone, paging system or in person to all affected staff.

COMPANY CONTACTS:

NAME	POSITION	CONTACTS	OTHER CONTACT

RISK ASESSMENT PLANNING:

CAN'T FIND WHAT YOU WANT?

If you cannot find a risk that exactly matches the incident that you are managing, look for a similar risk and use that as a model. For example, if you are using Microsoft Excel, and it crashes, you could follow the instructions for *Software – XXXX System Down*.

DURING EACH INCIDENT:

At all stages keep any affected area or person closely advised of progress – even negative progress.

Do not hesitate to advise a manager or the CEO of the incident and of progress.

If any incident could be possible involve the public, immediately contact any available manager or the CEO.

AFTER EACH INCIDENT:

After each incident, a standard set of tasks must be done. These have not been repeated under each risk, but they must still be done:

- ➤ Return all operations and services to their original form
- ➤ Contact all those affected and suppliers, to advise them that the incident is over, and things are back to normal
- ➤ **Thank Everyone** involved, preferably by personal phone call or email
- ➤ Review the way we managed the incident and consider if we need to change anything – if so, change it in this document too.

What next?

Now is your company time to create the business Risk management plan.

DISCLAIMER:

The information provided in this document is **<u>General Information Only</u>** and does not take account of your COMPANY financial situation or needs.

You should look at your own company financial position and requirements before deciding.

You may wish to consult a professional and qualified adviser when doing this.

You should be aware that the value of your investment may rise or fall.

Past performance is not a reliable indicator of future performance, especially considering current global crisis.

As this information is only a guide and general information based on your self-assessment e-VM Global Consulting does not take **ANY** responsibility for any decision making on this document and information.

Before to make any decision, you should consult with a professional and qualified adviser to provide options for your company issues.

For your company assessment, please contact us for a free consultation via zoom or any other
video-conference tool, on:

e-VM Global Consulting
8 Wattle Bark Place
MELTON, Vic. 3337, Australia
Phone: +61425 701 113
Fax: +613 9747 9055
Email: info@evmglobalconsulting.com.au