Test Valley Limited

Crisis & Risk Management Plan

Overview

This document describes:

1) Activities to minimise the likelihood and impact of a crisis event affecting the company
2) Activities to minimise the likelihood and impact of a crisis event affecting the company having a knock-on effect to its customers
3) Instructions on what to do in the event that the company is affected by a crisis event.

Next Review Due: July 2019

This document is version controlled.

Version Control and Amendment History

Version Number	This external facing document is adapted from V1.0 of master.

Contents

1.0 Introduction and Overview

A crisis is a LOW PROBABILITY, HIGH IMPACT event. It can cause a lot of damage to a company. The management team has carried out procedures across the company identify threats to assets and functions, and has assessed our exposure to risk. Disruptions come in all shapes and sizes, and no organisation is immune. Examples of causes of disruption that could affect our business are fires, floods, technology failure, supply chain failure and business crime. On a wider scale, as we often see in the press, events such as terrorism, pandemics and fuel protests do occur.

Through Risk Assessment, the business seeks to minimise the likelihood of such incidents occurring; however if they do occur, then the consequences could affect:

- Buildings and facilities
- Staff
- Technology and communications
- Data
- Supply Chain
- Equipment

The above assets are valuable to a business, and if one or more of these assets were affected then the smooth running of our business, and our customers' businesses, could be at risk.

2.0 Objective

The Crisis & Risk Management Plan will:

- Define and prioritise the critical functions within the business
- Analyse the risks of partial or total failure of the business's critical functions
- Detail the agreed response to a crisis
- Identify key contacts during a crisis

3.0 Management Statement

This plan will be reviewed regularly to ensure that all critical aspects of the company's work and activities are recoverable or transferable within 24 hours.

In the event of any of the procedures described in this plan being amended, it is the responsibility of each manager to inform the plan author of the necessary amendments to the plan, which will then be incorporated and distributed to all plan holders.

4.0 Executive Summary

Test Valley Ltd is in a strong position to cope with a crisis. In particular, the business operates from three separate buildings, has back-up office space available, and operates multiple vehicles. These facilities will help ensure the business's continued operation in the event of a physical crisis. To ensure continued supply to our customers in the event of a crisis, key products are stored across at least two buildings.

The key crisis risks identified are:

- Fire
- Flood
- Loss of Utility Services
- Loss of Telecommunications Services
- IT Failure
- Data Loss
- Data Breach
- Logistics Interruption
- Staff Unavailability
- Exceptional Demand
- Supply Chain Failure
- Customer Arrears
- Criminal Activity

5.0 Risk Assessment

This section shall assess each of the key crisis risks identified by Test Valley Ltd. Risks are categorised as per the matrix below.

Risk Matrix

Risk Impact	---------- Risk Score ----------		
HIGH = Unmanaged, this event could halt or significantly constrain business operations for more than four hours	**MEDIUM**	**HIGH**	**HIGH**
MEDIUM = Unmanaged, this event could halt or significantly constrain business operations for up to four hours	**LOW**	**MEDIUM**	**HIGH**
LOW = Unmanaged, this event would be inconvenient to the business but most operations could continue as normal	**LOW**	**LOW**	**MEDIUM**
Risk Likelihood	LOW = event expected to occur less than once every ten years	MEDIUM = event expected to occur once or more every five to ten years	HIGH = > event expected to occur once or more every five years

5.1 Fire

Crisis Type	Likelihood	Impact	Risk Score	Risk Management
FIRE	**LOW**	**HIGH**	**MEDIUM**	To minimise the likelihood and impact of a fire event, fire regulations are fully complied with, these include fire detection equipment, fire-fighting equipment and evacuation plans. A monitored fire alarm is operational at all times.

5.2 Flood

Crisis Type	Likelihood	Impact	Risk Score	Risk Management
FLOOD	**LOW**	**MEDIUM**	**LOW**	None of our buildings are in designated flood plain areas but all are located close to local rivers that are flow managed. With regard to internal pipework, heating is left on during cold weather to reduce the likelihood of pipes freezing.

5.3 Loss of Utility Services

Crisis Type	Likelihood	Impact	Risk Score	Risk Management
LOSS OF UTILITY SERVICES	**LOW**	**HIGH**	**MEDIUM**	The likelihood of utility services being unavailable is considered to be low. A battery back-up supply provides sufficient electricity to allow IT equipment to be shut-down in a controlled manner, thus reducing the likelihood of long-term damage to IT infrastructure and systems resulting from sudden power loss.

5.4 Loss of Telecommunication Services

Crisis Type	Likelihood	Impact	Risk Score	Risk Management
LOSS OF TELECOMM SERVICES	**LOW**	**MEDIUM**	**MEDIUM**	Back-up analogue telephone line is available for telephone call redirection. Mobile phones are also available as back-up. A back-up broadband service is available.

5.5 IT Systems Failure

Crisis Type	Likelihood	Impact	Risk Score	Risk Management
IT FAILURE	**LOW**	**HIGH**	**MEDIUM**	As per most businesses, IT is central to our business operations. To minimise the impact of any IT failure, we have back-up procedures in place for key operations. Our IT systems and infrastructure are fully supported by third parties. We regularly upgrade our software and maintain robust IT firewalls to help prevent virus attacks. In the event of IT server failure, a new server can be acquired and set up within a few hours. Our server configuration is backed-up each hour.

5.5 Data Loss

Crisis Type	Likelihood	Impact	Risk Score	Risk Management
DATA LOSS	**MEDIUM**	**MEDIUM**	**MEDIUM**	Data Loss relates to data that has been deliberately or inadvertently deleted or corrupted, or data that has been erroneously or maliciously changed to an incorrect value. Staff training is in place to minimise errors when modifying data, and processes are in place to manage situations where there is a concern regarding the possibility of malicious activity. All server data is backed up each hour, and separately each day.

5.6 Data Breach

Crisis Type	Likelihood	Impact	Risk Score	Risk Management
DATA BREACH	**MEDIUM**	**MEDIUM**	**MEDIUM**	Data Breach relates to business data that has been deliberately or inadvertently released to a third party. Breaches that include personal data are covered by the General Data Protection Regulations. The company has procedures in place to ensure its adherence to these regulations.

5.7 Logistics Interruption

Crisis Type	Likelihood	Impact	Risk Score	Risk Management
LOGISTICS INTERRUPTION	**LOW**	**MEDIUM**	**LOW**	There are multiple access routes into the industrial estate where our buildings are located. However, only one of these routes is suitable for large, high vehicles. Any closure to this route is likely to be short-lived due its commercial importance. However, in the event of this route being closed smaller vehicles from within our fleet would be used for deliveries, supported by third party carriers as necessary. In the case of a fuel shortage, the company has access to a secure road-fuel store. All company vehicles are regularly serviced to ensure legal compliance and to carry out preventative maintenance. Older vehicles are regularly replaced to ensure that the company maintains a modern, reliable fleet.

5.8 Staff Unavailability

Crisis Type	Likelihood	Impact	Risk Score	Risk Management
STAFF UNAVAILABILITY	**LOW**	**MEDIUM**	**LOW**	Business critical role knowledge is shared between multiple team members to ensure that business functions can continue as normal in the case of staff unavailability. To avoid the risk of spreading illness, staff are requested to remain offsite until fully recovered from any debilitating contagious infection.

5.9 Exceptional Demand

Crisis Type	Likelihood	Impact	Risk Score	Risk Management
EXCEPTIONAL DEMAND	**MEDIUM**	**MEDIUM**	**MEDIUM**	Stock management procedures are in place to track and forecast stock usage levels and ensure plentiful and timely stock replenishment. Year-on-year volumes are monitored to forecast peak trends, and customer consultation is undertaken to understand volumes for new lines, and seasonal usage variations.

5.10 Supply Chain

Crisis Type	Likelihood	Impact	Risk Score	Risk Management
SUPPLY CHAIN FAILURE	**MEDIUM**	**MEDIUM**	**MEDIUM**	For key stock lines, the company has a policy of having multiple suppliers to reduce the likelihood of supply problems. Key suppliers are included on the company's Approved Suppliers List. Unsatisfactory suppliers are removed from this list.

5.11 Customer Arrears

Crisis Type	Likelihood	Impact	Risk Score	Risk Management
CUSTOMER ARREARS	**MEDIUM**	**LOW**	**LOW**	Credit accounts are only made available to customers that have passed credit worthiness tests as dictated by our credit insurer. Credit limits are set in accordance with insurable maximums.

5.12 Criminal Activity

Crisis Type	Likelihood	Impact	Risk Score	Risk Management
CRIMINAL ACTIVITY	**LOW**	**MEDIUM**	**LOW**	Fraud, theft and criminal damage are considered the most likely criminal actions to affect the company. To minimise fraud, the company does not accept ad-hoc card payment orders and has robust card handling processes in place. Company premises are protected by intruder alarms including perimeter alarms and internal motion sensors. All key external locations are floodlit and monitored by CCTV. External doors are of steel construction with high security locks. Ground floor windows are protected by security shutters. Small vehicles are parked undercover at night and large vehicles are kept in a secure compound. All vehicles have tracking devices fitted.

6.0 Business Asset Crisis Tolerance Assessment

This section shall assess each of the crisis tolerance of key business assets i.e. the extent to which the business could cope with the loss of each asset in the event of a crisis.

Business Asset	Tolerance	Tolerance Description
SERVER **BROADBAND**	**CRITICAL**	Crisis tolerance is very low, cost of interruption is very high, impacted business functions could not be performed, and extensive post-event catching-up would be required.
KEY OFFICE SYSTEMS **TELEPHONE SYSTEM**	**VITAL**	Crisis tolerance is low, cost of interruption is high, impacted business functions could be manually performed for a short period, and significant post-event catching-up would be required.
PRINTERS **COMPUTERS (PC/LAPTOP)** **DELIVERY VEHICLES** **FIELD SALES VEHICLES** **FORKLIFTS**	**SENSITIVE**	Crisis tolerance is high, cost of interruption is low, affected business functions could be manually performed, and some post-event catching-up would be required.
PHOTOCOPIER **FAX MACHINE**	**MINIMAL**	Crisis tolerance is very high, cost of interruption is very low, impacted business functions could be manually performed, and minimal post-event catching-up would be required.

7.0 Company Operations - Back Up Summary

Business Function	
Who is dependent on this function?	Customers Customer Services Operations Purchasing Accounts Directors
What activities does this function carry out?	Stock Management Sales Processing Purchasing Administration Logistics
Who is responsible for this function?	Company Directors
What facilities are required to deliver this function?	Office Space Warehousing Vehicles
What would be the impact if this function failed for 24 hours?	Potential for delays to customer orders and stock replenishment.
Current Location	Offices - Unit 1 Watt Road, Salisbury, SP2 7UD Warehouses – Multiple sites used
Back-up Location	Offices - Unit 2, Watt Road, Salisbury, SP2 7UD plus offsite offices Warehouses – Multiple sites available

8.0 Crisis Procedure

This section includes information pertaining to the procedure to be followed in the event of a crisis.

8.1 Crisis Communication Procedure

This section illustrates the process to be followed in the event of a crisis.