

## Virtual Servers

---

Up until recently most servers were only capable of running a single operating system, now with the availability of more powerful hardware servers are capable of hosting multiple operating systems. Each hosted operating system is known as a virtual server. These virtual servers run their own operating systems independently of the host and the other guest virtual servers. Because they are no longer dependant on the hardware they are running on, it is very easy to transfer or replicate a virtual server from one physical host to another dissimilar physical host. For business continuity purposes, restoring a server onto dissimilar hardware is a long and complicated process, but with virtual servers the process is far easier and takes a lot less time.

Another advantage of virtual servers is that it is possible to run more than one virtual server on a physical host, thus taking advantage of any of its spare processing capacity. Also, in a business continuity scenario it is possible to have a few powerful physical servers hosting a number of virtual servers at a remote location, be it a branch office, a hosting centre or in the cloud. Virtual servers can be easily replicated or restored onto these alternative hosts ready to be activated in the case of a business continuity situation.

## Thin Clients

---

For a number of years now it has been possible to access systems remotely as if you were sitting at your computer in the office. Typically you would have a Citrix server, or servers, hosting thin client sessions for each of your users. Users might be sitting in the head office, at a branch or even at home, and can access your systems via the Internet. Thin clients offer great advantages in business continuity planning; for example if Citrix servers were used at a head office, as well as at either a branch office or hosting centre, thin client sessions could simply be redirected should an incident occur. This would allow your workforce to carry on working, unaffected by the incident.

## Replication

---

In order to reduce the time it takes to recover a server or data, replication should be considered. There are a number of different ways of replicating servers and data to other storage devices, other servers, or in the cloud. By using other storage devices data still has to be recovered. However, if data is replicated to other standby servers or servers in the cloud, it is simply a case of enabling these servers, to get you up and running again quickly using a recent copy of your data. Ideally these standby servers, with the replicated data on them, would be housed at a different location.

## How JMC can help you...

We can work with you to design systems to enable you to deal with your own unique business continuity challenges. Our extensive experience combined with long-standing relationships with other specialists mean that we can help organisations of all sizes put robust plans in place to protect their businesses.

Business continuity is as much a concern for JMC as it is for any organisation. Not being able to access data, emails, premises or make a phone call all have the potential to damage our business – and that is only the start. If our business continuity planning fails, so does that of our clients.

Our clients expect IT support on demand. Due to the depth and breadth of our business continuity plans and our investment in failover systems in multiple locations, home working and standby power generation clients can be confident we will be available whenever needed. Can you say the same for your current supplier?

## Key Phrases

### Snapshots

A snapshot is the process of copying data at a specific point in time.

### Recovery Point

A recovery point is the point in time on your system when it was last backed-up. If your IT system was to fail, the recovery point would be the point in time that it would be recovered from.

### Thin Client

Thin client is a networked computer that accesses programs and data from a server instead of storing them locally. This computer performs the majority of its operations on a server rather than using its own resources. Typically this would be a PC but it could be a device such as an Apple iPad.

### In short, we can:

- Design and implement a comprehensive IT business continuity plan
- Deliver a comprehensive range of solutions to ensure your system is as resilient as possible
- Provide all the services required to enhance your existing IT system
- Offer a wide-ranging support service to monitor and manage your system
- Undertake regular detailed business continuity tests to ensure that your plan works

Tel: 0161 925 7777

[www.jmc.it](http://www.jmc.it)



# Business Continuity

## An Introduction to Business Continuity

*Business continuity planning, encompassing disaster recovery, minimises the impact of an incident on an organisation by ensuring alternate processes are in place for key operational functions.*

Business continuity planning looks to preserve assets as well as an organisation's ability to achieve its mission, retain acceptable levels of productivity, customer service, and ultimately to stay in business.

### Can an organisation be too small for business continuity planning?

Business continuity planning is not consigned to large organisations; any provider of a service or product, whether it is financial, manufacturing, distribution or sales, is equally exposed to the effects of a disaster. Are you prepared if something goes wrong?

### Surely a business continuity plan is not needed if adequate insurance is in place?

Quite simply insurance does not buy back lost business, it only provides money. If this is not received immediately it could adversely affect cash flow, subsequent profits and client goodwill. Studies suggest that typically only 60% of actual losses are covered. Could your organisation survive the loss?

Disaster does not just occur following an incident on a grand scale. A small incident, over a short period, impacting a key process, could severely disrupt an organisation; for example, an incident in the local area that requires evacuation of your premises for hours or even days. Computers still run, phones still work and infrastructure is unharmed but there is no access to any of it until the incident is resolved. Interruption threats come from multiple sources;

some more likely than others. Premises may be flooded, destroying servers, or an organisation may be the victim of theft. A business continuity plan examines the likelihood of this happening and considers a response relative to the risk.

It is vital to determine what would be addressed first following an incident.

Who would be contacted first? How would staff be notified? To do this you need to examine your organisation, its people, its critical processes and how these are dependent upon considerations such as IT and infrastructure support, internal dependencies and suppliers.

The solutions are not just quick fixes but long-term considerations. It is possible to survive an incident, but not necessarily possible to recover from its long term impact.

## Where do I start?

---

The following pages highlight some key areas of IT business continuity that an organisation should consider. Business continuity is a huge area and this is by no means a definitive guide. What this solutions guide will hopefully do is stimulate thoughts and further questions about how we can help you implement cost-effective IT business continuity plans.

## Definition

---

Business continuity ensures an organisation protects its essential functions to enable it to continue to work during and after a disaster. Business continuity planning seeks to prevent interruption of mission critical services, and to re-establish full functionality as swiftly and smoothly as possible.

## What options are there?

---

IT business continuity planning needs to address both the hardware and data contained within your system. This section highlights some of the ways you can build protection around your system. At JMC comprehensive planning is ensured by using highly resilient servers, secondary power supplies including a backup generator, dual Internet connections, redundant storage and uninterruptable power supplies. As well as this we use thin client technologies, such as Citrix and Microsoft Remote Desktop Services, for remote access, and virtual servers to provide both flexibility and resilience. In addition cloud technologies deliver an abundance of ways to enhance your business continuity plans.

## Resilience

---

You can build a lot of resilience into your IT system hardware. The aim when creating a resilient system is to remove any single point of failure.

Hard disks used to store your applications and data are a likely point of failure, making them an area of risk and a key place in which to build resilience. You can build storage resilience by using a Redundant Array of Inexpensive Disks (RAID). By using RAID your system can lose a hard disk and still function without interruption, giving you time to replace the failed disk.

Another way to build resilience is to address the potential failure of power supplies. IT systems prefer clean power supplies; power outages or even dirty power can cause serious problems. You can build resilience by having hotspare power supplies receiving power from different sources. This way, if one source fails the other continues whilst the failed supply is fixed. As a minimum you should have all your servers on Uninterruptable Power Supplies or UPSs as they are more commonly referred to. UPSs continually clean and smooth the spikes out of incoming power supplies. In the event of a power outage UPSs keep servers running long enough to safely close them down or switch to an alternative power supply. If you cannot afford to have servers down, then you need to consider alternative power supplies like standby generators that kick in automatically if they detect a power outage.

Using more than one Internet Service Provider (ISP) builds added resilience into your communications infrastructure. If one communication link fails, the other can take over. However, just having different ISPs providing broadband connections is not always enough. A further consideration should be to ensure your links to the Internet do not use the same means of physical connection. ISPs often use the same cable and exchange, meaning that should there be a problem between your office and the exchange, it is likely you will lose both connections. To avoid this we would suggest implementing an alternative method of connecting to the Internet such as a radio link alongside a broadband link.

## What about my data?

---

Having considered your hardware, you also need to address the challenge of protecting your data. Both traditional solutions and new emerging technologies play a key role in comprehensive data protection. To ensure we protect our own internal data we have implemented a series of solutions. In addition to traditional tape backups we have implemented technology such as Microsoft System Centre Data Protection Manager (DPM) to provide continuous backups throughout the day. Due to the massive business benefits DPM offers, we consider it a key part of any comprehensive business continuity plan.

### Traditional Tape Backup

---

Tapes have traditionally been the most widely used option for backing up data on an IT system. During off-peak hours, the system is backed up to tape. Tapes should then be checked to see if the process has been successful and then taken off-site. This off-site location ensures protection of the data should an incident such as a fire occur.

Backup tapes are a great form of cost-effective backup, but it is important to be aware of their limitations. A large amount of data can be backed up onto one tape with the process typically being performed out of hours. This in itself might not suit some companies as off-peak hours are less common due to flexible working practices. Because of the way data is backed up to tape, recovery times can be quite lengthy as the data has to be located on the tape before it can be restored. In addition, if an incident occurs at the end of the working day, the recovery point would be the night before, meaning that you could lose an entire day's work.

### Continuous Data Protection

---

Continuous data protection is a solution where, as the name suggests, a system's data is continually being backed up. This removes the issues associated with traditional tape backups in that downtime is not necessary as your data is being backed up continuously as changes are

made. In order to enable this type of solution, adequate disk storage is required to store the most recent revised data. A snapshot of this data can then be taken periodically, for example daily, and the snapshots can be backed up to tape for longer term storage.

Microsoft System Centre Data Protection Manager (DPM) is a solution based on near continuous data protection.

DPM constantly monitors protected servers and only copies changes saved to the protected server to a DPM server. A major advantage of only copying the changes is the significantly reduced bandwidth required to protect the server. Because of this reduced bandwidth it is possible to protect servers in branch offices across a wide area network. DPM is also Microsoft application aware, meaning that it is compatible with applications such as Microsoft Exchange, Microsoft SQL and Microsoft SharePoint and can therefore protect these appropriately. By using snapshots and by being application aware, DPM can restore Exchange or SQL to within the last 15 minutes. It can also provide up to 512 recovery points by creating periodic snapshots. Snapshots can be created as often as every half hour if required but typically they are created at least once a day. Performing one snapshot a day and capturing changes every 15 minutes means you could have nearly 50,000 recovery points and potentially be able to recover data to any 15 minute point in time over an 18 month period. Realistically though you would normally have two to four weeks' data on disk which would then be offloaded to tape for long term protection. For further protection this could also be replicated off-site or in the cloud. DPM has been developed with ease of use as a priority. Unlike recovering items from traditional tape backups it is very easy to use the DPM console to find the item you wish to recover, view all its potential recovery points and then recover it to its original location or copy it to a new location.

This process takes far less time than it would to recover information from tape. If enabled, it is even possible for users to view previous versions of files and recover them without having to involve their IT department or support company.

Another factor DPM addresses is human error. Traditional tape backups require someone to check the previous night's backup and swap the tapes. Quite often it is assumed that last night's backup happened without any problems and the tapes are duly swapped. If for some reason the backup failed and no one noticed, the tape would be useless. DPM can back itself up to another DPM server in another location, either across the Internet, in the cloud, or via a wide area network. This can happen automatically and does not require human intervention. Using this method an off-site copy of the system is automatically provided each day. Though tape backups are still recommended for longer term storage, this automatic backup reduces the need to rely solely on them.

In the event of a major incident at your main site, data on your second DPM server can be quickly and easily restored onto alternative servers meaning that you can be up and running quickly. Combine this with virtual servers and thin clients and you have a very cost-effective business continuity option.

### Rapid Recovery

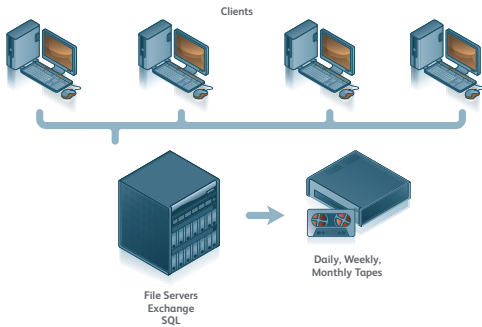
---

A comprehensive business continuity plan must address potential recovery times. With any plan, the main ambition is to get a working system as quickly as possible. Many recovery procedures only start when a problem occurs, meaning a long delay before you and your team can access the system. One solution to this is to have a second system containing a copy of your primary system, ideally in a remote location. However, the costs associated with achieving this can be significant and beyond the budgets of many smaller businesses. To address this challenge we partner with Plan B and offer their cost-effective solution.

Plan B provide remote servers that you access – and pay for – as and when needed. The service works by taking nightly snapshots of your key servers and their associated data. The changes to the snapshots are then sent securely to remote virtual servers at a highly secure location ready to be activated should they be needed. These virtual servers can then be made available within the hour; often within as little as 30 minutes should you need it. Your users can then connect remotely to these servers and start working securely on them.

## Tape Backup

Traditionally the most widely used form of backup, tapes offer a cost effective solution for secure data backup.



### Pros

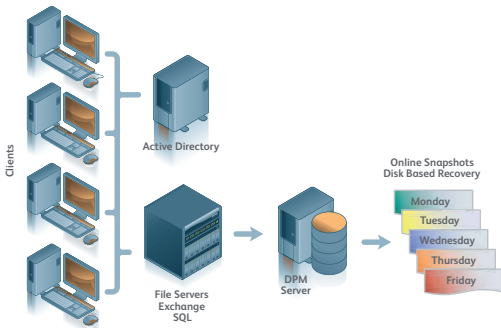
- ✓ Cost effective.
- ✓ Each tape can hold a large amount of data.
- ✓ Useful for long term storage requirements.

### Cons

- ✗ Backups need human supervision to ensure they have worked.
- ✗ Tapes must be taken off-site and securely stored.
- ✗ Data recovery times can be lengthy.
- ✗ Recovery could mean losing an entire day's data.
- ✗ They need to be checked regularly as they can fail.
- ✗ For complete data integrity data must be backed up during quiet periods (i.e. overnight).

## Data Protection Manager (DPM)

A comprehensive Microsoft data backup solution where data is continuously backed up.



### Pros

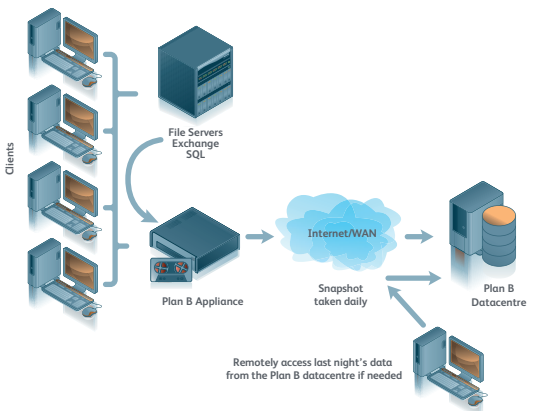
- ✓ Data can be restored to within the last 15 minutes.
- ✓ Downtime is not necessary.
- ✓ Servers in both head and branch offices can be backed up.
- ✓ Recovery is straightforward and a lot quicker than other methods.
- ✓ Users can recover their own files.
- ✓ No human intervention is needed.
- ✓ As it is a Microsoft solution it knows how best to backup Microsoft application data.

### Cons

- ✗ A large amount of disk space is required to keep multiple recovery points.
- ✗ You still need to backup long term data to tapes.

## Plan B

Rapid data recovery without the typical purchase cost and maintenance demands of the associated server hardware.



### Pros

- ✓ Provides an automated, complete system backup to a remote datacentre.
- ✓ Once the initial setup is complete it only copies the day's changes.
- ✓ Should it be needed you can be up and running with the previous night's data within 30 minutes.

### Cons

- ✗ Recovery could mean losing an entire day's data. You can only access the data held at the datacentre remotely.

## Off-site Replication

This complete business continuity solution offers the most comprehensive approach.

It combines DPM, off-site replication and tape backup. Data is backed up by DPM, replicated off-site and backed up to tape. Combine this with virtualisation techniques and, should your usual working practices be interrupted, you will be able to return to normal service quickly with little, if any, interruption.

