IAB Members Guide
Business Continuity Planning

Introduction

This IAB guide provides members an overview of what is meant by 'Business Continuity' how it may be important for your practice and some tips on a practical approach to planning. Business continuity is all about anticipation and forward planning. Spending a little time and thought in preparation now is worth the payback later if something happens. But planning does need to involve more than an intention, it will need careful consideration and usually some practical arrangements made beforehand.

Why is this needed?

Being able to keep your business up and running even when 'the worst' happens does make commercial sense and of course your clients will still expect their problems to be handled.

Under the Anti Money Laundering Regulations 2017 (s40), you also have a legal duty in respect of the information you hold on record. You are required to keep CDD records for 5 years, even where your engagement with that client has ceased. So, you need to make sure those records are kept secure and available.

At a minimum, the IAB expects that members will undertake adequate business continuity planning and be able to demonstrate there are practical arrangements in place for CDD records in compliance with AML Regulations. But, probably above all, planning ahead is worthwhile because if some crisis does befall your business, you will be pleased to have answers for some of the problems already worked out and your business can carry on

What exactly am I planning for?

Of course, no-one can exactly predict the future and it makes no sense to plan for every possible eventuality. But it is prudent to have some plans that are capable of being applied in different circumstances and which will deal with the damaging effects on your business.

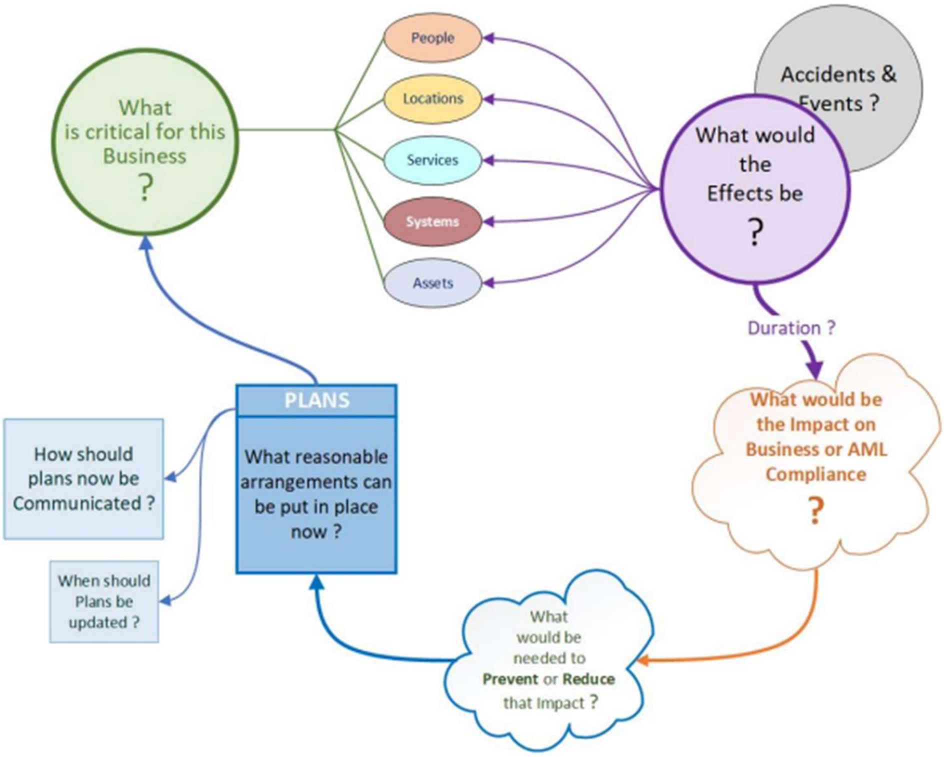
Any number of events may affect the people, locations, services, or business systems, that your business depends on. For example, COVID 19 has affected business around the world because of its effect on people. Those effects have been severe, but there are also other events that may have an impact. A local flood would affect a business because of damage to premises, stock, business records, or equipment. A fire would cause similar damage.

The key issue is having plans that will prevent or reduce the impact of the 'effects' on your business whatever the 'event' may be.

Broadly speaking 'effects' are going to involve:
▪ Absence of key people access to, or loss of:
▪ Premises
▪ Electronic data
▪ Systems including communications.
▪ Assets like equipment, supplies or hard copy records.

Depending on the event those effects could be large or small, they could be temporary or long lasting but planning ahead will help to manage the impact on your business.

How to Plan



Should the worst happen, planning will mean that you have some arrangements already in place and your business can continue but there are steps to go through.

First you need to assess who and what is 'critical' for your business:
▪ Key Staff (including yourself)
▪ Key Locations – Where work is done, where things are stored etc.
▪ Key Services – Power, Broadband, Water, Telephone etc.
▪ Key Systems – Computer software, Digital storage etc.
▪ Key Assets – Hard copy records or essential equipment etc.

Then you need to consider the consequences or 'impact' on your business in case of their loss or temporary absence and how those consequences might change over the short, medium, and long term. For example: 1 Week, 1 Month or 6 Months duration.

These considerations will highlight what might be manageable for a short/medium or longer duration and where you need a developed plan to prevent that effect or to provide a 'fall-back solution' that you will use in response to a crisis.

For example, you might conclude that the loss of unique hard copy documents, normally stored at your office would have a significant impact (i.e. the business would be in breach of AML regulations).

This would be something that must be prevented rather than responded to (perhaps by practical arrangements for keeping archive copies of the documents at a different location) But whichever the effect you are dealing with, your planning must be active and effective.

It is important to avoid assumptions, for example:

'If we couldn't get into the office, we would just work from home'.

This might sound like a straightforward plan, but it includes assumptions that the systems needed for work are already available 'at home'. Also, that 'home working' is a secure environment for private customer information. And, that all the staff do actually have the space to work at home.

If the office is unavailable, a 'work from home' solution is a good idea, but it needs an active and effective plan, which should be tested beforehand so you and anyone else involved understands any issues and how to fix them.

What about usually dependable services?

'We could manage if the broadband went down because they would fix it pretty quickly'.

This may not be an unreasonable assumption, but things do happen. In March 2004, in Manchester, a fire in a BT cabling tunnel destroyed the phone lines for 130,000 homes and businesses leaving them without communications. The effects included mobile communication networks, 999 services and data links. The damage was significant, and repairs took several months.

So, an important message is that you identify where you may have made assumptions and in the case of something that would have a significant impact on the business, that you make effective plans.

Sometimes you will decide to use a certain approach for normal business anyway; simply because it provides resilience. For example: systems to provide data backup, keeping a fax machine in case of broadband failure, or routinely sharing tasks between staff so they can each provide cover.

Having identified the most pressing issues and considered how long certain effects might need to be managed the next step is to work out the different types of solutions you will need:

• Preventive measures: For those effects with a significant potential impact and which must be avoided. (e.g. Loss of CDD Records)

• Fall-Back Arrangements: Where pre-planned action would be needed (e.g. No access to premises)

• Scalable Duration Plans: Where the effects are expected to be temporary but may extend (e.g. Loss of power supply)

• Generic Solutions: Which are adopted as normal practice providing resilience in different situations (e.g. Data back-up methods, publicised alternative contact details, or staff cover arrangements.)

Of course, the scope of this planning and the level of investment in any contingency arrangements is a matter of judgement for each business. For most, the arrangements will be realistic and reasonable; providing an adequate level of business continuity, and including the safe storage of necessary records.

Most practitioners will already have ‘cloud storage’ services in place which provide a secure and accessible ‘backup’ for digital records and files. Nevertheless, the terms and conditions as well as the efficiency of the chosen service should be understood and carefully considered. It may be prudent also to use additional data backup. A problem in any ‘crisis’ is often communication. So, it is always wise to pre-plan how people should contact you, your business, or your staff if the usual arrangements are not available.

Remember it is possible to take out insurance against some events and effects. Specialist companies can also offer business continuity planning or ‘disaster recovery’ services, but this may be expensive, particularly for smaller practices. You should document the arrangements you have in place, even if only briefly. Doing this means you can share your plans, for example with your staff or clients. It will assist you in testing or reviewing arrangements and it means you are able to demonstrate the planning you have carried out, for example, in compliance with AML regulations for the retention of records. A simple format for documenting plans might look like this:

Why – the risk this plan has been developed to deal with.
When- the circumstances that will trigger this plan.
What – the actions that will be taken.
Who – the people responsible for each action.
How – the way things will need to be done.
Where – the places things will happen, or people will be located.
Communication – who to inform and how we will keep in contact.

Continuity of Practice

The arrangements made by bookkeepers to cover their unexpected absence are sometimes misinterpreted as business continuity planning. It is true that ‘continuity of practice’ arrangements form a part of BCP as a ‘generic solution’ though, as we have seen, effective BCP should include other contingencies.

Nevertheless, sole practitioners will find it useful to have plans dealing with absence. For example: in circumstances where illness prevents communication directly with clients; it is useful to have clear arrangements agreed beforehand which involve another person (suitably qualified and authorised) who could provide clients with access to their own bookkeeping information or records where this becomes necessary.

Data privacy is still an important consideration and clients should always be made aware of such arrangements, so they know who to contact if necessary. It may be appropriate to include such information in the usual letter of engagement.

Summary

- Understand what your business relies upon
- Calculate the impact of different effects and how those impacts could be reduced
- Think through what you might need, before that need arises
- Avoid assumptions and actively plan ‘reasonable arrangements’ and generic solutions
- Make sure your CDD records are protected
- Test arrangements so you know they work
- Communicate with the people that would be involved