Business Continuity Planning in IT

**Introduction:**

The more your business relies on its IT systems, the more you need to consider how unexpected disruptions might affect your business. These disruptions could come in many forms, from fire and floods to theft or malicious attacks on your systems, such as viruses or hacking.

Business continuity planning improves your business' ability to react to such disruptions. It describes how you will restart your operations in order to meet your business-critical requirements.

This guide explains the importance of business continuity plans to the success of your business, how best to develop a plan, and what to do in the event of a systems failure.

---

**What is business continuity planning?**

Business continuity planning is the process of planning for the unexpected. An effective plan will provide you with procedures to minimize the effects of unexpected disruptive events. The plan should enable your business to recover quickly and efficiently, with minimal impact to your day-to-day activities.

**The importance of business continuity planning for IT**

Business continuity is a process developed to counteract systems failure. It is a management issue, not something that should just be considered by the IT department. If your IT systems fail or are unavailable, it is likely to have a significant impact on your whole business. Therefore, you should take an active interest in establishing business continuity plans for your IT systems.

A business continuity plan for your IT systems should include arrangements for providing:
- facilities and services to enable the business to continue to function
- the critical IT applications and infrastructure necessary to support the recovery of business processes

For more information, see the page in this guide on systems failure.

**Format and distribution of your business continuity plan**

It is important that your plan be:
- clear and concise, to ensure that people understand it and any responsibilities they have as part of the plan
- made available to all staff members responsible for any part of it

You could also summarize the plan for the rest of your staff so that they will know what to expect.
Updating your business continuity plan

Once a business continuity plan has been agreed, it is the start of an ongoing commitment. Businesses constantly evolve, and recovery strategies must evolve with them.

For example, you will need to update your plan:

- as people join, transfer and leave the business
- if you introduce new business-critical IT infrastructure

The benefits of IT business continuity planning

The main benefit of business continuity planning is enabling your business to recover quickly from unexpected events that disrupt your IT systems.

However, there are other good reasons to have a business continuity plan.

Legal requirements

In some industries, it is a regulatory requirement to have a recovery plan in place. For example, financial organizations must have continuity and security controls.

Customer reassurance

A business that can demonstrate an effective business continuity plan has a competitive advantage. For example, if you provide services to customers that are dependent upon your IT systems, like an internet service provider, then evidence of a sound plan can be used to win or retain customers. For instance, if your business is a partner in a supply chain, business continuity planning may well need to be an integral part of your quality assurance.

Insurance

Effective business continuity management can help businesses demonstrate that they are managing their business risks and so help to secure lower insurance premiums. In addition, drawing up a business continuity plan can help you assess what types of insurance you need the most.

This is because business continuity planning may help to identify potential business risks that you were previously unaware of, but which you recognize that you need to insure against. So, you may decide to opt for lower insurance cover across a broader range of risks - the original risks plus the recently identified ones - in order to remain within your budgeted insurance cost.
Risk assessments for IT business continuity planning

The first step in business continuity planning is to do a risk assessment. This helps you to decide on which business threats to concentrate. It involves:

- identifying the range of potential threats your business faces
- assessing their potential impact on the business
- assessing the likelihood of each threat occurring

Potential business threats

You first need to identify the threats your business could face.

For your IT infrastructure, these could be:

- physical threats, e.g. fire or flooding
- systems threats, e.g. malicious software such as viruses and trojans

For more information, see the page in this guide on systems failure.

Impact analysis

You should consider how much your business stands to lose as a result of each possible type of unexpected event. To do this you should identify:

- your critical business processes
- the potential damage or loss that your business would suffer if any of these services were disrupted

The damage can be measured as follows:

- in hard terms such as financial loss
- in soft terms such as loss of business credibility or damage to your business’ reputation

You should also consider if any damage or loss will get worse if the disruption lasts longer than you might normally expect. For example, what would be the impact to your business if your e-commerce site were down for a day rather than an hour? For some businesses, this may mean the difference between a temporary loss of revenue and going out of business.

Threat probability

Having determined the impact of each threat, you should determine the probability of each threat occurring. This will help you decide which threats to prioritize in business continuity planning.

For more information on risk assessment, see our guide on identifying and managing IT risks to your business.
Components of an IT business continuity plan

You will use information on threats to your business to create your business continuity plan. See the page in this guide on risk assessments for IT business continuity planning.

The plan should aim to reduce the risks posed by disruption to your business processes. Measures that may be needed include:

- A back-up and data recovery strategy, including off-site storage.
- The development of a resilient IT infrastructure with redundancies (spare capacity) in case of failure. For example, mirrored central server computers sited in different locations, each containing the same information, so that if one goes down, the other one is available to ensure continuity of service and alternative storage facilities.
- The elimination of single points of failure, such as a single power supply.
- The introduction of an uninterruptible power supply for your IT systems. This is a battery-powered device that allows your systems to keep running, giving you time to save any data that you may be working on.

Even if such measures are adopted, things can still go wrong. Therefore, the business continuity plan should specify the actions to be taken in order to recover from any unexpected disruptive event, covering:

- people and accommodation
- IT systems and networks
- services such as power and telecommunications
- critical business processes

Methods of recovery might include:

- carrying out activities manually until IT services are resumed
- moving staff at an affected building to another location
- agreeing with another business to use each other’s premises in the event of a disaster
- arranging to use IT services and accommodation provided by a specialist third-party standby site

Keep the business continuity plan short and readable. It should not duplicate other sources of information, and should be refer to any other relevant documents. Encourage staff to review the plan before it is formally issued.

For more information, see the page in this guide on systems failure.
Systems failure

A systems failure can be caused by fire, flood, earthquake, snowstorm, power supply problems, industrial action, sabotage, or user error. Therefore, it needs to be addressed in a structured manner.

What are the risks of systems failure?

Risks of a systems failure can range from minor inconvenience to disaster, depending on the type of system. For example, an unavailable webpage may be irritating but the failure of an online payment system may have much more of an impact on the business, and its customers.

You can assess and minimize the IT risks facing your business with our IT risk assessment service.

For an indication of whether you should be taking steps to protect your system, ask yourself the following questions:

- Are you dependent on any single thing (computer, person, building, telephone line, internet service provider, supplier, shipping agent, haulage firm, etc)?
- Have you analyzed your business processes in the context of 'what happens if this fails, goes wrong, or simply isn't there'?
- Do you understand the threats your business is facing?
- How would you reconstruct your company information should it be lost or corrupted, how long would this take, and how long could you survive in the meantime?
- Does your staff know whom to call if there is a major incident?
- Do you know the home and mobile telephone numbers of all your key people?

Systems failure prevention

To prevent or reduce the risk of systems failure within your business, you can perform a risk assessment as part of your business continuity management. See the page in this guide on risk assessments for IT business continuity planning.

For information on steps you can take to prevent or reduce the risks of systems failure, see the page in this guide on components of an IT business continuity plan.

Systems recovery

The key to recovery from system failure is preparation. If you are prepared, you will be in a much stronger position to cope with the unexpected. Some system failures need immediate recovery, but you can manage without other systems temporarily.

To read about methods of recovery, see the page in this guide on components of an IT business continuity plan.
Testing your IT business continuity plan

Testing a business continuity plan can be difficult. Simulating potential threats to your business can be time consuming and expensive.

However, testing your business continuity plans will help show whether you have covered all angles, and whether your plan is achievable. In addition, it can increase your business and trading partners' confidence in your business' ability to recover from disruption. Tests are also useful to raise staff awareness of the plans.

Setting test objectives

You should ensure that any test you undertake, whether technical - relating to the operation of the IT systems - or non-technical - relating to all associated activities - has clear objectives.

For example, the aim of the test could be to:

• measure the time needed to get your main IT system back up and running following a disruption
• find out how long it takes to contact all key personnel

This will enable you to measure the success, or otherwise, of each exercise, and highlight areas in need of further attention.

Data-loss and back-up tests

The main tests you should carry out should aim to check:

• the extent to which staff can function without access to data
• the restoration of data from back-up sources, particularly if the data is held off site

These will help to establish:

• whether or not your back-up data is up to date
• whether any third parties or service providers who are integral to the plan are ready to respond
• whether or not your expected timescales for recovering key business applications are realistic
• how prepared staff are for putting the plan into action

Periodic re-testing

Any initial testing should be followed by further tests on a regular basis, e.g. every 12 months. In particular, details of any changes to IT systems should be included in the plan and tests should be undertaken on the new systems.
Education and training in IT business continuity

All members of staff should be aware of the importance of business continuity planning. Training and awareness are important to make sure that your staff fully understands the plan and the role they will play in it.

Awareness can range from simple knowledge of the assembly points should the building have to be evacuated; through to the exact role each member of staff will have if an unexpected event occurs.

Awareness training should be undertaken on a regular basis, and included in any staff induction programs.

Staff who will have specific responsibilities for the recovery of IT systems should be given further technical training. This will ensure that they are able to recover systems and applications quickly and efficiently.

Any third parties who have a critical role in your business continuity plans should be part of this awareness training. If, for example, you have set up office-sharing arrangements with another business, then they need to know the procedures you will follow if your own office becomes unavailable.

You might also wish to consider training for any member of staff who may need to talk to the media in the event of a disruption or incident. This is particularly important if the reputation and public perception of your business is key to its ongoing success.

Key steps in developing a business continuity plan

The Business Continuity Institute's 'Business Continuity Management Life Cycle' model covers five key stages in developing and maintaining a business continuity plan.

Understanding your business

- Project initiation and management - get support from senior managers. Establish a management structure to develop and carry out the plan.
- Risk evaluation and control - identify the threats and the best defense. For example, with e-commerce, computer viruses might be a major threat - the appropriate defense might be regularly updated anti-virus software. See the page in this guide on risk assessments for business continuity planning.
- Business impact analysis - establishes your business’ critical processes and identifies the impact of any failures. For example, if your e-commerce website were critical to your operation, what would it cost your business if it went down for 24 hours?
Business continuity management strategies

- Develop an organizational business continuity strategy, which identifies critical areas of concentration. Focus on the critical operating requirements of the business, as identified above.
- Develop a process-level strategy - a documented framework clearly stating how critical processes will be restarted following an incident or failure. For example, if the payment system for your e-commerce website goes down, you need a specific strategy for resuming operations.

Developing and implementing a business continuity response

- Emergency response and operations - establish a crisis management process to respond to incidents.
- Develop and implement a business continuity plan. This describes specifically how you will deal with incidents. Focus on the priorities of your overall business continuity strategy.
- Put in place business unit plans for each department. For example, detail the actions that the IT department will have to carry out if IT services are lost.

Developing a business continuity management culture

- Awareness and training plans - ensure all staff are aware of the importance of business continuity and can operate effectively following an incident.
- Review the effectiveness of awareness training periodically. Identify any further training needed.

Exercising, maintenance and audit

- Test the business continuity plans. Test any technical aspects - for example if you plan to use backed-up data to restore operations. Carry out full live exercises to establish how the plans work in a disaster situation.
- Maintain the plans - ensure that the documentation remains accurate and reflects any changes inside or outside the business.
- Regularly audit the plans - do they meet the needs of your strategy? Act on your findings.