



## Business Continuity:

# A Case Study of a Leading Global Hedge Fund



### › Background:

Established as one of the leading hedge fund consultants, CloudGni provide assistance to several hedge funds and asset managers around the world. Their expertise enables institutional investors to access some of the best performing emerging markets in the world.

As a consultancy firm, CloudGni work with several funds across the City. One of their clients is considered to be a leading specialist asset manager offering a range of investment strategies focused on Russia and the former Soviet Union. With a veteran investment team based in Moscow, their local presence and experience in the region provides superior access to opportunities and information flow. The firm is owned and managed by a team of Western and Russian professionals in Moscow, New York and London. With multi-site offices, the fund has invested heavily in their own physical server environment, but a change in their business continuity strategy meant that deploying a secondary site would be far too costly and cumbersome.

The hedge fund industry is forecasted to add assets of \$80bn in 2012 according to a report from Barclays. CloudGni is well established to participate in helping funds enjoy growth over the next year. Due to compliance issues, we are unable to disclose the name of the particular hedge fund cited in this case study, however CloudGni are happy to be consulted as a reference.

### › The Problem

The hedge fund concerned took the option several years ago to invest in their own physical server infrastructure based on-site at their secure facility. Business Continuity had previously been delivered by a traditional

tape based back-up system. This method of backup is expensive and cumbersome as the tapes need to be stored off-site away from the physical servers and changed on a daily basis. Tapes are expensive and offer no guarantee of recovery should the tape be corrupted, lost or stolen.

Business continuity planning through disaster recovery and online backup is critical for both FSA compliance and to mitigate against the risk of data loss and server downtime. The key areas to consider are the 'Recovery Point Objective' (RPO) and the 'Recovery Time Objective' (RTO). The RPO is defined as the maximum tolerable period in which data might be lost from a server due to a major incident resulting in downtime. The RPO gives business continuity planners a time limit to work towards. For instance, if the RPO is set to 4 hours, then in practise, offsite mirrored backups must be continuously maintained. A daily offsite backup on tape, such as in this case, would not be sufficient.

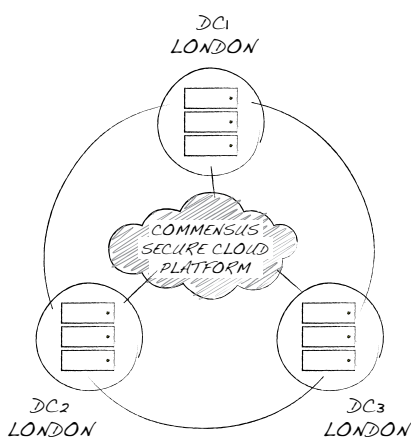
The RTO is the duration of time within which a business process must be restored after a disaster. For this fund, tape backups resulted in an RTO of several days and the RPO was set to the point when the previous tape had been taken off-site. This meant that potentially a whole day of data changes could be lost in the event of a failover. The ability to test their tape based disaster recovery method also posed an issue as there was no guarantee that the tapes had not been corrupted.

The IT departments daily routine would be to insert another tape into the recorder and give the old tape to a third party provider to take offsite. This meant that there was a huge amount of human involvement in the business continuity process and meant that too much risk could be proportioned to human error, in the event of a tape being lost or not being inserted back into the recorder.

CloudGni's IT Manager, Abdi Hersi was presented with the challenge of implementing a more robust Disaster Recovery plan and delivering it within the budgets presented by the Fund. Abdi commented, "Their previous business continuity plan was becoming incredibly out-dated. In the event of a failure, a tape restoration would take place on a donor server which was not efficient and would take several days to restore. In the event of a problem, we couldn't warrant the risk of being down for such a long period of time."

This problem left the company exposed to a significant RTO. As the fund's data volumes were set to grow, it became increasingly clear that the time to restore the data would take days and would open the business up to significant downtime should a failover occur. Other providers had suggested implementing a colocation facility within a datacentre environment where their servers could be replicated in real time. With the need for enhanced cooling, increased security not to mention the hardware

#### UK PLATFORM TOPOLOGY



To find out more please call:  
**0800 612 6610**

costs meant that this solution was not at all practical due to the level of investment that would be required. Commensus was able to provide a complete solution that presented all the benefits of a secondary facility in the Cloud, but with no upfront costs. With the Cloud, customers only need pay for the resources actually used each month. This ensures that capital expenditure previously spent on purchasing IT assets such as servers, could now be reallocated to an operational budget within the business.

CloudGni needed to find a solution that presented a RTO guarantee of less than 4 hours with the ability to monitor and retain security of their servers for compliance purposes. With Commensus, the RTO could be less than 1 hour and the solution could utilise the Cloud, ensuring that the data requirements could grow with the business and be fully scalable.

The capital expense involved in buying hardware and software for a secondary facility, along with the colocation costs to house it, exceeded the company's budget and was not at all practical. After much investigation they decided that a hosted DR from Commensus was the best solution.

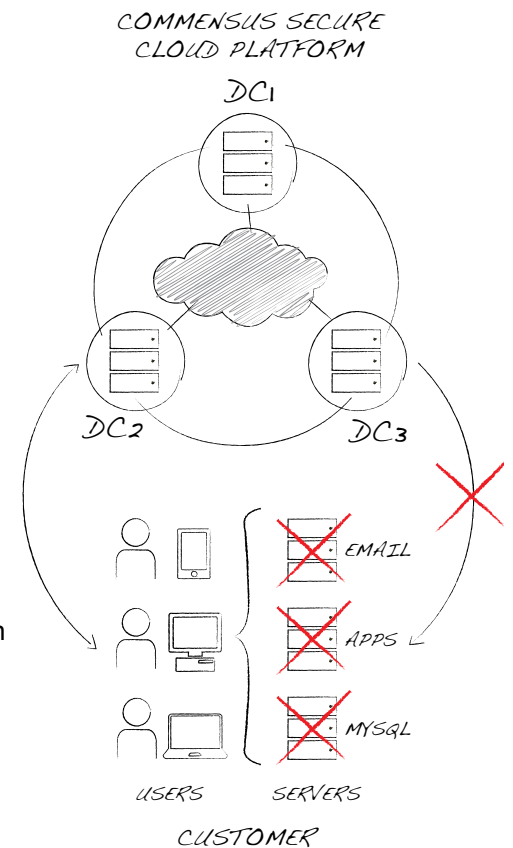
## Our Solution:

### Hosted Disaster Recovery

Commensus deployed a fully managed Private Cloud environment for the hedge fund on our Virtual Infrastructure Platform. This Private Cloud is fully dedicated to the fund and operates using VMware vSphere architecture on Tier 1 physical equipment; EMC for storage, Cisco for networking and HP blade servers throughout.

Commensus provide an enterprise level business continuity plan using the Private Cloud by replicating the firm's data from their secure facility onto our platform. The data physically resides in one of our five European data centres. For the fund concerned, UK compliance meant that the data needed to be replicated inside of the UK. The solution therefore replicated the fund's servers into one of our Tier 3+ specification data centres in London. All data centres deploy the highest standards of physical security through a complex series of firewalls, security protocols and BGP Internet routing. This ensures that our network is protected against attack at every layer of the infrastructure.

Within the Commensus Cloud platform, hardware is automatically replicated for maximum resiliency within the data centre. This means that if a Virtual Machine, Server or SAN were to fail at any time, then another Virtual Machine, Server or SAN would automatically take control within the Commensus platform. This removes the problems associated with downtime and ensures that the fund's DR servers are always ready to come online in the event of a failover.



*"The DR solution provided by Commensus is exceptional. It provides them with full control over their systems and complete peace of mind in the event of a failover."*

**Abdi Hersi**  
CloudGni

*“The Commensus Cloud and DR solution makes their services hard to ignore when compared to other solutions in the market.”*

**Abdi Hersi**  
**CloudGni**

By replicating their servers into the Cloud, the company gained access to a secondary site without the need to invest in a secondary facility. Data is replicated in real time through the Internet via a VPN. This ensures 0% loss in the event of a failover. Compared to the competition, the Hosted DR solution offered enterprise guarantees for a fraction of the cost which mitigated against the risk of a disaster or server malfunction.

Commensus offer two types of DR, firstly into an ‘active’ server environment. In this instance, the RTO is a matter of minutes in the event of a failover with no data loss whatsoever. The second option is for the servers to be replicated into a ‘passive’ server environment where the servers are essentially in stand by mode. In this instance, the server needs to be powered on in the event of a failover which extends the RTO by 1 to 2 hours.

The Fund opted for our passive replication solution guaranteeing the speed of recovery in the event of an invocation. Commensus are able to recover their virtual servers, regardless of data volumes within a one hour to protect the company from loss or downtime. The whole solution incurred no capital expenditure as the solution is paid for on a monthly basis ensuring that they only incur charges for the amount of cloud storage actually consumed.

#### ➤ **About Commensus**

*Commensus is one of the leading providers of IT managed services to the finance, insurance and alternative investment industries. Based in Central London, our enterprise Cloud Computing platform guarantees network uptime and is backed by 24/7 unrivalled support. Since 2008, we’ve grown to be recognised by the industry and our customers as a provider of superior IT services. Cloud Computing has enabled us to deliver a ‘one stop shop’ of technology services that help you to comply with relevant industry regulations whilst delivering uncompromised levels of security and resilience.*

➤ **Find out how Commensus could help your firm. Contact our Business Consultants today.**



**Commensus PLC,**  
**1 Vincent Square,**  
**London, SW1P 2PN**

**Call: 0800 612 6610**  
**Email: [sales@commensus.com](mailto:sales@commensus.com)**  
**Visit: [www.commensus.com](http://www.commensus.com)**