



## Service Overview

Version 1.2

January 2009



ISO27001 International Information Security Management Standard certified

## Benefits of Plan B Disaster Recovery Service

- **Very Fast Recovery** – your critical systems back in around 30 minutes.
- **Very simple to set-up** – it only takes about 20 minutes to install the Plan B DR appliance on your network.
- **No management required** – no ongoing support required from your staff or any need for changes to how they run your systems just because they are protected.
- **Virtualisation technology** – the use of virtualisation technology means no expensive hardware or maintenance costs, and the flexibility to dynamically manage your recovery system images and the resources they require.
- **Simple, predictable low monthly costs** – based on required rescue platform capacity and data, not on unused hardware or software.
- **Verified Service** - every daily server back-up is tested so you know it will work if and when needed.
- **Minimised bandwidth** – the intelligent Plan B DR appliance only sends server changes back.
- **Local file Backup** – we keep old copies of snapshots on the appliance, which provide a local historical file backup, and because each snapshot is tested, you can at last be confident you have a backup that will work when you need it!

## Why Plan B DR?

- **Recoverability** – service specifically designed to provide an extremely high level of recovery and almost immediate system availability at a fraction of the price of a traditional 'warm standby'.
- **Assurance** – service is automated and tested to ensure every snapshot is available, verified and will run on the rescue platform when you need it.
- **Simplicity** – the service is very simple to implement and live with, and the level of recoverability and assurance help to simplify the associated elements of your business continuity plan.
- **Managed service** – designed to deliver fully recovered systems, when you need them most via a team dedicated to you at your time of crisis. No distractions, no conflicts.
- **Low Cost** – use of virtualisation technology means no dedicated hardware or associated management costs, providing a 'warm standby' level of recoverability at a fraction of the traditional price.
- **ISO27001/2 Certified** – Plan B's information security management policies, processes and procedures have been audited and passed by the BSI to conform to the international organisational security standard ISO27001/2.

## Plan B's Disaster Recovery Service

Plan B's Disaster Recovery Service has two key elements; firstly the day to day process of 'snapshotting', converting and storing system images (copies of all the software on a server) in case they are needed, and secondly the invocation of the service in the event of a customer disaster. Invocation, covers the booting up of stored images on virtual servers, the authorisation to do so, connecting to the Rescue Platform and the eventual migration back off the Rescue Platform once the crisis is over.

More detailed information on the service can be found in the following sections:

### System Image Capture

Plan B operate a unique process for capturing the system images of servers we are protecting. This process is proprietary to Plan B and has been developed to be highly efficient and secure.

There are two key parts to the image capture process. Firstly, the 'snapshotting' of server images in the customers network and the transfer of snapshots to Plan B, and secondly the processing of those snapshots into 'Rescue images' and their conversion to run on Plan B's virtualised Rescue platform.

#### System Image 'Snapshotting'

Plan B capture system images of protected systems via a dedicated appliance that sits inside the customer's network. Once a client signs up for the Plan B service we courier them an appliance and instructions on its installation and configuration.



Once the simple configuration process is complete (which should take about 20 minutes), the Plan B appliance will automatically, poll each system it is set up to protect, and take a 'delta' copy of the system images of each machine. We call this a 'Snapshot'. Snapshots only contain files from a particular system that have changed since the last snapshot was taken. The base service takes Snapshots every 24 hours, but more regular snapshots can be taken if required.

Captured Snapshots are then encrypted for secure transfer to Plan B for processing and testing.

The appliances are completely autonomous and control all work associated with capturing snapshots, minimising the amount of data required to be transmitted and then securely sending that data to a Plan B Rescue Platform. The appliances have been developed to be inherently secure and accept no incoming connections of any nature, not even from Plan B.



Data sent by appliances is stored in Plan B's Snapshot storage system. This holds an up-to-date copy of every file contained within every host that we provide protection for. It also holds the 'Last known good' set of files for regression if the new snapshot fails its testing for any reason.

### System image 'P2V' conversion and testing

Once transferred to the Snapshot storage system, a new snapshot is scanned to calculate any changes to the previously held system image. The new snapshot is then combined with files that have not changed (and therefore not been transmitted from the appliance) to create a new physical system image. We call this a 'Rescue Image', and once created is then ready for conversion so it can run on the virtualised Plan B Rescue platform.

The 'Physical to Virtual' (P2V) conversion of the image is Plan B 'magic' and is done automatically by applying various Plan B 'Overlays'. These Overlays make changes to the system files so they can run successfully on a virtual machine. Plan B have many standard Overlays for common system elements and common applications, but will write new overlays for customers with unique configurations.

Once a Rescue Image has completed its P2V conversion, it will be queued for testing. Plan B test **all** new Rescue Images every time they are updated, which for standard systems would be at least once every day. Testing is done automatically by booting up a newly created Rescue Image on a live virtual server and applying a test harness that will check an image is functioning.

All Rescue Images that pass testing are then moved to the Rescue Image Repository, where they are stored ready to be booted up if needed. All images in the Repository are therefore images that are ready to run and have been proven to work. All that is needed to get a client's image running from this point is for Plan B to allocate it a virtual server and boot it up. Running images can therefore be ready literally within minutes!

If an image fails testing then the Plan B Process Scheduler will ticket it and a Plan B Engineer will investigate the cause of the failure. Customers can keep track of issues via the Customer Portal.

## Local file retrieval facility

The Plan B appliance keeps a copy of all data contained within the snapshots. It will also retain as many historical copies of data as its storage allows (and because it only stores files that have changed, it can be quite efficient).

As a result, the appliance can also provide a retrieval interface to allow nearly instant access to backed-up data, which may help prevent the need to invoke the full DR service for those events that are 'finger trouble' related, or where just getting back last week's spreadsheet for the finance department is the only requirement. Because the data is held locally on disk, it's significantly quicker to get data back than tape, or even online backup solutions.



Control of the Local File Retrieval facilities is done from the appliance interface by selecting the lost files from the directory tree for the affected server and instructing the appliance to either replace the files on their original volume, or to place them on any other protected machine, should that machine not be available.

## Recovery Service Invocation

In the event of a disaster Plan B will provide customers with replacements for their systems running on virtual servers on a Plan B Rescue Platform.

A disaster can be any event that in the opinion of the customer prevents them from using their IT systems, either temporarily or permanently.

The Plan B service is invoked by calling the Plan B Emergency phone number.

From this point on, Plan B engineers will be dedicated to getting you up and running as soon as possible. Your staff members are therefore free to concentrate on the problems at hand while we get your replacement systems running.

Because of the implications of bringing up a new service, all invocations must be authorised by a pre-appointed client executive(s) using a specific security process.

Once the authorisation process has been followed successfully Plan B Engineering will agree the course of action, allocate virtual servers and boot up the appropriate Rescue images. They will also activate other services such as DNS & email redirections, and set up VPNs. All actions to invoke a particular service, and any dependencies between systems are documented in the Plan B Configuration Management Data Base (CMDB).

Plan B Engineers will run test criteria to check the services are running OK and will then hand over the running systems to the customer's IT staff. In the extreme event of the customer's staff not being available, Plan B can provide operational support under a support contract.

During a disaster Plan B staff are dedicated to recovering your systems. No reliance on staff who are trying to recover a larger problem, or worries about being at the top of a service provider's priority list when they have many systems down at one time.

## Accessing the Rescue Platform

Customer access to recovered systems can be via a number of different methods depending on the situation, the customer's overall Business Continuity Plan (BCP) and other provisions.

If the customer's existing network is still available (which might happen if the disaster was confined to the server level) then the customer's staff can simply establish a VPN from that network to the Rescue Platform. Alternatively, if the customer has a pre-provisioned alternative DR location, then again a VPN can be set up from the DR location. If the situation means that existing locations are not available then a roaming VPN service can be established that can be accessed by the customer's laptops or other mobile or temporary machines.



Plan B can help with holding BCP information and communicating this with staff via the Plan B portal or via SMS broadcast. We will do whatever we can to ensure your recovery is as simple and straight forward as possible.

## Transferring off the Rescue Platform

Once the cause of a disaster has been dealt with and a customer's original systems recovered or replaced, Plan B will help with the transition back off the Rescue Platform.

The transition back to your live systems should be treated just like a traditional system migration, with the normal issues of data cut-over to be considered. If required, Plan B can help with the planning and implementation of the transfer.

Alternatively, customers may wish to consider taking the opportunity the original disaster has presented to consider rebuilding their systems on a virtualised architecture. Not only will this bring potential benefits of consolidation but also make transferring off the Rescue Platform extremely simple. Plan B can help plan and implement such a move to a virtualised architecture.

## Security

Because of the nature of what we do for our customers, security of our operation is paramount at Plan B. We take the requirements, implementation, monitoring and management of our systems and organisational security very seriously.

As part of keeping things secure is keeping security measures confidential, we do not as policy disclose any specifics about our security, however we can give a general indication of our approach.

### **General security approach:**

We take security seriously and operate our business and our systems according to documented policies and procedures within an overall security framework. Our organisational security is based on ITIL and we are certified ISO27001/2 International Information Security Management Standard compliant.

We take physical security seriously and only operate our systems from secure data centres that have strong physical security, and operate strong access and authorisation controls.

Our systems are designed and architected to be inherently secure and operate as coordinated elements within a whole, making them very hard to subvert from outside. We use encryption and Public Key Infrastructure (PKI) to ensure security of data in transit.

We understand that a business is only as secure and reliable as its people and so all Plan B staff are vetted to BS7858 standards before being employed. We allow no exceptions to this.

## Plan B Infrastructure

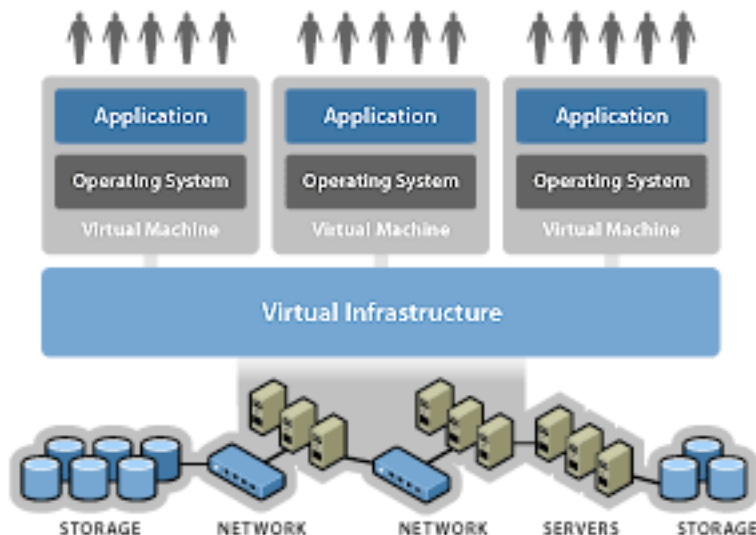
Plan B host their systems in specially selected data centres that can meet our exacting requirements for physical security, resilient N+1 subsystems and ITIL /ISO27001/2 processes and procedures, including:

- Dedicated substations
- Diverse main ring power feeds to substations
- Generator backed up N+1 UPS Power systems
- N+1 Air cooling and conditioning systems
- Full fire detection and suppression systems
- Full flood detection systems
- Strong physical security perimeter, including anti-tailgate systems and multi-layer entry controls
- 24/7 on site security and engineering

Our Rescue Platforms are designed around an N+1 architecture at all levels based on best of breed technology for both hardware and software.

## Virtualisation

At its most basic, server virtualisation is a technique that allows one physical server to run multiple software instances, each one with its own operating system, own settings, own applications, and each one believing that it is actually running on its own dedicated piece of hardware.



Virtualisation technology inserts a thin layer of software directly on top of the server hardware and allows multiple virtual machines to be run on a single server. Each virtual machine behaves exactly like a real server and can be configured (CPU/Memory etc.) as required.



Plan B implement VMware Inc.'s Virtualised IT Infrastructure products to create our Rescue Platforms. We believe VMware offer the most stable, efficient and manageable commercial grade virtualisation technology available in the market today.

VMware's infrastructure products allow us not only to create virtualised environments but also to manage our extended environment where we run many virtual machines and need to quickly manage resources across multiple systems. It allows us to centralise management of all our systems giving us control of our multiple virtual servers. It also allows rapid provision of new applications, rapid movement of virtual machines across physical servers, and comprehensive management of resource pools.

The key benefit the use of virtualisation brings Plan B and its customers, is to break the bond between an operating system and the hardware it is running on. Traditionally, if you want to take a copy of a server (a server image) and get that copy to run immediately, without alteration, on an alternative piece of hardware, you would have to ensure that the new hardware was absolutely identical to the original machine. Hence the traditional disaster recovery approach (to achieve a 'warm standby' level of recovery) is to have a second set of identical hardware sat in a second geographically separate data room just in case it is ever needed in a disaster. That second set of hardware would still need managing in exactly the same way the live hardware is managed, and also need data shipping to it periodically. This is costly and many companies find it impossible to justify versus the perceived level of risk.

Plan B's use of a virtualised Rescue Platform means we can take an image of a customer's system and get it running quickly on our hardware freeing the customer from the costs of buying, maintaining and updating their own dedicated disaster recovery servers.

To get a system image taken on a physical server to run within a virtualised machine does require a degree of customisation. This sorts out things like driver changes, network changes and also sets the systems up to boot and run in the Rescue Platform environment. This process is known as the Physical to Virtual (P2V) conversion. Plan B use our own proprietary technology to do this automatically each time we process a new Snapshot to create a new Rescue Image of a customer's machine.

Once a physical server's image has been converted to run on the virtual platform (P2V) it becomes completely independent of the hardware and can be run without alteration on any system running the same virtualisation technology.

Once a Client image has been converted and tested it can be brought back up on the Plan B recovery platform as easily as booting a physical server.



## Business Continuity

Plan B are specialists in IT Disaster Recovery, and we believe that our service will bring a wholly new level of recovery to many organisations.

However, being able to recover your IT systems is only part of solving the problems that come with a situation that threatens your business. We therefore firmly believe and suggest that our service should be implemented as part of a comprehensive Business Continuity Plan (BCP) that will put our customers in the best possible state to take advantage of the fast level of IT recovery our service can provide.

As an organisation we have extensive experience of business continuity planning and in particular IT disaster recovery in all its guises. However, we believe in sticking to what we do really well and therefore we don't provide general BCP consultancy but we can help with the IT element and general applicability of our service.

We also believe that business continuity plans should be tested periodically, and at least once a year. We encourage all our customers to test our service as part of their BCP testing and are happy to help facilitate dry runs as part of this. We can provide advice and guidance through the testing and can also help with regulatory audits.