Keep Trading – Discussion Briefing

Introduction

This is one of a number of documents to help owners and managers in small and medium sized businesses who want to think about how to protect their businesses from disruptions, small or large, natural or man-made. They can be seen as a practical introduction to managing business continuity, or how to 'keep trading' when trouble strikes.

The Ready Scotland website provides further information and links for those wishing to go further and for firms with more complex needs, such as larger businesses.

Keep Trading – Discussion Briefing

The *Discussion Briefing* (this document) is intended to help owners and managers of small and medium sized businesses discuss with colleagues how to protect their businesses from disruptions: how to 'keep trading'.

Keep Trading – Discussion Record Sheets

The *Discussion record sheets* are forms to record the outcomes of meetings based on the *Keep Trading – Discussion Briefing*. They can be used as the basis of a draft business continuity plan.

Keep Trading – Checklist

The *Checklist* is a two page list of hazards that might affect small businesses and questions to ask about your ability to get back to business as normal.

Discussion Briefing - Managing Disruptions to Business

*The output from these discussions can be recorded on the **Keep Trading Discussion Record Sheets***

1 Disruption of normal business

- Things happen to interrupt business
  - *Short term – staff off due to illness; failure of electricity, sewage etc*
  - *Large scale, longer term – flood or fire, building unusable for weeks; loss of data; business failure in major trading partner*
- We are not immune
- There are things we can do to help ourselves
  - *Emergency services may be busy elsewhere*
  - *May be a commercial issue*

2 Outputs for Today

- Understand where our business might be vulnerable
- Identify ways to make us more resilient:
  - *Reduce chance of trouble*
  - *Reduce the impact if it does happen*
- Think about how we would respond to an emergency

There may be other benefits, e.g. greater focus on business priorities, ideas about leaner ways of working, team building.

3 Understand where our business might be vulnerable

- Being clear about what we do, and how we do it, helps to identify what could go wrong.

4 *What?* and *What if?*

- What do we make / do / output?
  - *What are our priorities?*
- What do we need to do this?
- What could go wrong?
- How can we make it less likely?
- What can we do to put it right?

5 What is our business about?

- What would we most want to preserve about our business following a disaster?
- What do we offer our customers and trading partners?
- What makes us distinctive?
    - *Core products vs. secondary outputs*
    - *Reputation and brand*

6 What do we need to continue our core business?

- People – our staff
    - *Different roles and skill mix*
    - *How many people?*
    - *Which locations?*
    - *Special authority*
    - *Relationships with customers, suppliers etc*
- Premises
    - *Buildings, facilities*
    - *Utilities: light, heat, power etc*
- Equipment
    - *Large and small items*
    - *Consumables / raw materials*
- Suppliers and providers
    - *Supply chain, including outsourcing*
    - *Maintenance arrangements*
    - *Raw materials*
- Systems and processes
    - *Arrangements to manage processes and to maintain quality*
    - *Communications systems – staff, public, suppliers*
    - *Financial systems*
    - *IT systems*
    - *Information about how to do things*
    - *And the data they hold*
- Information
    - *Contacts, phone numbers*
    - *Accounts and financial*
    - *Contracts*
    - *Bank and insurance policy details*
    - *Correspondence / e-mail*
    - *Procedures – how to do things*
    - *Data on IT systems, phones, paper etc*

7 What could go wrong?

Focus on what is more likely or would have the greater impact

- Absence or failure of any of the dependencies identified
- Staff:
  - *Large-scale temporary staff absence*
  - *Permanent or long-term loss of staff*
  - *Loss of key / specialist staff*
  - *Threats to staff safety*
  - *Identity theft*
- Buildings
  - *Denial of access to site or buildings*
  - *Effects of flooding, severe weather*
- Utility loss:
  - *Mains electricity*
  - *Mains water and sewerage*
  - *Telephones – landlines / mobile*
  - *Computer systems, internet or network access, e-mail, website failure*
  - *Disruption to road/rail/air transport system affecting staff and supplies/products*
  - *Availability of oil and fuel*
- Natural & man made disasters:
  - *Flooding*
  - *Storm / severe weather*
  - *Fire*
- Production process
  - *Failure of major suppliers (or purchaser)*
  - *Key equipment failure*
  - *Product defects*
- Legal and criminal
  - *Crime, vandalism, theft, identity theft / cyber crime*
  - *Changes to regulations, breach of regulations*
  - *Criminal acts internal to our business*
  - *Bomb / terrorism threat*
- Information
  - *Loss of financial records, contractual documents, other data*
  - *Loss of undocumented knowledge held by staff*
  - *Loss of diary and contacts lists*
  - *Electronic data and/or hard copy documents*

8 How can we improve the situation?

- Two approaches
  - *Lessen the likelihood of disruption*
  - *Lessen the impact if it does occur*

9 Lessen the likelihood of disruption

- Know the risks we are taking
  - *All staff awareness of risk and response*
- Avoid 'single points of failure' i.e. 'all the eggs in one basket'
  - *Share skills and knowledge*
  - *Have deputies for key posts*
  - *Back-up data*
  - *Identify alternative ways to the same result, e.g. suppliers*
- Identify most risky and most important processes
  - *Have spare capacity for these*
  - *Review just-in-time approach*
- Is there a less risky method?
- Can preventative maintenance or active risk-hunting help?

10 Lessen the impact if business is disrupted

- Have response and recovery planned in advance
  - *Get back to normal quickly*
  - *Focus on our priorities*
  - *What have plans do we have? Are they fit for purpose?*
- Use our back-up solution
  - *Alternative staff, alternative methods, restore lost data*
  - *Use reserve capacity, move resources*

11 What can we do to put things right?

- Responding and recovering

12 Responding – activation

- Are we clear about:
  - *How to alert staff to a disruption*
  - *How to activate response arrangements*
  - *Who leads / has authority to decide?*
  - *Who needs to be involved – specialist skills – who does what?*
  - *How to get information about the problem (inward communication)*

13 Responding – priorities

- What are our priorities?
  - *What can we safely defer?*
- What functions must be restarted first?
  - *How quickly (day, week, month)?*
- What resources we will need to do this?
  - *Staff, equipment, IT, premises, external suppliers, etc.*
- Who is managing the rest of the business?

14 Responding – communication

- Be clear how we will communicate with:
  - *Staff*
  - *Suppliers*
  - *Customers*
  - *Public*
  - *Emergency services*
- What are the key messages?
- How do we look to an outsider?

15 Outputs for today

- Understand vulnerabilities
- Ways to improve resilience:
  - *Reduce chance of trouble*
  - *Reduce impact*
- How to respond to a disruption

16 Next Steps

- Record useful points
- Take actions to prevent loss of business or loss of income
  - *Reduce risk*
  - *Review your response / recovery plan*
  - *The discussion record sheets should contain enough information to create a first draft*
- Identify a person to lead on business continuity / resilience
- Share ideas with staff
- Set a date to review arrangements
- Have a dry run at responding