Business Continuity and Disaster Recovery

Policy Brief

proactis

Table of Contents

1 Introduction

There is a growing demand from Contracting Authorities for assurances that, in the event of unforeseen circumstances or disasters, your business will continue to function and provide the contracted services.

There are two key areas that authorities may want reassurance in:

Business Continuity Planning – This is focused on contingency planning to ensure the continuation of vital business functions. For example, if you are unable to access your company's offices one morning, how will you provide the services you've been contracted for?

Disaster Recovery – This is a subset of business continuity, focussed on the resilience of your IT infrastructure. For example, if there is a power cut how much data will you lose?

2 What is a disaster?

This is anything which affects your business, and can include things like:

- Your building burning down
- A power cut
- A chemical spill rendering the area around your office inaccessible
- Bad weather preventing staff from getting to work
- Mass staff absence – possibly caused by the spread of illness through the workplace
- Cyber-attack bringing down your online services

3 What's involved?

The first step in developing your business continuity management system is to write a Business Continuity Plan. There are a number of key factors that should be outlined in a plan including, but not limited to:

- Which areas of the business are essential?
- Which members of staff are essential to those areas of the business?
- What sort of disasters may impact these business areas?
- How long can these essential areas be disrupted without impacting your business?
- How long can the rest of your business be disrupted without causing ongoing harm?
- How can you mitigate the effects of these disasters?

proactis

4 Where do I start?

Do a risk assessment. The best idea is to do it on a spreadsheet, and start by listing your business 'assets' (these could be identified by business function, job title, department, or various other metrics, and can range from staff members through to electronic data). Once you have these listed, you can work out how important they are, and thus how long you can live without them.

After you've got this register of your assets, you can start looking at what your risks are. There are a number of approaches you can take. You could draw up a list of disasters that might conceivably affect your business, and then list next to each which of your assets it would affect. Or you could assess each asset individually to identify what disasters might affect it directly.

Once you've paired your assets with relevant disasters, you should start outlining what mitigation measures you can put in place. The best outcome is to completely negate the possibility of a specific disaster affecting you – for example if you are assessing the impact of a power cut, you could obtain a secondary power supply for your building.

However, normally you'll only be able to minimise the affect – in the same example of a power cut, if you implement an Uninterruptable Power Supply, this would provide your IT systems with a grace period of a few minutes to properly shut down without losing functionality or data.

If you can't find a way to minimise the chances of a disaster taking place, you want to find ways to maintain your business after it has happened. Work through your assets in order of importance, and identify how you can ensure their continuation, regardless of circumstance.

Some options to consider – have a backup data centre (also known as a disaster recovery site); have a secondary work site (office space in a different part of the city); be able to implement home working for vital staff with little notice; and have fire/flood prevention in place.

5 Anything else?

Your plan needs to outline who is responsible for initiating your business continuity process, and then who is responsible for what thereafter. Does your MD call each Department Head at home to tell them to open the red envelope? Or perhaps your Office Manager will call key staff members directly, before alerting the rest of the company?

Also remember to practice. Carry out drills and practice sessions with all your staff. If they know what they're doing when disaster strikes, your business will be much more secure.

6 How do we prove we're going to be ok?

ISO 22301 is the international standard for business continuity. Being certified to this standard can give a Contracting Authority absolute confidence in your ability to withstand the unforeseen.

If you do not have ISO 22301 certification, you may find authorities willing to accept ISO 27001 certification in its place. This is because the objective of Annex Control A17.1 is specifically "Objective: Information security continuity shall be embedded in the organization's business

continuity management systems" and the objective of Annex Control A17.2 is "To ensure availability of information processing facilities."

Whilst ISO 27001 does not absolutely certify your business continuity contingencies, it would be nearly impossible to obtain 27001 certifications without having a solid business continuity management system in place.

If you don't have either ISO certification, then you may be able to provide assurance to an authority by demonstrating what continuity measures you have in place.

7 More help?

If you've read this and still aren't too sure where to start, or perhaps you've written up a basic plan and need some help fine tuning it, please don't hesitate to get in touch and see how we can help you.

Call **0800 222 9010** or email us at **askus@tendersdirect.co.uk**